CYBER SECURITY DIGEST

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

DT : 13-09-24

Editor's Note

Welcome to our first edition of Cybersecurity Digest, where we bring out the most critical updates and insights from the world of cybersecurity. In this edition, we explore the basics of Cybersecurity, CIA Triad, cybercrime news and some of its best practices and safety tips. Our goal is to keep you informed and empowered to protect our organization's digital assets.

Cybersecurity is an ever-evolving landscape, and staying ahead of threats requires constant vigilance. We hope this digest provides you with valuable information to help you navigate the complex world of cybersecurity.

We welcome your feedback and suggestions for future topics. Please reach out to us at ciso@Megrrb.in

Stay vigilant

CISO

CIA TRIAD

The security of any organization starts with three principles: **Confidentiality, Integrity and Availability**. This is called as CIA, which has served as the industry standard for computer security since the time of first mainframes.

Confidentiality: The principle of confidentiality assert that only authorized parties can access sensitive information and functions.

Integrity: The principle of integrity assert that only authorized people and means can alter, add or remove sensitive information and functions.

Availability: The principle of availability assert that systems, functions and data must be available on demand according to agreed-upon parameters based on levels of service.

CYBER SECURITY

Cyber Security is the protection to defend internet connected devices and services from malicious attacks by hackers, spammers and cyber criminals. Companies use the practice to protect against phishing schemes, ransomware attacks, identity theft, data breaches, financial loss, etc. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smart phones to networks and databases, from attacks.

CISCO Systems, the tech conglomerate specializing in networking, the cloud and security, defines cyber security as "….the practice of protecting systems, networks and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users or interrupting normal business processes.

In today's digital world, one cannot ignore cyber security. One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals.

CYBER CRIME

Cyber Crime is defined as any unauthorized activity involving a computer, device or network. There are three generally recognized classifications of cyber crime: computer assisted crimes, crimes where the computer itself is a target and crimes where the computer is incidental to the crime rather than directly related.

CYBER SECURITY

Cyber Security Best Practices

- Use VPN to privatize your connections
- Check properly before clicking on any links
- Do not be lethargic with your passwords
- Scan external devices for viruses
- Store sensitive information in a secure place
- Enable two-factor authentication
- Double check the HTTPS on websites
- Remove adware from the computer
- Disable Bluetooth connection when you are not using it
- Avoid using public networks
- Invest in security upgrades

Cyber Safety tips

- ✓Keep software up-to-date
- ✓Avoid opening suspicious emails
- ✓Use antivirus and antimalware software on the electronic devices
- ✓Use a security file sharing solution to encrypt data
- ✓Use strong passwords
- ✓Backup your data
- ✓Be cautious of phishing scams
- ✓Use two-factor authentication
- ✓Don’t reuse passwords

Cyber crime victim in city gets back money

A victim of cyber crime from the city got back the entire money siphoned off by a company.

The victim, whose identity is protected, lodged an FIR resulting in investigation and recovery of the money within four months after the matter was reported.

The lady working in a government sector had lodged the FIR at Crime Branch PS Shillong stating that in January 2023, she was lured to invest Rs 17,50,000 in a reputed company by her friend in good faith.

The victim was allowed to work from home. But after a month, she realised that the activities of the company were doubtful though it made a lot of promises in various zoom meetings she attended.

She then contacted her friends and a mentor who claimed to be representing the company. She also emailed to the company to return her money but in vain .Finding no alternative, she approached the Crime Branch Police Station Shillong in April 2023 following which a case was registered.

After freezing various bank accounts of the accused by the police, he had no other option than to flee the country for three months but under pressure, he agreed to pay the money through the company representative.

On August 2023, she received the full amount through demand draft.

Scammer poses as CJI DY Chandrachud requests Rs 500 for Cab fare in viral scam

Former bank employee opened 16 fake accounts used for cyber fraud, landed in Delhi Police net

Two more persons including Bank Official held in Rs 175 Cr online fraud

Cyber criminals looted Rs 1750 Cr upto April this year- NPCI

Chinese hackers breach US, India internet firms, Lumen says

Cyber Security Digest

Bi-Weekly Update by the CISO section of Meghalaya Rural Bank

Vol: I Issue 2

Date: 01-10-2024

Lebanon's Kinetic Cyber Attack

On Tuesday 17th September, hundreds of pagers in Lebanon exploded simultaneously in a coordinated chain attack, targeting members of the political party and paramilitary group Hezbollah which had in previous months ordered, shipped and distributed the pagers to some of its members.

A day later, a similar attack struck again when hundreds of walkie-talkies used by Hezbollah detonated.

But how could these tiny, old-school pagers and humble walkie-talkies be forced to explode?

Experts points out to two possibilities– the first is a cyber attack in which malware forced the pagers' lithium batteries to overheat and then explode.

The second and more likely scenario points to a supply chain attack in which a shipment of pagers bound for Lebanon was intercepted and a tiny amount of explosive surreptitiously inserted with extra electronics to trigger the detonation, which was then remotely activated.

While the world focuses on securing modern digital platforms, this incident highlights a significant vulnerability in older technology. The use of exploding pagers and walkie-talkies indicates that 21st century warfare is not only about technological advancements but also about the creative use of existing tools. This incident underscores that security is not just about the latest technology but understanding the full spectrum of potential threats, including those from seemingly antiquated devices.

Exploding Walkie –Talkie

Exploding Pager

Centre to train 5000 'Cyber Commandos' in next five years to fight cyber threats

Recently, the Central Government announced the plan to train and prepare 5000 cyber commandos over the next five years to tackle the rising cybercrime threats. This announcement was made during the first Foundation Day celebration of the Indian Cyber Crime Coordination Centre (I4C). I4C is a national-level coordination centre for addressing cybercrime issues. These cyber commandos will be trained in IT infrastructure security, digital forensics and incident response. Other launches along with Cyber Commandos: Centralized Suspect Registry, Samanvaya Platform and Cyber Fraud Mitigation Centre (CFMC)

CYBER CRIME NEWS

- **Cyber fraudsters misuse 1930 helpline number to scam people : *Times of India***
- **BookMyShow under the radar as lawyers file cyber crime complaint over Coldplay tickets : *CNBC TV18***

EMAIL ATTACKS

First , let's see how an email works. Suppose John is sending an email to Jack. The email first goes to the email server. Then it goes to the DNS server to find the IP address of the destination. From the source email server, the email goes to the destination server. From there, the email is sent to the IP Address on which Jack is working. It is illustrated in the picture below.

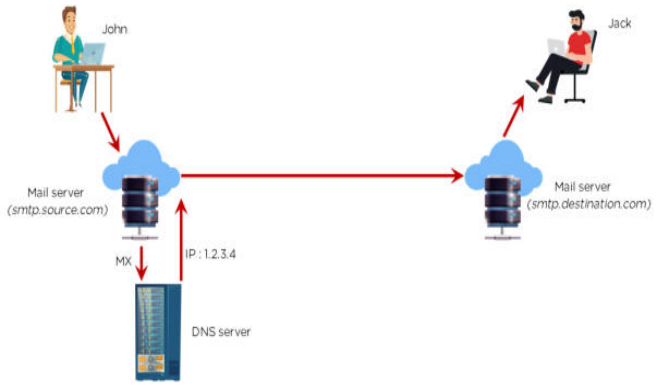


Fig: How email works

2) **Spoofing**: The attacker pretends to be another person or organization and sends you an email stating that it is a legitimate email. For example: Fig 2

After seeing this email, you might share the password to your computer. Always ask the person from whom you received the email one more time to confirm that he is the right person.

3) **Email attachments**: You can send files through emails. These files may be images, documents, audio, or videos. Attackers send you an email, and you are encouraged to open the attached file. For example: Fig 3

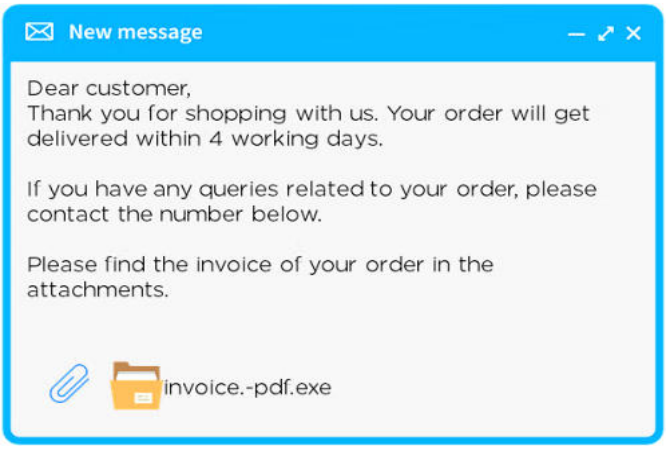


Fig 3

There are three types of email attacks:

1) **Phishing**: The attacker sends bait, often in the form of an email. It encourages people to share their details. For example, you receive an email like this:

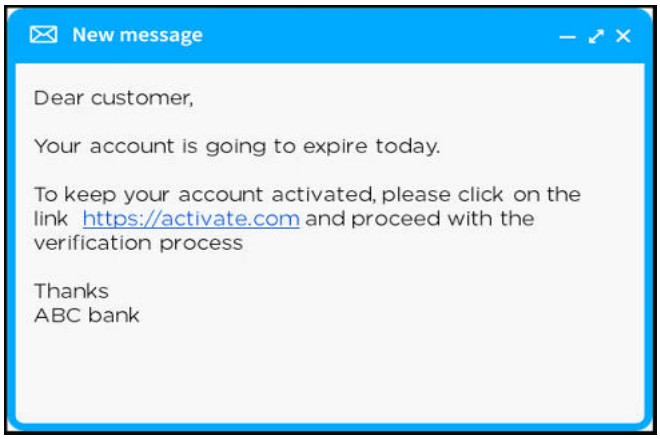


Fig 1

If someone is a customer of ABC bank, he would probably open the link and give the details. But these kinds of emails are always phishing; banks do not send emails like this.

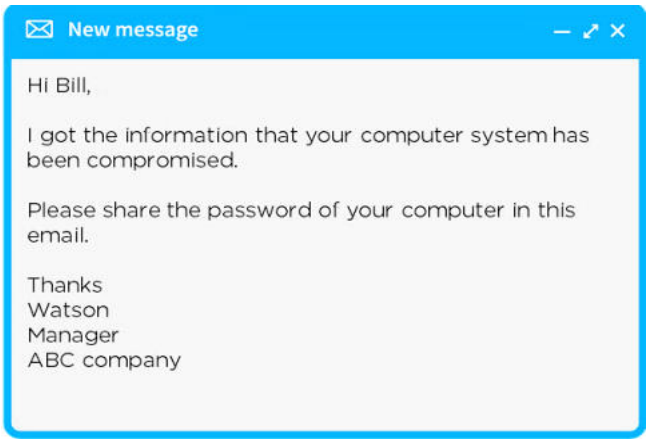


Fig 2

Date : 15-10-2024

Volume 1, Issue 3

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

"Never trust anything you see on the Internet"

The Kerala Deepfake scam serves as a reminder of the importance of being vigilant when using technology. People should be careful about the information they share online and should be cautious about the people they interact with online.

The Evolution of Generative AI: Deepfakes

Generative AI refers to the subset of AI technologies capable of creating new content that resembles human-generated outputs, text, images, videos or even code. This capability is built upon machine learning models, particularly generative adversarial networks (GANs), variational autoencoders (VAEs), and, more recently, large language models (LLMs) like OpenAI's GPT series. These models are trained on vast datasets, learning to replicate and innovate on the data patterns they're exposed to.

On the other hand, deepfakes, a portmanteau of "deep learning" and "fake", are a specific application of generative AI focused on creating hyper-realistic video and audio recordings. Leveraging techniques such as GANs and deepfakes can manipulate existing media to make it appear that individuals are saying or doing things they never did. Initially gaining notoriety in misinformation and digital forgery, deepfakes have also found legitimate applications in filmmaking, gaming, and virtual reality, demonstrating the technology's ambivalent potential.

In the meantime, deepfakes, which are high-quality AI-generated fake videos, have been circulating online. Synthetically generated deepfake videos have exceeded acceptable limits in terms of reality distortion. This disruptive technological development significantly impacts the truth. Due to the easy accessibility of generative AI models, the probability of misuse of this technology aggressively increases. Though deepfake technology came into this game in 2017, large language models like ChatGPT, Bing, Bard, GPT-4, etc. add a whole new dimension to this scenario. In particular, political figures are targeted in deepfake videos, contributing to the erosion of media credibility.

This technology has spread information, rumors, and propaganda, provoked political strife, blackmailed individuals, and threatened democracy. The capabilities of this technology to manipulate reality have gone too far. This paradigm-shifting technological revolution is altering the truth and creates a zero-trust society insidiously.

Case Study: Kerala's First Deepfake Fraud

In July 2022,Kerala witnessed its first reported deepfake fraud case. A 73-year-old-man, Radhakrishnan, fell victim to a sophisticated deepfake scam that resulted in the loss of ₹ 40,000.

The victim received a Whatsapp call from someone who appeared to be his former colleague, Venu Kumar. The caller, using deepfake technology, perfectly mimicked Venu Kumar's voice and appearance. The caller asked Radhakrishnan for a loan of ₹ 40000, claiming that he was in urgent need of money. Believing that the caller was indeed his former colleague, Radhakrishnan transferred the money without hesitation.

After realizing that he had been scammed, Radhakrishnan filed a police complaint. The police investigation revealed that the deepfake call was made by a fraudster using sophisticated AI software.

Hunting in Cyberspace: Tracking down Watering Hole Attacks

The term **Watering Hole Attack** comes from the hunting. Rather than tracking its prey over a long distance, the hunter instead determines where the prey is likely to go, most commonly to a body of water (the watering hole) and the hunter awaits there. When the prey comes of its own will, often with its guard down, the hunter attacks.

A watering hole is a cyberattack technique used by attacker to identify websites that are frequently visited by their target victims and then infecting these websites by injecting malicious code (often JavaScript/ HTML) into web pages to gain access to visitors' devices and information or access assets on network.

The payload may be automatic, or the attacker may cause a bogus prompt to appear or fake error page telling the user to take an additional action that will download malicious code.

Fake error page to lure victim to click

How a Watering Hole Attack works?

- **Target Identification**: Attackers identify websites frequently used by their target victims. These websites could be industry forums, professional association websites, or popular news portals.
- **Website Compromise**: Attackers exploit vulnerabilities in the target websites to inject malicious code. This could involve exploiting unpatched software or weak security configurations.
- **Victim Infection**: When victims visit the compromised websites, the malicious code executes on their devices, infecting them with malware. The malware exploits weaknesses in the target's cybersecurity. The attacker delivers and installs malware without the target realizing.

Cyber Crime News

- Cyber attack cripples **Uttarakhand Government IT System**, halts entire digital operations–***The420.in***
- Cyberattack group '**Awaken Likho**' targets Russian Government with advanced tools—***TheHackerNews***
- **American Water**, the largest water utility in US, is targeted by a cyberattack—***APNews***

Cyber Security Awareness Month -October 2024

NABARD, DoS CSITE-Cell is commemorating Cybersecurity Awareness Month in October 2024.

Unleash your inner cyber superhero and join the movement to secure our world.

Cybersecurity Digest

Uploaded by the CISO Section of Meghalaya Rural Bank

Vol I Issue 4

Newsletter
Date:01-11-2024

Cyber Arrest

Cyber Safe

Cyber World

Cyber arrest is a cyber-crime technique, whose incidence has been on the rise since a year and a half. Fraudsters posing as law enforcement officials of various agencies, including the state police (particularly the crime branch), CBI, ED, Income Tax, Narcotics Control Bureau (NCB), RBI and even the Supreme Court, put victims under immense mental stress, accusing them of knowingly or unknowingly indulging in major crimes, such as human trafficking, narcotics smuggling and/or trafficking or money laundering or that their close relative is under arrest for any or a combination of these alleged crimes.

The fraud typically begins with a video call where the con artists make the otherwise worldly wise believe they are in conversation with genuine investigators of a major law enforcement agency to build fear psychosis. Once softened, the scamsters confine the targets to their premises, including a room, where they are placed under cyber arrest (digital arrest) and directed to keep their cellphone cameras and microphones on 24X7. Demand for money could follow for securing bail. The other ruse is to verify whether their savings aren't proceeds of crime.

To do that, they advise the targets to transfer their funds to a special purpose digital receptacle for a short while till the verification is complete, which essentially are certain specific bank accounts. After the funds are dropped in the receptacle, they are sucked out in no time through multiple layers/ chains of bank accounts and the caller hangs up for good.

How the victims fail to see through the trick of digital verification of funds and allow themselves to be conned to voluntarily load them into the special receptacle, boggles the mind. But such are the mind games the scamsters are successfully playing with otherwise sharp individuals having pretty deep pockets.

Cyber Arrest

"Cyber security is not just a necessity, it's a responsibility.

Protect data, protect the nation"

Cyber Arrest: Case Study

SP Oswal, Chairman and Managing Director of the Vardhman Group, was recently duped of more than ₹ 7 crore. He was misled into believing that he was under probe in a money laundering case. Besides using fake documents and claiming the CBI was hot on his heels, the cyber fraudsters went to the extent of creating a fake Supreme Court bench led by Chief Justice of India D Y Chandrachud to hear his case. That Oswal reportedly paid up after the 'court verdict', indicates the dexterity and sophistication the digital crooks are capable of.

Build a Secure Digital Future: Be Cyber Aware

Avoid Phishing Attacks : Do not click on suspicious links or attachments. Phishing emails are designed to trick you into giving away sensitive information. Look for signs like unfamiliar email addresses, grammatical errors, or urgent requests for personal data.

Use strong passwords : Create strong passwords with a mix of letters, symbols and numbers. Your passwords are the first line of defence. Avoid using easily guessable information like birth dates or common words.

Enable multi-factor authentication : Enable multi-factor authentication (MFA) for added security. Even if your password is compromised, MFA ensures only you can access the account.

Keep software updated : Regularly update your system and software to avoid vulnerabilities. Outdated software can have security flaws that hackers exploit. Ensure that your operating system, antivirus, and all apllications are up to date with the latest security patches.

Report suspicious activity : If you notice any unusual activity, promptly inform your bank. You can also file a complaint on the Cyber Crime Portal at **https://cybercrime.gov.in** or call the helpline at **1930**.

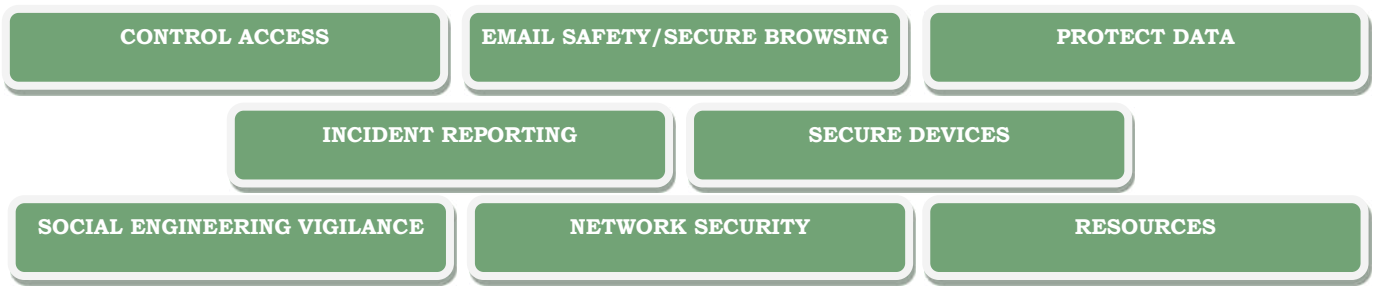
Cyber Crime News

- Cyberfraud losses could amount to 0.7% of GDP, projects Ministry's study—***The Hindu***
- Meta, government launch initiative against online scams—***The Hindu***
- Under 'digital arrest', Pune senior citizen loses ₹ 45 lakh in cyber fraud—***The Indian Express***
- Tamil Nadu cybercrime police bust fake NCRP website—***Times Now***
- Government launches system to block 'fake' international scam calls—***Times of India***
- Deputy Bank Manager amng 2 held for helping cyber cons park money—***Times of India***

Cyber Security : Cultivating a Culture of Society

— Department of Supervision, NABARD

As we continue our focus on cybersecurity, it's vital to recognize that securing our digital environments is an ongoing commitment. Just as we remain vigilant in our personal safety, we must apply the same diligence to our online transactions. In this bulletin, we present **eight essential cyber security habits** to reinforce our collective security efforts.



Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 1, Issue 5

Newsletter Date: 15-11-2024

PIG-BUTCHERING SCAM

A pig-butchering scam is a type of investment fraud that lures individuals into investing their money in seemingly legitimate and profitable ventures. Typically, the scammers promise high investment returns within a short period. Pig-butchering scammers often use fake images and impressive-yet-fraudulent investment portfolios to convince victims of the legitimacy of their schemes. Once victims are hooked and have invested a significant amount of money, the scammers suddenly disappear, leaving victims with no way to recover their funds. The term "pig butchering" is derived from the idea that the scammers fatten up their victims with the promise of lucrative returns before "slaughtering" them for their money.

Pig Butchering Scam

The scam often begins with a seemingly innocent chat initiated by a random person. The scammer might claim to have received the victim's number from a mutual friend, while also appearing unsure if they have the correct number. However, this is just an act to engage the victim in conversation. Scammers have also been known to use images of attractive people to lure victims, preying on their desire for companionship or romance to build trust and establish a connection.

As the conversation progresses, the scammer gradually introduces the victim to the fake investment scheme and promises significant profits within a short period if the victim invests a certain amount. Unfortunately, many victims fall for this fraudulent scheme due to the scammers' persuasive tactics and convincing appearance of legitimacy.

The Group Chat Strategy

By adding multiple people to chat groups that are centered around investment discussions, scammers can quickly gauge the interest of their targets. Those who remain in the group are more likely to be interested in investing, making them prime candidates for the scam. On the other hand, individuals who leave the group are either aware of the scam or are uninterested in investing. Hence, they are less likely to be persuaded by the scammer's tactics.

The scammers consist of a group of individuals with different roles and objectives. Some of the chat group members are fake profiles created by the scammers themselves to make the group seem more authentic. This approach makes the process for scammers easier, enabling them to focus their effort on individuals who are more susceptible to their fraudulent schemes. It also creates an environment that promotes a sense of community and social validation, as potential victims would see that other people are engaging in discussions about investment and are not calling out the scam.

Inside this issue:

Pig Butchering Scam	1
The Group Chat Strategy	1
Warning signs of Pig Butchering Scam	2
Cyber Crime News	2

Saving victims from falling prey to pig-butchering

Given the alarming trends and the growing sophistication of pig-butchering scams, it is crucial for individuals to take proactive steps in safeguarding their investments and personal information. The following recommendations are designed to help individuals recognize the warning signs of these scams and take appropriate action:

1. **Be cautious of unsolicited messages and group chats.** As previously discussed, scammers often initiate contact through seemingly innocent chat messages or by adding individuals to investment-themed group chats. Be wary of engaging with strangers and carefully consider the source of any unsolicited messages or group chat invitations.
2. **Verify the legitimacy of brokerages.** Before investing your money, make sure that you conduct a thorough investigation of the brokerage you're considering. Check for recently created domains via registration data or news articles. If something seems suspicious, trust your instincts and avoid engaging with the platform.
3. **Monitor identity theft resources for leaked personal information.** Be vigilant about the security of your personal information. Regularly check or sign up for reputable identity theft monitoring services to track any leaks or breaches involving your data and take appropriate steps to secure your information if needed.
4. **Be skeptical of high investment returns with low risks.** If an investment opportunity promises high returns with minimal risk, it is likely too good to be true. Always research and verify investment opportunities before committing your money.
5. **Educate yourself about emerging tactics.** Stay informed about the latest strategies employed by scammers, such as the use of group chats and fake brokerages. By understanding how these scams work, you can better recognize the warning signs and avoid becoming a victim.
6. **Report suspicious activity.** If you encounter a potential pig-butchering scam, report the incident to law enforcement. Your report could help prevent others from falling victim to the same scam. If you have already transferred funds to fake brokerage websites, it is best to report this as soon as possible to potentially recover them.

Cyber Crime News

- Cyber crimes: 4.5 lakhs 'mule' accounts frozen, many in public sector banks - ***The Indian Express***.
- Incidents of cyberattacks in India may reach 17 trillion by 2047: Study - ***The Hindu***.
- Indians lose ₹ 1.5 lakh to cyber criminals every minute: Official – ***The Hindu***.
- Cyber Fraudsters impersonate TRAI officials, MHADA employee scammed of ₹ 3 lakh in digital arrest scheme –***The 420.in***
- Class XI "influencer" student scams 200 Instagram followers with a fake investment scheme - ***The Indian Express***.

CYBERSECURITY DIGEST

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 1, Issue 6

Newsletter Date
01-12-2024

UPI Scam: The unprecedented surge

The rise of digitization in India has brought sweeping changes, with one of the most significant being the adoption of the Unified Payments Interface (UPI). Launched in 2015, UPI revolutionised banking by empowering popular apps like BHIM UPI, Google Pay, and PayZapp. Now, leaving home without cash is no longer a worry because your phone serves as your wallet.

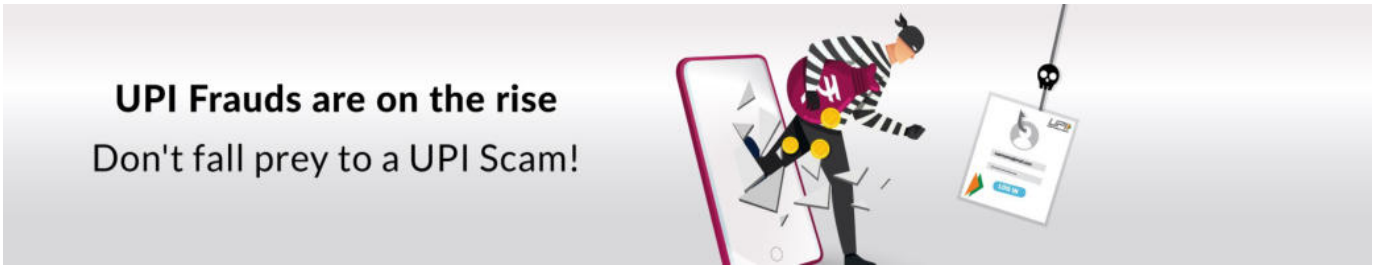
However, alongside its convenience, UPI has also brought challenges, notably in the form of scams like phishing scams, QR Code frauds, SIM swapping scams, fake payment apps and overcharging schemes. Cyber scams, already a prevalent threat, have amplified with UPI's popularity, leading to a surge in digital payment fraud in India. According to the RBI Annual Report, digital payment fraud reached a record 14.57 billion rupees ($175 million) in the fiscal year ending March 2024.

The main downside of UPI is that scammers who have your UPI ID can flood you with collect money or autopay requests. If you mistakenly approve these requests, you'll end up paying the fraudster, enabling them to use your money for their purchases.

The UPI scam operates on a simple principle-you are deceived into believing a false story or are caught off guard and approve an unknown UPI collect money or autopay request. You might wonder why you would approve such unfamiliar requests. The reason is that you may not be able to distinguish between a genuine request and a fraudulent one. It's important to note that the collect money or autopay request itself is valid, but the person initiating these requests is a fraudster.

UPI IDs are generally expressed as phone numbers followed by the UPI provider extension. This is exploited by scamsters. Phone numbers and details are soft targets since phone numbers are shared often and are quoted at multiple places - e-shopping, restaurants, malls, parking places and so on. Given that it's easy to crack UPI IDs, customers using the same for online and digital transactions need to be well aware of the risks. There have been a number of fraud cases in the past where customers have approved transactions thinking it's a receipt but have ended up transferring money from their account.

To safeguard against these threats, it's crucial to remain vigilant and exercise caution. Always verify the authenticity of communications and transactions, avoid clicking on suspicious links, secure your SIM card, and opt for secure UPI IDs for transactions. By staying informed and proactive, individuals can protect themselves from falling victim to these prevalent UPI scams and ensure safe digital transactions in an increasingly interconnected world.



How Do Hackers Execute UPI Fraud?

It's been observed that fraudsters follow a pattern whilst executing these elaborate plans. As a result, we've managed to weave a stepwise timeline of how these plans are generally performed. Let's take a look at how UPI fraud occurs:

- **STEP 1:** It all starts with a random call. Fraudsters usually call targets to get their attention, as opposed to texting. They commonly disguise themselves as a bank representative, calling for a seemingly harmless issue.
- **STEP 2:** To make the call sound legit, they proceed to ask verification questions like your date of birth, name, or mobile number.
- **STEP 3:** There is always a problem. Hackers use technical difficulties in the app or website to talk to you. They usually weave false stories that convince you to forfeit your personal information to resolve the issue.
- **STEP 4:** Once the fraudster has convinced you, they ask you to download an application on your phone. Some of these apps are AnyDesk and ScreenShare, which are available on the Google Play Store.
- **STEP 5:** While downloading AnyDesk or a similar application, it asks for privacy permission, like other regular apps. But don't be fooled; these apps can access everything on your phone.
- **STEP 6:** The fraudster will then ask you for a 9-digit OTP generated on your phone. As soon as you reveal the code, the hacker will also ask to grant permission from the phone.

STEP 7: When the app acquires all permissions required, the caller starts to take complete control of your phone without your knowledge. After gaining full access to your phone, the hacker steals passwords and begins transacting with your UPI account. Thus, you become one of the many victims of UPI fraud.

We identified other approaches, too. For example, fraudsters send an SMS and ask you to forward it to another number they provide. After the message is successfully sent, the fraudster can link your mobile number or account through UPI to their mobile.

Pagejacking

Page hijacking is a deceptive technique used by cyber attackers to manipulate web traffic. By creating a duplicate of a legitimate website, attackers aim to redirect users to a malicious site. This can be achieved by exploiting search engine algorithms, which may mistakenly prioritize the malicious site over the original.

Often referred to as 302 redirect hijacking or URL hijacking, this method involves using temporary redirects to trick search engines. The ultimate goal is to transfer the page authority and ranking signals from the legitimate site to the hijacker's site, thereby misleading users and search engines alike.

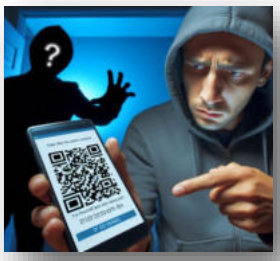
Traffic is the primary currency for securing and amassing revenue on the internet. This traffic and, ultimately, income is what pagejackers aim for, as they try to divert as much as possible from the original site.

Newsletter Date
16-Dec-2024

Vol I Issue 7

Cybersecurity Digest

Bi-Weekly Update by
the CISO Section of Meghalaya Rural Bank



QR Code Scam

Inside this issue:

Quishing Scam	1
Scareware	1
Zero Trust Model	2
UPI Fraud Prevention	2

Quishing Scam: The new Cybercriminal Tool

Quishing, or QR phishing, is a cybersecurity threat in which attackers use QR codes to redirect victims to malicious websites or prompt them to download harmful content. The goal of this attack is to steal sensitive information, such as passwords, financial data, or personally identifiable information (PII), and use that information for other purposes, such as identity theft, financial fraud, or ransomware.

This type of phishing often bypasses conventional defenses like secure email gateways. Notably, QR codes in emails are perceived by many secure email gateways as meaningless images, making the users vulnerable to specific forms of phishing attacks. QR codes can also be presented to intended victims in a number of other ways.

QR codes, or Quick Response codes, are two-dimensional barcodes that can be scanned easily with a camera or a code reader application. The main component of a QR code is data storage. QR codes have the capability to store significant amounts of information including URLs, product details, or contact information. Scanning technology allows smartphone cameras or code readers to easily and quickly access the website to which the URL points.

In a quishing attack, the attackers create a QR code and link it to a malicious website. Typically, the attacker will embed the QR code in phishing emails, social media, printed flyers, or physical objects, and use social engineering techniques to entice the victims. For example, victims might receive an email urging them to access an encrypted voice message via a QR code for a chance to win a cash prize.

Upon using their phones to scan the QR code, victims are directed to the malicious site. The site may prompt victims to enter private information, such as login information, financial details, or personal information. In the example above, the site may request the user's name, email, address, date of birth, or account login information.

Once this sensitive information is captured, attackers can exploit it for various malicious purposes, including identity theft, financial fraud, or ransomware.

Scareware

A scareware is a cyberattack tactic that scares people into visiting spoofed or infected websites or downloading malicious software (malware). Scareware can come in the form of pop-up ads that appear on a user's computer or spread through spam email attacks.

A scareware attack is often launched through pop-ups that appear on a user's screen, warning them that their computer or files have been infected and then offering a solution. This social engineering tactic aims to scare people into paying for software that purportedly provides a quick fix to the "problem." However, rather than fix an issue, scareware actually contains malware programmed to steal the user's personal data from their device.

Zero Trust Model

Zero Trust is a network security strategy based on the philosophy that no person or device inside or outside of an organization's network should be granted access to connect to IT systems or workloads unless it is explicitly deemed necessary. In short, it means zero implicit trust.

In 2010, Forrester Research analyst John Kindervag proposed a solution he termed "Zero Trust."

It was a shift from the strategy of "trust but verify" to "never trust, always verify." In the Zero Trust model, no user or device is trusted to access a resource until their identity and authorization are verified. This process applies to those normally inside a private network, like an employee on a company computer working remotely from home or on their mobile device while at a conference across the world. It also applies to every person or endpoint outside of that network. It makes no difference if you have accessed the network before or how many times — your identity is not trusted until verified again. The idea is that you should assume every machine, user, and server to be untrusted until proven otherwise.

UPI Fraud Prevention

- Beware of fraudulent calls or messages from individuals posing as bank representatives. Verify the authenticity of unknown numbers using apps like Truecaller, and refrain from responding or providing any personal information.
- Avoid sharing your UPI PIN, password or OTP (One-Time Password) with anyone, including bank representatives. Legitimate bank representatives will never ask for such information over phone calls, emails or text messages
- Avoid using public or unsecured networks that can be easily accessed by hackers.
- Do not disable push notifications and transaction alerts on your UPI apps.
- Never leave your bank account unattended.
- When conducting UPI transactions, ensure that you are using a secure and trusted Wi-Fi network.
- Regularly update your UPI apps to the latest version available. Software updates often include security enhancements that can protect you from potential vulnerabilities.
- Keep a close eye on your UPI account activity and transaction history. If you notice any unauthorised or suspicious transactions, immediately contact your bank and report the issue.

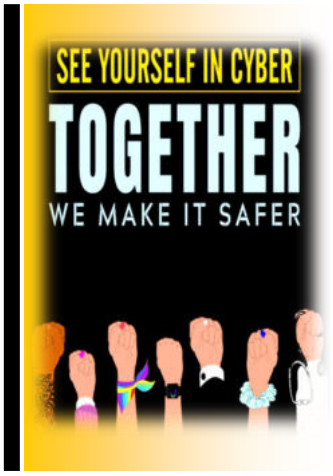
Vol I Issue 8

Cybersecurity Digest

Bi-weekly update by the CISO Section of Meghalaya Rural Bank

Newsletter Date : 01-01-2025

Honeypots



In cybersecurity honeypots are decoy servers or systems that are deployed next to systems your organization actually uses for production. Honeypots are designed to look like attractive targets, and they get deployed to allow IT teams to monitor the system's security responses and to redirect the attacker away from their intended target.

There are various honeypots, and they can be set up according to what your organization needs. Because they appear to be legitimate threats, honeypots act like a trap, enabling you to identify attacks early and mount an appropriate response. This honeypot meaning points to some of the ways they can be used to direct attackers away from your most important systems. While the attacker falls for the bait, you can gather crucial intelligence about the type of attack, as well as the methods the attacker is using.

A honeypot works best when it appears to be a legitimate system. In other words, it must run the same processes your actual production system would run. It should also contain decoy files the attacker will see as appropriate for the targeted processes. In many cases, it is best to put the honeypot behind the firewall protecting your organization's network. This enables you to examine threats that get past the firewall and prevent attacks engineered to be launched from within a compromised honeypot. As the attack ensues, your firewall, positioned between the honeypot and the internet, can intercept it and eliminate the data.

How do Honeypots work?

In many ways, a honeypot looks exactly like a genuine computer system. It has the applications and data that cyber criminals use to identify an ideal target. A honeypot can, for instance, pretend to be a system that contains sensitive consumer data, such as credit card or personal identification information. The system can be populated with decoy data that may draw in an attacker looking to steal and use or sell it. As the attacker breaks into the honeypot, the IT team can observe how the attacker proceeds, taking note of the various techniques they deploy and how the system's defenses hold up or fail. This can then be used to strengthen the overall defenses used to protect the network.

Honeypots use security vulnerabilities to lure in attackers. They may have ports that are vulnerable to a port scan, which is a technique for figuring out which ports are open on a network. A port left open may entice an attacker, allowing the security team to observe how they approach their attack.

Honeypotting is different from other types of security measures in that it is not designed to directly prevent attacks. The purpose of a honeypot is to refine an organization's intrusion detection system (IDS) and threat response so it is in a better position to manage and prevent attacks.

SALAMI ATTACK

A salami attack is a fraudulent technique used by cybercriminals to steal small amounts of money or data from multiple victims, gradually accumulating a significant gain for themselves. It is a deceptive and subtle form of hacking that can go unnoticed for a long time, making it difficult to detect and trace back to the perpetrator.

A salami attack derives its name from slicing thin and indiscernible pieces, just as a salami slicer slices the meat thinly without arousing suspicion. Similarly, cybercriminals in a salami attack carry out their malicious activities stealthily, making it challenging for victims and investigators to identify and stop the breach.

The origin of salami attacks can be traced back to the early days of the digital age when financial systems became increasingly interconnected. As technology advanced, so did the methods employed by cybercriminals, leading to the emergence of salami attacks as a sophisticated technique for financial gain.

Real-Life Examples of Salami Attack

Salami attacks have been carried out in various industries, targeting both individuals and organizations. One notable example occurred in banking, where cybercriminals manipulated financial transactions by rounding off decimal points. By siphoning off the fractions of rupees, the attackers accumulated significant sums over time, all while remaining undetected.

Another salami attack occurred in the e-commerce industry. Cybercriminals exploited vulnerabilities in the payment systems of online retailers, making small alterations to purchase amounts. These seemingly insignificant changes went unnoticed by customers, but the attackers accumulated substantial profits by skimming off a fraction of each transaction.

> Ever spotted a weird, tiny charge on your bank statement? It might have only been a couple of rupees, and you wrote it off as an error. But what if it wasn't? Or maybe it was the first step in an elaborate cybercrime strategy called a salami attack?

Citibank : SALAMI Attack

The Citibank hack was the first significant cybercrime involving banks. In 1994, Russian computer programmer Vladimir Levin tricked Citibank's computers into transferring money to his account. He then used the money to buy goods and services in various locations around the world. Levin pleaded guilty in January 1998, admitting that he had hacked into Citibank's systems and obtained the customer information.

Although Levin did not steal any money directly, he did gain control of funds belonging to others. Citibank denied that anyone within the bank helped Levin carry out the crime. However, no one has ever claimed responsibility for Levin's actions.

According to published reports (Citigroup), Citibank's internal systems detected suspicious activity involving two wire transfer requests totaling $26,800 and $304,000. When bank personnel contacted the Federal Bureau of Investigation, they could trace the source of the funds to an account belonging to Michael R. Levin, a resident of New York City. Telephone records showed that Levin had used his home telephone number to make the fraudulent requests. In addition, investigators determined that Levin had transferred money out of the United States through Western Union offices in Moscow, Russia.

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

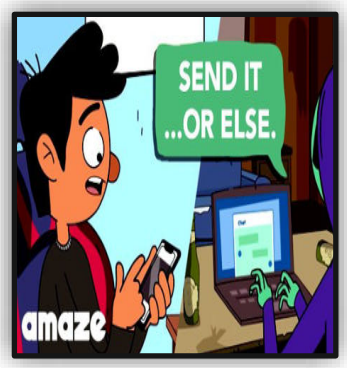
Date: 16-01-2025

Volume 1, Issue 9

Sextortion Frauds

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked"

- Richard Clarke



Sextortion frauds are those type of frauds that can take place both against male and female victims (although majority of the victims are primarily females) and the perpetrator can be both an unknown person or a known one. In such crimes, the culprit usually entices and induces the victim to share their private and nude photographs or videos over phone, which are then stored and saved by the former for future extortion (sextortion).

In a lot of cases, people come in contact with unknown persons through dating apps or even matrimonial websites/apps. The profiles that they connect with, are mostly fake. The person behind the profile is actually a criminal whose main motive is to extort money from the victim. These fake profiles are deliberately made to look very attractive so that people fall prey to this scam easily. The persons who operate these fake profiles first talk to the victims normally for a few days and then induces them to share their intimate/nude pictures and videos with them. Once the criminal has access to these private pictures and/or videos, he starts extorting the sender for money, sometimes up to several lakhs claiming that in case the victim does not pay up, he will upload their pictures/videos on the internet or share those with his/her relatives, family and friends.

In a new variant of this Modus Operandi, a lot of people (mostly men) are being contacted on Instagram recently by women with attractive profiles, who immediately ask them for a sex chat or a nude video call. When the person agrees to it, they record the entire episode and start blackmailing/extorting the victim for money threatening to share the video with his relatives and friends.

This crime can also be committed by someone known to the victim and with whom the victim has had an intimate relationship. Sometimes, such people get access to or clandestinely obtain private pictures/videos of the victim and then, when the relationship ends, they use it to extort money from the victim.

Safety Precautions

1. Please remember – the internet never forgets or forgives. If you have shared something once, it will remain present on the Net forever, in one form or the other.

2. Secondly, the reach and speed of the internet is enormous. In a short span of time, the offensive content can spread to millions of people. Therefore, it is very important that under no circumstances, nothing that could, if leaked into the public domain, cause harm or embarrassment at a later stage, should be posted, shared, transmitted, recorded, etc.

3. During an online interaction or chat, if the person on the other side is trying to rush through the things and develop intimacy, then it is cause of alarm.

Spam Traps

A spam trap is an email address that's used to identify and monitor email spam. It's also a type of honeypot because it uses a fake email address to bait spammers. Internet service providers (ISPs), antispam organizations, blocklist providers and corporations use spam traps to monitor and reduce the amount of spam traffic to their networks.

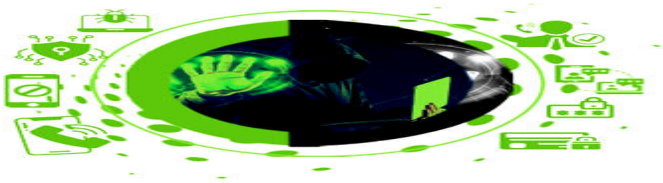
A spam trap uses filters to block certain email addresses that have a history of sending spam. The spam trap analyzes all or part of the email address to identify it and decide whether to mark it as a spam-sending address.

Despite their objective of blocking spam email addresses, spam traps can unintentionally block legitimate, nonspam email addresses as well, which can damage the sender's reputation and email deliverability. Spam traps can cause the sender's domain list or Internet Protocol (IP) address to be denied.

Spam Traps

Cybersecurity Tips & Best practices

- Keep software up-to-date.
- Avoid opening suspicious emails.
- Keep hardware up-to-date.
- Use a secure file-sharing solution to encrypt data.
- Use anti-virus and anti-malware.
- Use a VPN to privatize your connections.
- Check links before you click.
- Don't be lazy with your passwords!
- Disable Bluetooth when you don't need it.
- Enable two-factor authentication.
- Remove adware from your machines.
- Double check for HTTPS on websites.
- Don't store important information in non-secure places.
- Scan external storage devices for viruses.
- Avoid using public networks.
- Avoid the "secure enough" mentality.
- Invest in security upgrades.
- Backup important data.
- Train employees.
- Use HTTPS on your website.
- Employ a "White Hat" Hacker.



DIAL 1930
FOR ONLINE FINANCIAL FRAUD
REPORT ANY CYBERCRIME AT
WWW.CYBERCRIME.GOV.IN
FOLLOW CYBERDOST FOR UPDATES ON CYBER HYGIENE

Cybersecurity Digest

Bi-weekly update by the CISO Section of Meghalaya Rural Bank

Vol I Issue 10 **Date: 01-02-2025**

Layering - Money Laundering

Many forms of criminal activity generate significant amounts of money. To avoid attracting the attention of law enforcement, criminals must find a way to disguise the source of their ill-gotten funds. That's the goal of money laundering, which involves criminals engaging in a series of transactions to conceal the criminal origins of their money.

Money laundering involves three stages:

1. A criminal (or those under their direction) introduces funds earned through criminal activity to the financial system.
2. A money launderer (or the criminal themselves) engages in a series of transactions to create layers between the illegal source of the cash they control.
3. The criminal moves laundered money back into the financial system.

During the layering stage, the goal is to disconnect the money from the illegal activity that generated it. Generally, the more layers money passes through, the harder it becomes to connect the funds to criminal activity.

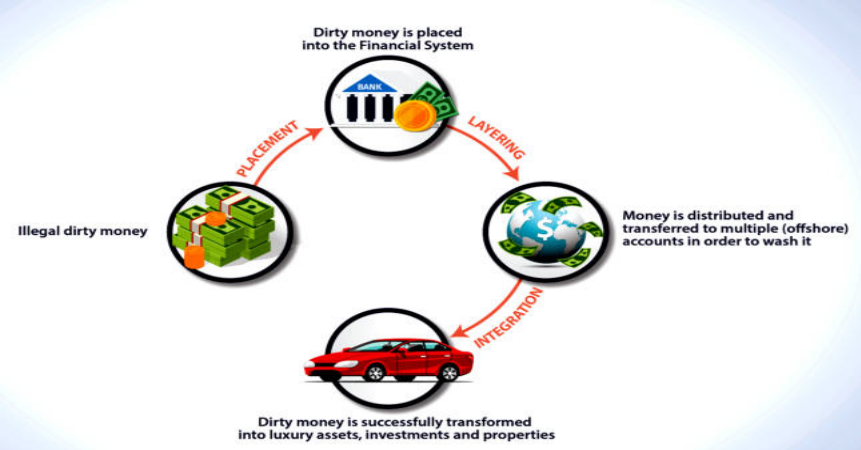
Layering can include changing the nature of the assets, i.e. cash, gold, casino chips, real-estate, and can also involve electronic transactions such as wires and ACHs, paper transactions, and/or manual movement of the funds between countries using covert means.

Challenges in detecting and combating layering in money laundering

The layering stage in money laundering is arguably the most crucial for the launderers. Illicit funds come out of the dark and blend with legitimate instruments. Launderers conclude these multiple transactions to confuse standard money laundering controls, which institutions primarily establish.

After separation from the original source, the crime proceeds enter into the financial system. The funds are dispersed and disguised to reduce the chances of suspicion or detection from law enforcement agencies. These funds are fragmented into smaller transactions and often transferred overseas to keep the money moving internationally, preventing the authorities from tracking the movement easily.

The possibility of transferring money electronically makes the cross-border movement of funds easy without inviting the attention of the authorities.



Smurfing

A Smurf is a money launderer who seeks to structure large transactions into smaller ones to avoid monetary thresholds requiring more scrutiny by banks and financial institutions. Smurfing is a layering technique wherein a Smurf resorts to structuring large amounts of cash into multiple small transactions and spreading them across many different accounts. Smurfing is a known money laundering technique adopted by criminals to circumvent the radar of regulatory authorities.

Red flags indicating layering in money laundering

Criminals across the globe use some common methods for layering a transaction. Some of the red flags indicating layering in money laundering are:

- Large number of fund transfers within a single bank
- Large number of transactions with rounded-off amounts
- Multiple fund deposits and immediate withdrawals
- Large number of wire transfers in quick succession
- Fund transfers from high-risk customers or high-risk geographies

Measures for Identifying and Preventing the Layering of Illegal Funds

Adequate Customer Due Process

- Robust KYC (Know Your Customer), involving identification and verification of the customer and the Ultimate Beneficial Ownership (UBOs).
- Screening the customers against the sanctions list
- Identifying the customer's relationship with Politically Exposed Persons (PEP) or nexus with any adverse media related to financial crime.
- Enhanced Due Diligence for customers identified as high-risk

Ongoing Transaction Monitoring

- Continuous transaction monitoring to detect and report suspicious patterns and red flags indicative of layering and money laundering activities..

Documenting the red flags

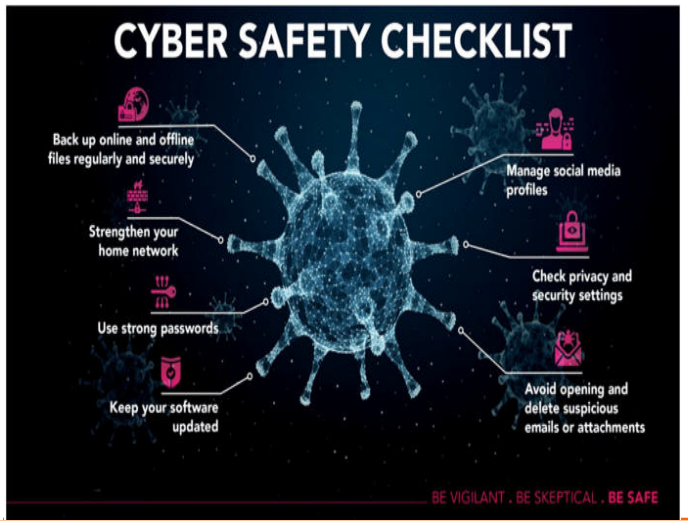
- Documentation and dissemination of identified risk indicators associated with the layering stage of money laundering to the team is crucial for awareness and necessary action..

Training the team

- It is essential to onboard teams from various business segments to create an unbreakable shield against layering activities. This is possible only when the team is adequately trained in detecting the risk indicators and applying necessary controls.

RBI Direction

In a move to combat financial fraud, the Reserve Bank of India (RBI) has mandated that banks and other regulated entities (REs) utilize the **'1600xx'** numbering series exclusively for transactional calls to customers. For promotional communications, the **'140xx' series** should be employed. This directive aims to enhance the security of digital transactions and protect customers from fraudulent activities.



Volume I Issue 11

Date : 16-02-2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Doxing—The Weaponisation of Personal Data

Online Doxxing

The word “doxing” (also spelled "doxxing") is derived from the term “dropping dox,” or “documents.” Doxing is a form of cyberbullying that uses sensitive or secret information, statements, or records for the harassment, exposure, financial harm, or other exploitation of targeted individuals.

This doxing meaning involves taking specific information about someone and then spreading it around the internet or via some other means of getting it out to the public. This practice has been fervent for many years, simply because documents contain permanent records of facts about people and things they have done and said, which can be powerful weapons against them. However, the term “doxing” first gained popularity in the 1990s when hackers began dropping docs on people who had been hiding behind fake names. In this way, hackers could expose other attackers with whom they had been in competition. Removing their anonymity left them exposed to authorities and others trying to track them down.

Doxing has taken a prominent role in modern culture wars, which involve people targeting those who support a cause or hold a belief that is in opposition to one they are trying to push forward

> Doxers can extract personal data from seemingly harmless social media posts
>
> : **Cybersecurity experts**

How does Doxing work?

Doxing is based on the fact that nearly everyone has data about them floating around on the internet, protected by varying levels of security—and in some cases, barely any at all. Once this data has been found, it is weaponized and used against the target.

People often use the same or similar usernames on different accounts for a variety of websites and web applications. It is relatively easy therefore for cyber criminals, activists, or others to use the usernames you have to pinpoint accounts that belong to you. Data from each of these accounts can be taken to compile a more thorough portfolio of documents that reveal information about you

What information are Doxers looking for?

1. **Phone numbers**: These can be used to contact the victim directly while pretending to be someone else and then asking questions to get more information. They can also be used to gain access to secure user accounts.
2. **Social security numbers**: A social security number is required to validate the identity of a person on a variety of websites and with a wide array of companies that hold private data.
3. **Home address**: Not only can a home address be used to verify someone's identity while trying to gain access to a private account, but it can also be used by an attacker to apply for new accounts while pretending to be the victim.
4. **Credit card details**: Credit card information can be weaponized for profit or to harm a victim's credit rating, as well as gain access to other sensitive information.
5. **Bank account details**: Because bank account details are typically only available after someone has satisfied security measures, they can be used to "verify" your identity for someone pretending to be you. They can also be levied to transfer money from your account to someone else's or published in a doxing attack to make the target more vulnerable.

How to protect against Doxing?

Secure Password Protection

Strong passwords are critical for protecting against doxing attacks. For optimal security, passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols with at least 8 characters in length. Using distinct passwords for each account is vital to ensure that if one password is exposed, other accounts remain secure.

Check out our blog post for password best practices.

Multifactor Authentication

Two-factor authentication (2FA) and multifactor authentication (MFA) add extra layers of security by requiring users to provide a username/password combination and another form of verification, such as a code sent via text message or email, before they can access their account. This makes it much more difficult for attackers to gain unauthorized access, even if they manage to get hold of someone's credentials through doxing or other means.

Limit Information Shared Online

Another way to protect yourself from doxers is by limiting the personal information you share online, particularly on public forums, social media sites, or discussion boards where people may search for targets using keywords related to location, job title, or interests. Be mindful when posting photos, too – avoid including details that could identify where you live or work unless absolutely necessary.

Not only is it essential to safeguard your information but also that of those around you. Friends and family members who might not understand how easy it can be for malicious actors to find their personal details should also be educated about good digital hygiene practices.

Doxing is scary because it involves exposure of potentially sensitive information to the public in a way that could damage the victim's reputation or expose them to theft or identity fraud. A doxing attack can also be used to blackmail the target or to embarrass someone's family or friends. Further, doxing can be a weapon for getting someone fired from a job due to things they have done that their employer disagrees with.

Volume 1, Issue 12 Date : 01-03-2025

CYBERSECURITY DIGEST

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Agentic AI: A Tipping Point Anticipated for 2025

While generative AI models like GPT-4 and Claude Sonnet 3.5 and artificial general intelligence have certainly transformed the way businesses interact with data and dominated headlines over the last two years; the new phrase on the lips of many players in the AI space is agentic AI — intelligent systems or so-called "agents" that don't just generate content but autonomously reason, adapt, and take action.

Non-Agentic rule based AI systems, while effective at automating routine tasks, are fundamentally limited by their rigid adherence to predefined rules. This constraint hinders its ability to adapt, learn, and make independent decisions. Hence, they have proven inadequate in addressing the dynamic needs of modern enterprises while Agentic AI promises to revolutionize enterprise operations by delivering end-to-end solutions that can autonomously achieve business objectives.

The landscape of AI is evolving rapidly, and Agentic AI architecture represents a transformative approach in the field of artificial intelligence. This paradigm shift enables the development and deployment of agentic AI systems capable of dynamic learning, decision-making, and interaction within complex environments. Agentic AI can optimize complex workflows, reduce operational costs, and respond more effectively to changing business needs. This adaptability drives higher productivity and enables organizations to stay competitive in an increasingly dynamic marketplace.

Understanding the Need for Agentic AI in Banking

Banking has remained a slow, tedious process that many customers find unconstructively engaging. With the advancement in the use of the internet and advancement in technology, specifically in the use of mobiles, banking has become online banking. Still, even such improvements have their drawbacks. Different consumers today hold very high expectations of organizations regarding efficiency and the time taken to respond, as well as customized services, which traditional systems can only but fail to address.

With the help of such means as developed algorithms and machine learning, Agentic AI contributes to the ability of banks to process information more effectively and quickly. It saves time by performing repetitive tasks and offers forecasts that banks can use to understand the customers' needs and market trends. This proactive strategy is essential in any organization despite the rapid changes in the industry.

How Does Agentic AI Transform Banking for Banks and Consumers?

For Banks

Efficiency: Agentic AI as a form of an agent significantly reduces the amount of time taken to accomplish ordinary processes, reduces expenses of running the operations, and provides high-quality work with minimal rates of error. Operations like data input, loan documentation, and transaction checks can be tended to by software so that the employees remain engaged only in more important activities.

Data Insights: AI agents use big data to offer strategic and tactical solutions, hence improving decisions made. In conclusion, assessment of prior results and present trends enables the right decisions to be made regarding product portfolios, pricing, and risk within the context of a bank.

Risk Management: Real-time fraud detection, monitoring of compliance and other aspects become possible, given that AI runs through the transactions in real-time. This capability increases the structured risk monitoring and management capability of the bank and will aid it in preventing circumstances that generate costly legal episodes and undesirable media exposure.

" No one can stop the progress of artificial intelligence ; it will inevitably be a central force in our future."

-Max Tegmark

For Consumers

Personalization: Agentic AI helps banks tailor their products and services to the needs and preferences of their customers. Through customer behavior observation of spending and financial needs, banks can suggest products that would meet every customer's need.

Accessibility: When customers engage in AI chatbots, they are constantly supported, and their problems are solved in due course. The readiness of such technologies always enables a customer to get the required support at a particular time and build confidence in their banking channel.

Speed: Non sunk costs are incurred once and there is always an improvement in the timely credit evaluation and other transactions which are advantageous for the customers. Agentic AI facilitates this as it performs credit assessments within instants and delivers funds transfers in as short a time as possible to meet society's dynamic nature.

Indian Cyber Crime Coordination Centre

सहवीर्यं करवावहै • Working Together With Vigour

Volume I Issue 13 Date: 16-03-2025

Cybersecurity Digest

Bi-weekly update by the CISO-Section of Meghalaya Rural Bank

Juice Jacking - The hidden danger

The term "juice jacking" was first coined in 2011 by investigative journalist Brian Krebs. It is a form of cyberattack where a public USB charging port is tampered with and infected using hardware and software changes to steal data or install malware on devices connected to it. The attack is used by hackers to steal users' passwords, credit card information, addresses, and other sensitive data stored on the targeted device.

Juice jacking attacks can take place in any public place with portable wall chargers, or public USB charging stations found in shopping malls, cafes, and hotels.

Juice jacking

How does juice jacking work?

To perform the attack, hackers infect USB ports or charging cables in public areas before the users connect to them. Most attacks target both Android and iOS mobile devices, with older devices being particularly vulnerable due to their outdated software. USB ports have multiple pins, but only one pin is used for charging while the other pins are used for data transfers. When users connect their devices to compromised USB ports, hackers use the connection to hack into mobile devices and steal personal data or deliver malware.

Types of Juice Jacking Attacks

Juice-jacking attacks can vary in their impact, even though the method remains the same. The different attack forms include data theft, malware installation, disabling attack, and multi-device attack.

In a data theft attack, hackers use juice-jacking to steal data from a device. The process is typically fully automated, and hackers often use crawlers to search the mobile device for personally identifiable information. Hackers may also use malicious apps to clone a device's data to another phone. However, cloning requires additional steps, such as a laptop as an intermediary to charge the targeted device.

In a malware attack, hackers use charging ports to install malware or viruses on connected devices, which are then used to perform ransomware, spyware, or trojan attacks.

Inside this Digest

Juice Jacking	1
How does juice jacking work	1
Types of Juice Jacking	1
PreventionTips	2
Cybersecurity News	2
Hackers can now access your bank	2

Juice Jacking– Prevention Tips

- **Avoid Public USB Ports:** Whenever possible, users should prioritize using a regular wall outlet with their own power adapter to charge their devices, eliminating the risk of data transfer or malware installation.
- **Carry a Power Bank:** Users can carry a portable power bank that they can keep charged beforehand, reducing their reliance on public charging stations.
- **Use a Charging-Only Cable:** Some companies sell special USB cables that only allow charging and block data transfer. While not foolproof, these cables can add a layer of protection.
- **Only Charge in Trusted Locations**: If users must use a public USB port, they should try to do so in a well-lit, populated area with security cameras.
- **Be Wary of Unfamiliar Ports**: Users should look for any signs of physical tampering with the charging port before plugging in their devices.
- **Monitor Your Device**: Users should stay vigilant while their device is charging and be mindful of any unusual activity or pop-up messages.

Cybersecurity News

A newly uncovered technique allows threat actors to bypass Microsoft Outlook's spam filtering mechanisms, enabling the delivery of malicious ISO files through seemingly benign email links.

This vulnerability exposes organizations to increased risks of phishing and malware attacks, particularly when combined with previously disclosed execution bypass methods.

Hackers can now access your bank account without OTP!!!

Cybercriminals have developed advanced methods to defraud individuals, bypassing the need for a One-Time Password (OTP) or ATM PIN. They are now leveraging deceptive messages containing fraudulent links that appear to be from legitimate banks. Once an unsuspecting recipient clicks on the link, their money is stolen without any OTP verification. The National Payments Corporation of India (NPCI) has issued a warning about a newly emerging scam involving call merging techniques, which fraudsters use to manipulate victims into unknowingly disclosing their OTPs, leading to financial fraud.

Scammers initiate a call, posing as a friend or acquaintance of the target. They claim to have obtained the victim's contact information through a mutual connection and request that they merge the call to include another individual. Unaware of the scam, the victim complies, inadvertently linking to a legitimate OTP verification call from their bank.

The fraudsters carefully time their calls so that when the victim receives an OTP, they assume it is related to the ongoing conversation and unwittingly share it. The criminals then use the OTP to authorize unauthorized transactions, resulting in financial losses for the victim.

CYBERSECURITY DIGEST

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

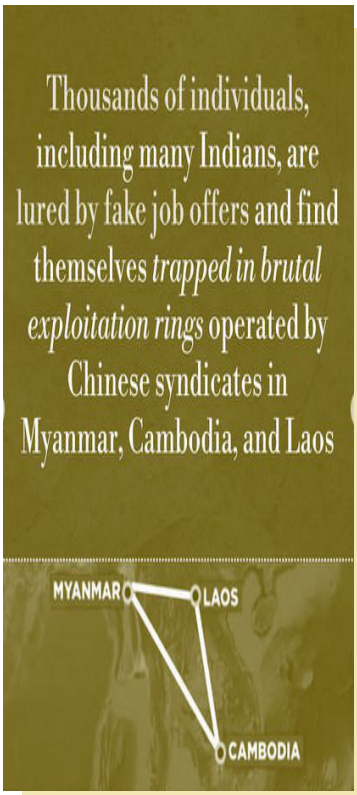
Volume 2 Issue 1 **Date: 01-04-2025**

'Cyber slavery': The new job con trapping Indian youth abroad

Cyber scams and fraud are on the rise in India. These scams typically involve spam calls, with the callers posing as government officials in an attempt to obtain Aadhar, ATM, and other sensitive information. To evade detection, these scammers now operate from foreign countries and even use Indian mobile numbers to make their calls appear genuine. This new approach has led to the emergence of a troubling phenomenon known as 'cyber slavery.'

As indicated by its name, cyber slavery is a modern form of exploitation in which individuals are unlawfully confined and forced into engaging in cyber scams. The individuals are lured to South East Asian nations under the pretence of securing high-paying data entry positions, only to be coerced into committing cyber fraud.

Upon arrival, their passports are confiscated, and they are coerced by fraudulent organisations to fabricate fake social media profiles featuring women in order to persuade individuals to invest in cryptocurrency apps or fraudulent investment schemes. Once the victims invest, all communication is abruptly terminated or blocked.



How were victims recruited?

Recruit through legal, primary job matching websites: Traffickers pretend to be regular companies (e.g. gaming companies) recruiting workers.

Recruit through private job matching groups on social media: Traffickers use Facebook groups and other social media to approach and lure victims.

Recruit through personal networks: Some victims reported that they were invited by their university or high school friends who were already working in Cambodia or Myanmar. Some victims also described that they were assigned to the 'human resource' department in the scamming compounds and were forced to lure 5 to 10 more victims to join the company.

Traffickers pose as potential clients to lure professionals: Traffickers pretend to be potential customers, inviting magicians, interior designers, and tour guides to visit Cambodia and provide services.

Traffickers kidnap victims on the street: Some victims were kidnapped during their visit to Cambodia and forced to work in the scamming compounds.

Indians trapped in Cyber slavery in South -East Asian region

How to identify red flags?

Red flags in job offers: Be wary of job offers that seem too good to be true, especially those offering high salaries for minimal qualifications.

Avoid upfront payments: Genuine employers do not demand large sums of money in advance as a "service charge" or recruitment fee.

Check for inconsistencies: Be cautious if recruiter uses unofficial email addresses, lacks professional communication or avoids face-to-face interactions.

Consult government resources: Use official government websites, embassies or official organisatons to verify job offers abroad.

"Serious and organised crime continues to threaten our security, our economic prosperity, and the safety of the public we serve"

How to avoid getting trapped?

Research extensively: Before applying for any overseas job, conduct thorough research into the company, recruiter and job offer to confirm their authenticity.

Stay in touch with family: Share your travel plans and contact details with family members when travelling aborad for work.

Keep records of communications: Save copies of emails, contacts and conversations with recruiters in case they are needed as evidence later.

Don't succumb to pressure: Be wary of recruiters who pressurize you into making quick decisions or paying large sums upfront.

Already Trapped? What steps can be taken

Contact authorities: Reach out to local law enforcement in the country where you are being held or contact your country's embassy for immediate help.

Find a safe way to communicate: If possible, use trusted individuals or fellow employees to help report your situation to authorities if your captors are monitoring your communication.

Avoid participating in illegal activities: If possible, avoid participating in cyber scams you are being forced into and try to delay or resist complying with your captors' demand.

Gather evidence of your captivity: Document as much information as possible about your captors, location and operations you are being forced into to assist law enforcement in rescuing you.

Seek help through international agencies: Contact organisations such as Interpol or NGOs that work to combat human trafficking.

Plan cautiously: Carefully plan any communication attempts to avoid further danger from your captors.

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 2

Date: 16-04-2025

ATM Jackpotting

ATM jackpotting is the exploitation of physical and software vulnerabilities in automated banking machines that result in the machines dispensing cash. These attacks can happen at any time and typically take very little time so culprits can quickly commit the crime.

ATM jackpotting uses the elements of both physical crime and cybercrime to get an ATM to dispense cash. The offenders use a portable device to physically connect to the ATM. This "rogue" device can be a laptop, a smartphone or a tablet PC. They also use malware to target the machine's cash dispenser and force it to dispense cash.

Furthermore, attackers will often use deception to limit risk, like dressing as service personnel to avoid scrutiny while selecting easier targets, such as ATMs in isolated locations or unprotected by human security guards.

ATM jackpotting

With physical access to a machine, ATM jackpotting enables the theft of the machine's cash reserves, which are not tied to the balance of any one bank account. Successful thieves who remain undetected can potentially walk away with all the cash that was stored in the machine at that time.

Malware used in ATM jackpotting

Two of the most commonly used ATM malware families are Ploutus and Anunak.

Discovered in the wild in 2013, Ploutus enables criminals and money mules to bypass an ATM's security measures and physically control it in order to steal its money. That can be accomplished in just a few minutes either by attaching an external keyboard to the machine or remotely via SMS messaging. Because Ploutus can be remotely controlled after its installation on the ATM's internal computer, criminals can use it to steal cash at will. Moreover, the malware can operate undetected so that it can persist in the system and potentially cause significant losses for banks and their customers.

Anunak malware, also known as Carbanak malware, is a backdoor based on Carberp malware that allows attackers to remotely control the infected ATM and cash out large amounts of money at will. The malware includes capabilities like key logging and desktop video capture that allow them to steal both ATM data and cash. Carbanak is also used for espionage

Is a fun, stylized image worth risking our privacy forever?

The latest Internet fad is turning photos into Ghibli-style art. Popularised by GPT4, the photo trend has taken over the world, and social media is flooded with remakes of photos in the trademark, dreamy Ghibli aesthetic. However, while millions eagerly upload their photos to AI-powered apps for a fun transformation, cybersecurity experts warn that the risks far outweigh the rewards.

The seemingly harmless act of sharing personal images online could expose users to privacy breaches, deepfake manipulation, and even long-term surveillance by AI companies. The far-reaching consequences of it range from harmful to dangerous.

Targets and outcomes of ATM jackpotting

Standalone ATMs, such as those in retail premises like malls and service outlets, are the more likely targets of ATM jackpotting attacks because they are away from the tighter monitoring and security controls of a bank's premises. ATMs that receive less foot traffic are also more vulnerable than ATMs in busier locations.

The security controls of older machines might not be fully up to date, which makes them common targets for ATM jackpotters. That said, any ATM can become the target of an ATM jackpotting attack, so all ATM owners should be cognizant of the risk and apply adequate controls to prevent incidents.

In addition to stealing cash from the target, attackers can also install malware on it or replace its hard drive. They can also reboot the ATM, making it temporarily unavailable and causing access problems for the ATM's customers

Strategies to prevent ATM jackpotting attacks

ATM monitoring is the most basic security control that all banks should implement to prevent jackpotting attacks. Routine monitoring can help to identify suspicious activities like multiple failed login attempts that might indicate a criminal trying to launch a jackpotting attack.

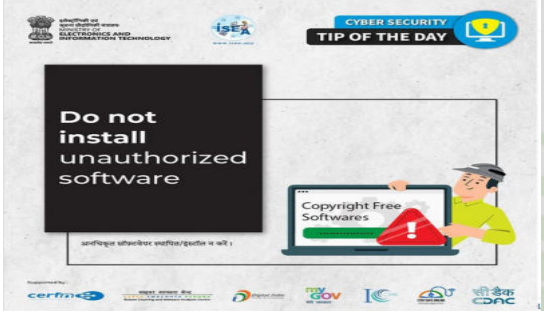
It's also important to regularly update the ATM with all required security patches and software upgrades. In addition, updated security software, such as firewalls, antivirus software and antimalware should also be installed to protect the machine.

Another strategy is to disable the ATM's auto-start and auto-boot functions. Attackers often take advantage of these functions to compromise ATMs, so disabling them closes at least one door on this type of crime.

Electronic surveillance systems are another crucial security measure for ATMs. While human security guards are also important, they cannot monitor the location 24/7. They are also prone to human weaknesses like fatigue and sleepiness that affect their ability to remain alert to potential attacks. Moreover, they might not be trained to detect and mitigate jackpotting attacks. Video cameras, motion sensors, intruder alarms and access controls help to plug these gaps and provide more reliable 24/7 surveillance of ATMs, allowing banks to detect and in many cases, prevent, ATM jackpotting attacks.

Cybersecurity Awareness on AI Creativity

- Always read the privacy policy before uploading your data.
- Use trusted platforms with clear data usage policies.
- Avoid sharing sensitive images that could be misused.



Volume 2 Issue 3 Date: 01-05-2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Lottery Fraud

Fake lottery scams are a pervasive form of fraud that prey on people's hopes and dreams of instant wealth. These scams often arrive through unsolicited emails, phone calls, or letters, claiming you've won a large prize in a lottery or sweepstakes you never entered. While the promise of easy money can be tempting, falling for these lottery scams can lead to significant financial losses, identity theft, and emotional distress.

A lottery scam is a type of fraud where scammers falsely notify individuals that they've won a substantial prize in a lottery or sweepstakes, even though they never entered or purchased a ticket. The scammer's goal is to trick the victim into sending money or personal information under the guise of claiming their supposed winnings.

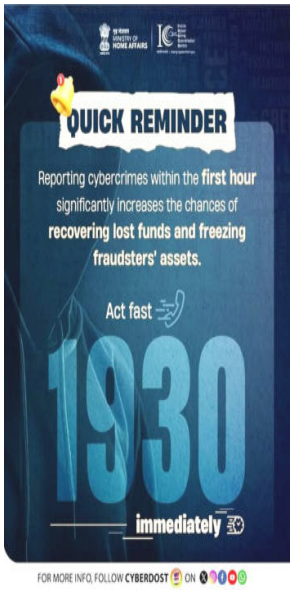
These scams often use the names of legitimate lotteries or well-known organizations to appear credible. They may claim you've won a foreign lottery, a government grant, or a prize from a major company. The scammer will typically demand upfront payment for taxes, processing fees, or other charges before releasing your "winnings." In reality, there is no prize, and any money sent is lost to the fraudsters.

Common Tactics Used in Fake Lottery Scams

Lottery fraudsters employ various tactics to make their scams seem believable and entice victims to part with their money or personal data. Some common methods include:

1. **Unsolicited contact:** Scammers reach out via email, phone, text, or mail, claiming you've won a prize in a **lottery** or sweepstakes you never entered.
2. **High-pressure tactics:** They create a false sense of urgency, insisting you must act quickly to claim your winnings or risk forfeiting the prize.
3. **Requests for personal information:** Scammers ask for sensitive data like bank account numbers, credit card details, or copies of identity documents to steal your money or commit identity theft.
4. **Demand for upfront payment:** They require you to pay taxes, processing fees, or other charges in advance, often via wire transfer or gift cards, to receive your supposed winnings.
5. **Inconsistent or vague details:** Information about the lottery, prize amount, or company is unclear, changes, or lacks specifics that could be verified.
6. **Unprofessional communication:** Messages contain poor grammar, misspellings, generic greetings, or lack official contact information.
7. **Fake checks or websites:** Scammers may send counterfeit checks that initially appear to clear but are later rejected, or direct you to fraudulent websites that mimic legitimate ones.

Key Signs of a Fake Lottery Scam



To protect yourself from fake lottery scams, watch out for these telltale signs:

- **Unsolicited notification:** Legitimate lotteries do not contact winners who haven't bought a ticket
- **Pressure to act immediately:** Real lotteries give ample time to claim prizes without rushing you
- **Upfront payment demanded:** Authentic lotteries never require winners to pay fees or taxes in advance
- **Personal data requested:** Scammers use your sensitive information to steal money or commit identity theft
- **Inconsistent information**: Details about the lottery, prize, or company are vague or change
- **Unprofessional messages:** Communications have poor grammar, misspellings, or lack official contact information
- **You didn't buy a ticket:** It's impossible to win a real lottery without purchasing a ticket

How to Protect Yourself from Fake Lottery Scams

To avoid falling prey to fake lottery scams, follow these proactive measures:

- Be cautious of unsolicited notifications claiming you've won a prize, especially if you haven't entered a lottery or sweepstakes.
- Never pay upfront fees, taxes, or charges to claim lottery winnings. Legitimate lotteries deduct taxes before paying out prizes.
- Protect your personal information. Don't give sensitive data like bank details, credit card numbers, or identity documents to unverified individuals or organizations.
- Verify suspicious win notices by directly contacting the official lottery or sweepstakes company through their verified website or customer service channels.
- Read the fine print and research the legitimacy of any lottery or sweepstakes before entering or making purchases.
- Be wary of lottery sweepstakes or prize offers that seem too good to be true. Genuine lotteries don't require you to pay to play or win.
- Stay informed about the latest lottery scam tactics and common red flags. Awareness is key to recognizing and avoiding these fraudulent schemes.

Protect Yourself From Lottery Frauds

Fake lotteries and sweepstakes scams continue to deceive countless individuals worldwide, exploiting their dreams of easy riches. By learning to recognize the common signs of these fraudulent schemes, such as unsolicited win notifications, demands for upfront payment, and requests for personal information, you can protect yourself from falling victim to lottery fraud.

Remember, legitimate lotteries never require winners to pay fees or taxes in advance or share sensitive data to claim a prize. If you suspect a lottery scam, cut off contact with the scammer immediately and report the incident to the proper authorities. Stay informed, trust your instincts, and prioritize your financial and personal security. By remaining vigilant against lottery fraudsters and their tactics, you can avoid the devastating consequences of falling for a fake lottery or sweepstakes scam.

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 2, Issue 4

Date: 15.05.2025

Gift Card Fraud

Gift cards have become a popular gifting option, as they save people from the hassle of choosing gifts and allow recipients to purchase items of their choice. The gift card market has seen a steady growth over the years due to the growth of e-commerce as well as greater adoption by corporations that present gift cards as recognition to their employees. Gift cards provide retailers with a promising business stream that enables them to increase revenue and retain customers.

But there's a dark side to this phenomenon. Because they are fungible and difficult to track, gift cards provide thieves with quick money and generally easy getaways. In addition, the global market is poised for growth at an estimated CAGR of 6.9% over the next four years, expected to reach over $668 billion by 2027[1]. This has made it a lucrative target for cyberattack, resulting in the rising instances of gift card fraud.

Gift Card Scam

Gift card fraud refers to using gift cards to commit dishonest activity. Bad actors exploit both gift cards and prepaid cards because they can be easily manipulated. It can happen offline – for instance, when scammers steal gift card numbers from stores – but increasingly it is becoming a digital business. Cybercriminals use botnets to perform brute force attacks on gift card websites by testing thousands of card numbers and PIN combinations per minute. They also use bots, sweatshops, or click farms to continually check the card balances and redeem them. They hack into a user account and abuse the auto-load feature to drain the account of the funds.

Once these attackers are successful in their account takeover attempts, they can redeem the credit card points by requesting for a gift card and escaping with the money undetected. This is because gift cards do not require the kind of authentication that a credit card or a bank account would.

How Gift Card Fraud is monetized

The simplest way to illegally monetize gift cards is to resell them on third-party websites. But there are plenty of other ways criminals make money from gift card fraud. Some malicious actors sell them on the dark web. Then there are websites that offer conversion facilities - gift card to cash - at a fee of about 30-40% of the card value. Similarly, there are physical kiosks where users can convert gift cards into cash.

Cybercriminals also post fake ads of fictitious items on ecommerce websites and offer heavy discounts on these expensive but non-existent items. Using social engineering, they trick users into sharing gift card numbers instead of using credit cards for payments. On receiving the money, the thief and the ads simply vanish.

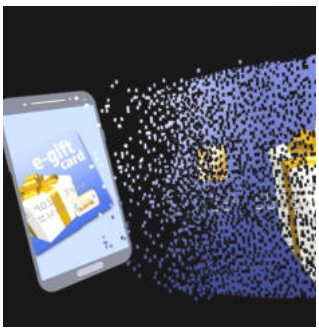
Cyberattackers use account takeover attacks to access users' credit cards or loyalty reward points and redeem these points for gift cards, which can easily be exchanged for cash. Unlike credit cards and bank accounts, consumers are not too active when it comes to monitoring their reward points. This provides attackers with a freeway to the unused points sitting ripe for abuse. Attackers are also increasingly using gift cards as a means for money laundering and moving illegal funds because of the ease and anonymity that gift cards offer.

Buying and Using Gift Cards

Gift cards are for gifts. Only gifts. Not for payments. Never buy a gift card because someone tells you to buy one and give them the numbers. Whenever you buy gift cards:

Stick to stores you know and trust. Avoid buying from online auction sites because the gift cards may be fake or stolen.

Inspect the gift card before you buy it. Make sure the protective stickers are on the card and that it doesn't look like someone tampered with them. Also check that the PIN number on the back isn't showing. Pick a different gift card if you spot a problem and show the tampered card to a cashier or manager.



Always keep a copy of the gift card and store receipt. Take a picture of the gift card and store receipt with your phone. The number on the gift card and store receipt will help you file a report with the gift card company if you lose the gift card or if you need to report fraud.

Don't give scammers a Gift

Computer Security Practices to avoid Phishing Attack

- Don't email personal or financial information. Email is not a secure method of transmitting personal information.
- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.
- The best policy is to refrain from downloading files or clicking through links in a strange email, unless you trust the source. Malware, viruses, and other types of malicious material can be easily downloaded to your server or computer through attachments or malicious links

How to be cyber vigilant

Keep softwares and operating systems updated.

Use antivirus software for your devices.

Set your social networking profiles to private.

Use and enter only secure websites.

Use strong passwords for all your accounts.

Do not open attachments in spam emails.

Do not give bank account details to unknown people.

Be alert while using public wifi hotspots.

Volume 2 Issue 5

Date: 01.06.2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Threat:

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Examples of threats include computer viruses, Denial of Service (DoS) attacks, data breaches, etc.

Vulnerability:

In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals. In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Risk:

Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat.

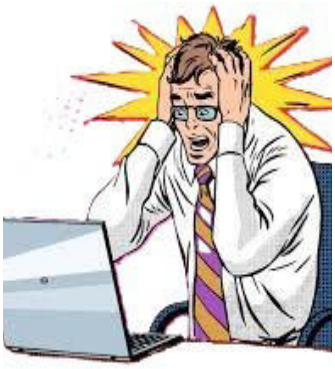
Human Cyber Risk– The First Line of Defence

Humans are often regarded as the weakest link in a cybersecurity program. Whether resulting from manipulative cybersecurity tactics or limited cybersecurity awareness, human errors remain the most prevalent attack vectors in every information security program, no matter how sophisticated your cybersecurity stack may be.

Human cyber risk refers to potential human behaviors that could result in a cyber incident. These could include clicking on malicious phishing email links or providing sensitive internal information to unauthorized persons.

In cybersecurity, a human vulnerability is any area of weakness that could result in a security breach. Unlike digital cyber threats, which could be exploited programmatically by reverse engineering software flaws, human vulnerabilities are exploited by manipulating human behavior.

The human element is complex, and not all individuals share the same vulnerabilities—some are more susceptible to a phishing attack than others. An experienced cybercriminal determines each person's unique area of weakness and devises a plan to exploit that weakness to advance their cybercrime objectives.



Human risk factors in Cybersecurity

Human risks are predominantly concentrated at the IT security boundary, at the interface of cybercriminals, and in an organization's private network. This is why human errors usually facilitate initial network access to unauthorized users. Cybercriminals aim to exploit this gateway, and they have cultivated their tactics to exploit the human factors of cybersecurity with the following types of attacks:

Phishing email attacks: When hackers send emails containing links infected with credential-stealing malware to employees to gain access to the corporate network.

Social engineering attacks: When hackers try to trick employees into exposing sensitive internal information, either via a phone, in-person conversation, or an internal messaging tool, such as Slack.

Poor Cyber Hygiene Actions

Even without prompting from hackers, human errors can permeate the information technology boundary with the following poor cyber hygiene actions:

- **Shadow IT practices:** When applications and external hardware are connected to corporate networks and devices without first being approved by the IT department. Such practices create attack surface bloats security teams are unaware of, making these regions of the digital surface perpetualy vulnerable to cybercriminal compromise.
- **Accidental data sharing:** Sending sensitive internal information, such as customer data, to the wrong email address.
- **Neglecting Multi-Factor Authentication (MFA):** Failing to set up MFA for critical business accounts.
- **Ignoring security warnings:** Bypassing browser security alerts (e.g., ignoring "*This connection is not secure*" warnings) or disabling antivirus software to remove interruptions associated with a desired action.
- **Delayed software updates:** Postponing or ignoring prompts for system and software updates.
- **Insider threats:** When an employee abuses their internal credentials to access sensitive internal information that is then leaked outside of the corporate network.
- **Neglecting secure communication protocols:** Discussing confidential business matters over unsecured or public channels, such as personal email accounts, messaging apps, or during in-person interactions.
- **Inadvertent social media disclosures:** Employees sharing too much information about their workplace position and activities, such as company projects or upcoming corporate travel plans, could arm hackers with enough intelligence to launch a targeted phishing attack.

Best practices for reducing Cyber Human Risk

Personalised, role-specific training: Training isn't a one-size-fits-all solution. Make sure content is being adapted to each employee's role, location and cyber knowledge level..

Leadership commitment: Ensure that leadership demonstrates a commitment to cybersecurity, setting an example for the rest of the organization.

Open communication: Encourage open communication about security issues and make it easy for employees to report suspicious activities without fear of repercussions.

Recognition and rewards: Recognize and reward employees who demonstrate positive security practices.

Incident response plans: Develop and regularly update incident response plans to ensure a swift and effective response to security incidents.

Regular software updates: Ensure all software and systems are regularly updated and patched to protect against known vulnerabilities.

Secure browsing practices: Educate employees about secure browsing habits and the risks of downloading software from untrusted sources.

Physical security: Emphasize the importance of physical security measures, such as locking screens when away from desks and securing sensitive documents.

Multi-factor authentication (MFA): Require MFA for accessing sensitive systems and data to add an extra layer of security.

Cyberattack via Picture? No OTP, No Link—Hackers Just Need One WhatsApp Image Now

In the digital age where phishing links and OTP frauds are the usual suspects, a new threat has emerged—one that hides in plain sight. Hackers are now using WhatsApp images as Trojan horses to deliver malware directly into users' devices. Unlike conventional scams, this technique relies on steganography, a method where malicious code is embedded within seemingly harmless image files.

Once the infected image is opened, the malware installs silently on the victim's phone. From there, it can siphon sensitive data—banking credentials, one-time passwords, and even carry out unauthorized financial transactions—without the user's knowledge.

Cybersecurity Digest

Bi-Weekly Digest by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 6 **Date: 16-06-2025**

SIM Swapping Fraud

Unauthorized SIM changes, sometimes called SIM swapping or SIM hijacking attacks, occur when a customer's phone number is transferred to a different SIM card or eSIM profile under the control of a criminal. If the SIM swap is successful, the criminal may intercept the customer's phone calls and text messages to receive one-time security codes from social media, banks, credit card companies, cryptocurrency exchanges, and other financial institutions, allowing them to potentially access those accounts and cause financial and reputational harm to the customer.

But, not all SIM changes are bad! Authorized SIM swaps may happen when you upgrade your device, or when you troubleshoot or replace a lost or stolen device.

Criminals typically use SIM swaps as a way to steal your phone number so they can access your bank or other financial accounts. They often start by gathering as much personal information about you as they can from social media, the Internet, the dark web, previously compromised accounts, and directly through phishing. They use this information to pretend they are you, in an effort to gain access to your account and transfer your mobile number to a different SIM card or eSIM under their control. Once they've "swapped" your SIM, calls and texts to your phone number route to the phone in the criminal's control. At that point, the criminals can use their phone to receive one-time security codes or calls that banks and other companies use to safeguard customer accounts. In some cases, you might not know this has even happened until your phone no longer works.

SIM Swap Scam—Causes

Understanding the underlying causes of SIM swap scams is crucial for identifying vulnerabilities and implementing effective preventive measures. Following are the causes of SIM swap scam:

Social engineering: Scammers use various techniques to deceive victims and mobile carrier employees into believing they are the legitimate owner of the phone number. This can involve phishing emails, calls, or text messages to collect personal information.

Data breaches: Large-scale data breaches can provide scammers with the necessary information to impersonate victims This data can include names, addresses, social security numbers, and phone numbers.

Insider threats: In some cases, scammers may bribe or coerce employees within mobile carrier companies to facilitate the SIM Swap.

Weak security practices: Mobile carriers sometimes have insufficient security protocols for verifying identity before transferring a number to a new SIM, making it easier for scammers to execute their schemes.

Signs you might be a victim of a SIM swap scam

- **Sudden loss of service:** If your phone suddenly loses service and displays " No Service" or "Emergency Calls Only", it could be a sign that your number has been transferred to another SIM.
- **Inability to make calls or send texts**: If you can no longer make calls or send texts, it might indicate that your SIM card has been deactivated.
- **Unusual account activity:** You might receive notifications of unusual login attempts or password changes from your email, bank, or social media accounts.
- **Receiving messages about SIM card changes**: If you receive notifications from your mobile carrier about SIM card changes that you did not initiate, this is a red flag.
- **Access denied to accounts:** If you are suddenly unable to access your bank accounts, email, or social media accounts despite entering the correct passwords, it could be a result of a SIM Swap.

How to protect yourself from SIM Swap Scams

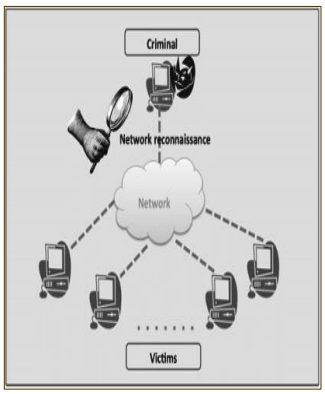
Protecting yourself from SIM Swap scams involves strengthening account security, limiting the sharing of personal information, and staying vigilant for suspicious activities. We can reduce the risk of falling victim to this form of identity theft by taking the following proactive measures:

- **Enhance account security**: Use strong, unique passwords for all online accounts and change them regularly. Avoid using easily guessable information such as birthdays or common words.
- **Enable two-factor authentication (2FA):** Use 2FA methods that do not rely on SMS-based codes. Consider using the authenticator apps or hardware tokens instead.
- **Be wary of phishing attempts**: Do not click on links or download attachments from unknown or suspicious emails and messages. Verify the sender's identity before responding.
- **Monitor your accounts**: Regularly check your bank, email, and social media accounts for any suspicious activity. Set up alerts to notify you of any unauthorized transactions or changes.
- **Contact your mobile carrier:** Ask your mobile carrier to add a PIN or password to your account for an extra layer of security. Some carriers also offer the option to disable remote SIM swapping entirely.
- **Use identity protection services:** Consider using identity theft protection services that monitor your personal information and alert you to potential threat.
- **Report suspicious activity**: If you suspect you are a victim of a SIM swap scam, contact your mobile carrier immediately to restore your service and secure your accounts. Additionally, report the incident to your bank and other relevant institutions.

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 7 **Date: 01-07-2025**



Reconnaissance

Reconnaissance is the preliminary phase of a cyber attack. It involves the systematic surveying or scanning of systems, networks, or web applications to gather information about potential vulnerabilities that can be exploited.

The term 'reconnaissance' originates from military operations, where it refers to the exploratory surveying or spying conducted to gain information about an enemy. In the cyber realm, it carries a similar meaning. Cybersecurity reconnaissance involves cybercriminals gathering data about a target system's vulnerabilities, which can then be exploited in a subsequent attack.

How Do Reconnaissance Attacks Work?

1. Collect data about the target: This can involve a range of activities, from searching publicly available information (like corporate websites or social media platforms) to monitoring network traffic for valuable data.

Cybercriminals aim to gather as much information as possible at this stage. This could include details about the target's network infrastructure, systems, and software, as well as potential vulnerabilities that could be exploited.

2. Identify the scope of the target network: Once the hacker has gathered enough data, the next step is to define the target network's scope. This involves identifying the IP addresses associated with the target and mapping out the network's structure.

By understanding the target network's range, hackers can identify potential points of entry and plan their attack more effectively. This step often involves techniques like IP scanning and port scanning.

3. Identify active tools: The final step in the reconnaissance process is identifying the active tools within the target's system. These could include firewalls, intrusion detection systems (IDS), or other security measures that could potentially thwart an attack.

By identifying these active tools, hackers can plan their attack to avoid detection and increase their chances of success. This step often involves complex technical methods and requires a high level of expertise.

4. Locate open ports and access points: Just as a traditional burglar might look for unlocked doors or windows, a cyber attacker will search for open ports in a network that can be used as entry points.

These open ports and access points might be the result of improper network configuration, forgotten backdoors from previous IT work, or simply default settings that have never been changed. The process of finding these vulnerabilities can be done manually, but often automated tools are used to speed up the process and avoid detection.

5. Identify services on the ports: Once an attacker has identified open ports and access points, the next step is to determine what services are running on those ports. This is similar to a thief figuring out what's behind each door in a house. For example, a port might be running an outdated version of a service with known vulnerabilities, providing an easy entry point for an attacker.

In most cases, cyber attackers use automated scanning tools to identify what services are running on open ports. These tools can quickly catalog the services running on each port and can even identify the version of the software being used. This information is then used to plan and execute subsequent attacks.

6. Map the network: The final step in the reconnaissance process is mapping the network. This involves creating a visual representation of the target's network, including the location and connection of all devices, servers, routers, and other network components.

Mapping a network gives the attacker a clear understanding of the target's system architecture. It reveals the most valuable assets, their locations, and the paths to reach them. Such information is crucial for strategizing an attack. For instance, an attacker might target a server containing sensitive data, or a router that controls access to several parts of the network.

How Businesses Can Protect Themselves From Reconnaissance Attacks

Network Monitoring

One of the most effective ways to protect against reconnaissance attacks is through network monitoring. This involves regularly checking and analyzing network traffic to identify any suspicious activity.

Network monitoring can help detect reconnaissance activities such as port scanning or network mapping. By catching these early signs, businesses can take preventive measures before an actual attack takes place.

Honepots

Honeypots are decoy systems or data set up to attract cyber attackers. These traps are designed to mimic real systems that appear vulnerable and appealing to attackers, diverting them from valuable assets and gathering information about their methods and tactics.

By engaging attackers with honeypots, businesses can analyze attack patterns and techniques without risking their actual data or systems. This insight allows organizations to improve their security measures and prepare for real threats. When implemented effectively, honeypots serve as both a diagnostic tool, which can capture reconnaissance attempts, and also a deterrent that adds an extra defensive layer.

Firewalls and Access Controls

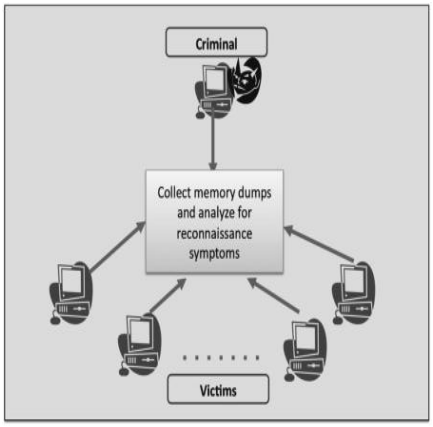
Firewalls and access controls are another essential part of a business's cybersecurity strategy. Firewalls serve as a gatekeeper, controlling which traffic is allowed in and out of a network.

Access controls, on the other hand, manage who has access to what within a network. These controls can prevent unauthorized access to sensitive areas of the network, thereby limiting the damage a potential attacker could do.

Patch Management

Patch management is a critical security measure that involves regularly updating software and systems to fix vulnerabilities that could be exploited by attackers. In the context of reconnaissance attacks, patch management plays a vital role in closing the gaps that attackers seek to exploit.

A robust patch management strategy ensures that all software, including operating systems, applications, and network tools, are up-to-date with the



latest security patches. This process involves regularly scanning systems for missing updates, testing and applying patches in a timely manner, and verifying that the patches have been installed correctly. Effective patch management not only reduces the risk of reconnaissance attacks but also strengthens the overall security posture.

Data Encryption and Privacy Measures

Data encryption and privacy measures are essential in safeguarding sensitive information from unauthorized access during a reconnaissance attack. Encryption involves transforming data into a coded format that is unreadable without the proper decryption key, ensuring that even if data is intercepted or accessed, it remains protected.

Implementing strong encryption protocols for both data at rest (stored data) and data in transit (data being transmitted over a network) is crucial. Additionally, privacy measures such as access controls and data masking can limit the exposure of sensitive data.

Threat Intelligence

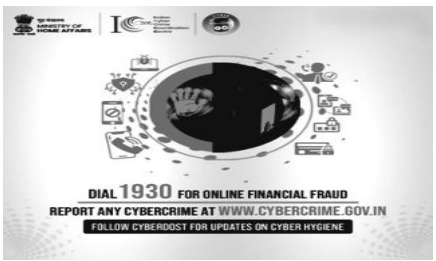
Threat intelligence is a proactive approach that helps organizations stay ahead of potential reconnaissance attacks by identifying emerging threats and vulnerabilities.

Threat intelligence includes gathering and analyzing data from various sources, including threat feeds, hacker forums, and dark web monitoring. By understanding the tactics, techniques, and procedures (TTPs) used by attackers, businesses can develop targeted defenses against reconnaissance and other cyber threats.

Security Awareness Training

Security awareness training is crucial in educating employees about the risks and signs of reconnaissance attacks. Since human error is often a significant factor in security breaches, equipping staff with the knowledge and skills to identify suspicious activities can greatly enhance an organization's defense.

Training should cover topics such as identifying phishing attempts, safe browsing practices, and the importance of strong passwords. Regular updates and drills can help keep security at the forefront of employees' minds. An informed and vigilant workforce is a formidable first line of defense against cyber threats, including reconnaissance attacks.



Volume 2 Issue 8

Date: 16.07.2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Cybersecurity is a constant evolutionary arms race

As long as humans continue connecting to the internet, they create security risks

In a rapidly changing landscape like cybersecurity, no one can claim to know everything all the time

Inside this Digest:

Quid Pro Attacks	1
Anatomy of a Quid Pro Attack	1
Recognizing Quid Pro Attacks	1
Why we fall for Quid Pro Quo Scams	2
Fortifying against Quid Pro Quo Attacks	2

Quid Pro Quo Attacks

Quid pro quo attacks fall under the umbrella of social engineering frauds, where the attacker offers a service or benefit in return for information or access. Imagine someone posing as a tech-support agent offering to speed up your computer. They seem reliable and say all the right things to make you believe you need their services. In fact, they really help you speed up your computer, and you believe you received your side of the bargain. However, what if, in the process of speeding up your computer, they gain access to your sensitive files and steal your info? This is the deceptive give-and-take at the heart of quid pro quo attacks.

Anatomy of a quid pro quo attack

Recognizing quid pro quo attacks

While distinguishing a quid pro quo attack from a genuine offer for products or services can be challenging, some signs help you detect a quid pro quo attempt. If you notice any of the following, approach them with caution and reach out for help if needed:

Unsolicited offers or requests: One sign of a quid pro quo scam is the unsolicited nature of the offer or request. Remember that employers don't typically reach out to individuals with job offers out of the blue, and legitimate tech support doesn't magically appear at your doorstep. Similarly, valid medical solutions don't manifest without prior inquiry.

High-pressure tactics: Scammers are masters at creating a sense of urgency to make you act hastily without thorough consideration. You might encounter phrases like "This offer won't last long," "Other buyers are waiting to cash in," "Many candidates have already applied," or "We only have a limited number of positions available."

Requests for personal or financial information: Since quid pro quo scams often appear to involve a fair exchange, requests for personal information can appear discreet and necessary. Watch out for demands that deviate from the ordinary, such as requests for your social security number or bank details. Legitimate transactions rarely require such sensitive information upfront.

Unclear or unrealistic promises: The age-old adage "if it seems too good to be true, it probably is" applies perfectly to quid pro quo scams. Whether it's a miracle cure, a get-rich-quick scheme, or a job that promises substantial returns with minimal effort, these unrealistic offers should trigger your skepticism. They are often traps designed to deceive you into providing fraudsters with information or money.

Suspicious payment requests: Financial matters should be transparent and reasonable. If a potential service provider suddenly requests payment for services, training, or equipment you haven't requested or they haven't provided, it should raise a red flag. Be careful with unspecified and unexplained payment requests and ensure that such transactions have been previously authorized.

The human element: Why we fall for quid pro quo scams

The success of quid pro quo attacks is mainly due to psychological manipulation techniques that are used by attackers. By offering to do a favor or help, attackers create a sense of indebtedness in the target, making them more likely to comply with their requests. This is further reinforced by the principle of reciprocity, which is deeply ingrained in human behaviour.

In these scams, attackers often impersonate trusted authority figures or experts, making it easier for them to gain the trust of their targets. This can be in the form of impersonating, for example, an IT support person or a customer service representative. Individuals are more likely to trust and comply with the requests of someone they perceive as an authority figure.

In addition, attackers may also create a sense of urgency in their targets by using tactics like time-sensitive offers or threats. This can make the target feel stressed and act quickly without thinking things through, making them more vulnerable to falling for the scam

Digital hygiene: Fortifying against quid pro quo attacks

While there is no guarantee against quid pro quo attacks, chances are you are more likely to detect and not act upon them if you apply a set of security best practices. Here are some things to improve your digital hygiene and help you to recognise and deter quid pro quo attacks:

Employee training: Educate your staff about the dangers of quid pro quo attacks and provide clear guidelines for identifying and responding to potential threats. Regular and continuous training sessions can reinforce their awareness and vigilance

Robust authentication: Implement strong authentication measures to verify the identity of individuals requesting sensitive information or access. This can include multi-factor authentication (MFA) and verification procedures

Comprehensive security policies: Develop and enforce comprehensive security policies that outline how sensitive data should be handled, shared, and protected. Ensure your employees are aware of and follow these policies

Incident response plan: Prepare for the worst by creating an incident response plan that outlines the steps to take in the event of a security breach. Timely action can minimize the damage caused by an attack.

Regular monitoring and assessment: Continuously monitor and assess your organisation's digital security posture. Regular security audits can help identify vulnerabilities and areas for improvement.

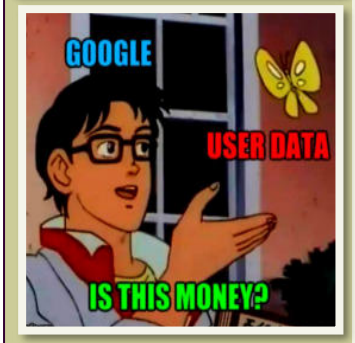
Volume 2 Issue 9

Date: 01-08-2025

Cybersecurity Digest

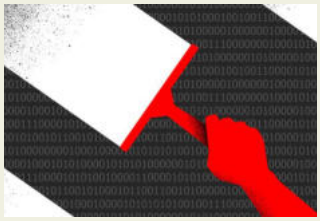
Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Wiper Attacks



Cyber threats are evolving at a very high pace in today's digital landscape which keeps organizations vigilant and proactive. In such threats, wiper attacks stand out as one insidious form of cybercrime. They specialize in wiping out data and disrupting operations. While its variants tend to bank on financial gains through encrypted hostage data, the purpose of wiper attacks is to destroy valuable information irretrievably. This destructive intent can cause significant damage to the concerned organizations, leaving them to face huge operational setbacks and recoveries.

The aftermath of wiper attacks is not only pure data loss but at times results in reputational damages, loss of customers' trust, and monetary implications as well. Business impact can be severe since businesses face extended downtimes with loss of intellectual property and legal repercussions. The organizations, as well as the individuals, in today's global network, must know how wiper attacks are carried out, what the effects would look like, and how to prevent them. That way, stakeholders are educated on how they can better prepare to fight off those risks created by the absolutely devastating cyber attacks



What are Wiper Attacks?

Wiper attacks are malicious cyber incidents involving malware specifically created to wipe data off a system. Data destruction could be as minor as deleting individual files, while major incidents would corrupt entire databases and completely render any critical information unusable. These attacks commonly target organizations operating in high-stakes industries so that they can create chaos, disrupt operations, and cause long-lasting damage.

Such a blow might bring debilitating effects because losing important information would stop business processes, damage the customer's trust, and provide difficulties of very large recovery dimensions

What makes Wiper Attacks so dangerous?

The danger of wiper attacks lies in their ability to cause instant and permanent harm. Since important data is wiped, then attackers are likely to fully cripple the operations within an organization, slow down productivity, and cause costly downtime events. This is unlike ransomware, whose possibility might be regaining lost data via some financial payment, but the wiper attack seems to completely have this chance erased.

This has a lot at stake in terms of integrity in relation to data and also disrupts business continuity since organizations would be unable to operate efficiently in the wake of such an attack. The psychological damage on employees and stakeholders, in addition to possible financial implications, makes wiper attacks especially menacing in the world of cybersecurity

Notable Wiper Attacks

Shamoon (2012): This was one of the first and most known wiper attacks that focused on the state -owned oil company Saudi Aramco. In this incident, data on thousands of computers were destroyed. The malware spreads across the organization's network rapidly to erase critical data and renders operational systems inoperable. Operations of the company experienced not just disruption but also big recovery efforts, rebuilding the whole IT infrastructure of the company. Such was the importance of Shamoon that it became a moment of consciousness in cybersecurity, and organizations realized that they could also suffer from similar hostile and damaging actions

Dustman (2019): Dustman was focused against Bahrain National Oil Company, overlaying files with random data on infected computers, effectively purging their information of principle that had links with Iranian state-sponsored threat actors. This indicates how nation-states may wield wiper malware as an influence or for economic disruption purposes. The critical sector targeted in the Dustman attack was oil production, and thus, it demonstrated the ability of wiper malware to disrupt critical services and underscored the geopolitical motivation for such cyber operations. In doing so, it vindicated the observation that organizations conducting businesses in critical infrastructure sectors have a reason to be constantly alert and perhaps more proactive concerning their cybersecurity posture in preventing all risks associated with state-sponsored attacks.

Best Practices

Immediate Isolation: Once the presence of a wiper attack is established, isolate affected systems immediately from the network. It will prevent the malware from spreading further and minimize data loss if the access of the infected devices from other systems is removed. This may include taking the systems offline or disabling their network connections to make sure that the spread is not possible

Data Recovery: Data recovery should begin once affected systems have been isolated. This typically occurs by leveraging accessible current backups to recover lost data. Anyone who regularly takes scheduled backups that are stored securely and tested for integrity may find those to be extremely helpful at this recovery stage. If no backups exist or those too are impacted, companies may have little option but to look for data recovery services, with no guarantee of success.

Forensic Analysis: A thorough forensic analysis would give the organizations involved knowledge of the nature of the attack. It would involve studying the entry process of the wiper malware, the weaknesses it exploited, and what was lost. Such information would aid immunity against such attacks in the future. Moreover, the process would be incident documentation to fulfill all the requirements on the aspects of compliance and reporting

Communication: Keeping the stakeholders, customers, and employees well-informed on the issue of the wiper attack is very important. Taking them into confidence maintains transparency and trust. Letting the stakeholders know the status of the recovery activities and their potential effects on customers or services would be very helpful. Proactive communication is hence positive as it negates reputational damage or any other losses, using credible communication to exhibit stakeholder concern that the organization takes the incident seriously.

Review and Revise Incident Response Plans: In organizations, the process of recovery serves as an avenue to review their incident response plans and processes. This review will discern the things that have worked well in responding to the incident and also determine the areas that are calling for change. By this, the organization will be better situated to counter any future threat after integrating the lessons learned into the incident response strategy.

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 10 **Date: 16-08.2025**

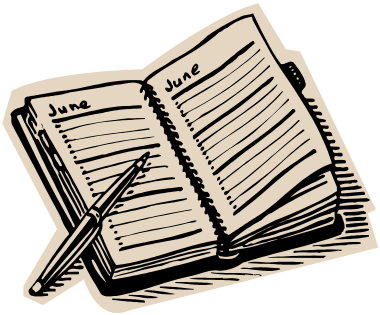
Aadhaar Biometric Fraud

In today's digital age protecting your personal information is of utmost importance. The bad actors are constantly on the lookout for ways to misuse your sensitive or personal data. The Aadhaar card is a crucial document that is utilised by all of us for various aspects. It is considered your official government-verified ID and is used for various purposes such as for verification purposes, KYC purposes, and even for financial transactions. Your Aadhaar card is used in so many ways such as flight tickets booked by travel agents, check-in in hotels, verification at educational institutions and more. The bad actors can target and lure the victims by unauthorized access to your Aadhaar data and commit cyber frauds such as identity theft, unauthorized access, and financial fraud. Hence it is significantly important to protect your personal information and Aadhaar card details and prevent the misuse of your personal information.

Fingerprint Cloning

Cybercrooks have been exploiting the Aadhaar Enabled Payment System (AePS). These scams entail cloning individuals' Aadhaar-linked biometrics through silicon fingerprints and unauthorized biometric devices, subsequently siphoning money from their bank accounts. Fingerprint cloning also known as fingerprint spoofing is a technique or a method where an individual tries to replicate someone else's fingerprint for unauthorized use. This is done for various reasons, including gaining unauthorized access to data, unlocking data or committing identity theft. The process of fingerprint cloning includes collection and creation.

Safety measures for the security of your Aadhaar Card data



Locking your biometrics : One way to save your Aadhaar card and prevent unauthorized access is by locking your biometrics. To lock & unlock your Aadhaar biometrics you can visit the official website of UIDAI or its official portal. So go to UIDAI's and select the "Lock/Unlock Biometrics" from the Aadhar service section. Then enter the 12-digit Aadhaar number and security code and click on the OTP option. An OTP will be sent to your registered mobile number with Aadhaar. Once the OTP is received enter the OTP and click on the login button that will allow you to lock your biometrics. Enter the 4-digit security code mentioned on the screen and click on the "Enable" button. Your biometrics will be locked and you will have to unblock them in case you want to access them again. The official website of UIDAI is "**https://uidai.gov.in/**" and there is a dedicated Aadhar helpline 1947.

Use masked Aadhaar Card: A masked Aadhaar card is a different rendition of an Aadhaar card that is designed to amplify the privacy and security of an individual Aadhaar number. In a masked Aadhaar card, the first eight digits of the twelve digits Aadhaar number are replaced by XXXX- XXXX and only the last four digits are visible. This adds an additional layer of protection to an individual Aadhaar's number. To download a masked Aadhaar card you visit the government website of UIDAI and on the UIDAI homepage, you will see a "Download Aadhaar" option. Click on it. In the next step, you will be required to enter your 12-digit Aadhaar number along with the security code displayed on the screen. After entering your Aadhaar number, click on the Send OTP. You will receive an OTP on your registered phone number. Enter the OTP received in the provided field and click on the "Submit" button. You will be asked to select the format of your Aadhaar card, You can choose the masked Aadhaar card option. This will replace the first eight digits of your Aadhaar number with "XXXX-XXXX" on the downloaded Aadhaar card. Once the format is selected, click on the "Download Aadhaar" button and your masked Aadhaar card will be downloaded. So if any organisation requires your Aadhaar for verification you can share your masked Aadhar card which only shows the last 4 digits of your Aadhaar card number. Just the way you keep your bank details safe you should also keep your Aadhaar number secure otherwise people can misuse your identity and use it for fraud.

Monitoring your bank account transactions: Regularly monitor your bank account statements for any suspicious activity and you can also configure transaction alerts with your bank account transactions.

It is important to secure your Aadhaar card data effectively. The valuable security measure option of locking biometrics provides an additional layer of security. It safeguards your identity from potential scammers. By locking your biometrics you can secure your biometric data and other personal information preventing unauthorized access and any misuse of your Aadhaar card data. In today's evolving digital landscape protecting your personal information is of utmost importance. The cyber hygiene practices, safety and security measures must be adopted by all of us hence establishing cyber peace and harmonizing cyberspace.

DIAL 1930 FOR ONLINE FINANCIAL FRAUD

REPORT ANY CYBERCRIME AT WWW.CYBERCRIME.GOV.IN

Stay Safe

Stay Alert!!!

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Date: 01.09.2025 **Volume 2 Issue 11**

How to Transfer Files Securely:

- **Cloud-based secure file sharing solution**: Automatically encrypt files that are exchanged between you and other collaborators, and access them from anywhere, anytime.
- **Password-protecting files and folders:** Password-protect or create password zip files before sending them via email. This is an excellent method for infrequent file transfers.
- **Secure File Transfer Protocol (SFTP):** Uses encryption to protect files as they traverse the web.
- **Password-protecting devices:** Flash drives and hard drives can be encrypted before you share them to keep your confidential information secure.
- **Email Add-Ins:** Bypass the file size limitations and automatically encrypt email content.

Secure File Sharing in the Digital Age

The digital age has revolutionized the way we work, learn, communicate, and live our lives. From online collaboration to remote work and e-learning, the digital world has opened up new opportunities for people around the globe. However, with this convenience and accessibility comes the need for secure file sharing.

Secure file sharing refers to the process of transferring files between individuals or organizations in a manner that ensures confidentiality, integrity, and availability of the data being shared. Many organizations use secure file-sharing software to share large files securely and collaborate with clients and teams. Secure file sharing usually involves data encryption, advanced access controls, audit trails, and password protection.

The Importance of Secure File Sharing

1. Protecting Confidential Information:

In today's digital world, businesses and individuals must protect confidential information such as financial data, legal documents, personal data, and intellectual property from cyber threats. Cybercriminals are always on the lookout for opportunities to exploit security weaknesses in digital systems to gain unauthorized access to confidential data. If a cybercriminal successfully intercepts a file transfer and steals client information it can result in identity theft, blackmail, and financial loss.

Secure file sharing offers a way to protect confidential information by providing encryption, authentication, and access control to ensure that only authorized users can access the data. Encryption scrambles the data into unreadable code that can only be decrypted by authorized users with the encryption key. Access control limits access to files to only those with authorization, and authentication ensures that users are who they claim to be

Cont...

2. Ensuring Privacy and Compliance:

Secure file sharing is essential for maintaining privacy and compliance with data protection regulations. In some industries, such as healthcare and finance, there are strict regulations around the handling of sensitive information. Failure to comply with these regulations can result in hefty fines and legal consequences.

In addition, sharing personal information such as medical records or financial information without appropriate privacy controls can result in identity theft, which can have severe consequences for the individual affected. Secure file-sharing solutions can help ensure compliance with data protection regulations to protect sensitive information from unauthorized access.

3. Facilitating Collaboration:

Collaboration is an essential part of modern-day work, and secure file sharing enables teams to work together on projects and documents with ease. Secure file sharing enables users to collaborate in one centralized location, view and request documents, and leave feedback. This improves productivity, enhances communication, and saves time, which is essential in today's fast-paced business environment. Additionally, secure file-sharing solutions can help to ensure that sensitive information is protected while still allowing for seamless collaboration between colleagues, clients, and co-counsel.

4. Minimizing Risks of Cyber Attacks:

In the digital age, cyber-attacks are becoming increasingly common and sophisticated, and businesses and individuals must take measures to protect sensitive information from such attacks. Unsecure file sharing can expose confidential information to cyber attacks such as malware, phishing, and ransomware. Cybercriminals can exploit vulnerabilities in digital systems to gain unauthorized access to sensitive information, causing data breaches that can result in significant financial losses and reputational damage.

Secure file sharing solutions are the shiny armour that companies need. It provides an additional layer of security to protect sensitive information from such attacks, minimizing the risks of data breaches. Automatic encryption ensures that the data shared is unreadable to entities other than the intended recipient. Two-factor authentication requires a unique code from a secondary device in addition to passwords in order to access accounts – decreasing the likelihood of a breach. If an attacker manages to access your account, password-protected channels prevent them from accessing the content, rendering their hacking attempts useless.

ZERO TRUST SECURE FILE SHARING IS SECURE FILE SHARING VIA A PLATFORM BUILT UPON ZERO TRUST PRINCIPLES

5. Improving Mobility:

In today's fast-paced business environment, mobility is essential, and employees need to access data from any location, on any device. Secure file sharing enables users to access data securely from any device, including smartphones, tablets, and laptops. This improves productivity and efficiency by allowing employees to work from anywhere, at any time.

6. Building Trust:

Secure file sharing helps to build trust among employees, customers, and partners. When sensitive information is protected, it builds confidence and trust among stakeholders, which is essential for building long-term relationships. This is particularly important in highly regulated industries such as finance, legal, and healthcare, where trust is a critical element of the business.

Give your clients peace of mind knowing their confidential information is protected to the greatest extent with secure file-sharing solutions. Not only do regulation compliance and encryption protect their confidential information, but it also reflects positively on your company.

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 12 **Date: 16.09.2025**

Your employees are using AI. But are they using it safely?

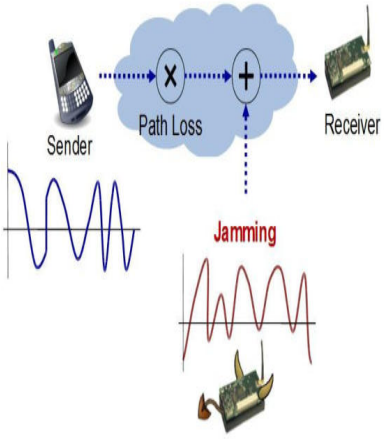
"Shadow AI", the use of unapproved AI tools at work, is more common than you think. New research reveals that 80% of companies are showing signs of this risky behaviour. From sales teams entering customer data into ChatGPT to HR uploading resumes into Claude, the potential for data leaks is massive.

Jamming– The Rising Cyber Threat

Jamming attacks are the use of malicious interference on wireless communication systems, including Wi-Fi, Bluetooth, and cell phone networks. GPS systems can also be the target of jamming attacks. In 2020, for example, 85% of cargo truck thefts in Mexico reportedly involved GPS jamming.

The intention of a jamming attack is to "jam" a network, preventing devices from communicating, disrupting essential services, or even bringing down a network altogether in a denial of service (DOS) attack.

Jamming attacks generally use physical devices to overload a network with strong signals, disrupting usual operations. Fraudsters can also take advantage of the service disruption, and therefore the confusion to callers, by committing telecommunications fraud attacks such as call spoofing.



Jamming attacks can happen on both a small and large scale. They can be weaponized as a wartime tactic or in terrorist attacks, or used for relatively superficial purposes. For example, jamming attacks can be used to cut off sound to Bluetooth speakers if the music is too loud at a neighborhood party

GPS Jamming

GPS jamming became a common part of vehicle theft from around 2010. An inexpensive device is used to disrupt signals to and from GPS satellite devices, essentially allowing a stolen and tracked vehicle to "disappear off the radar". Such devices have been used both for car thefts and for thefts of lorries with valuable cargo.

The same jamming devices can also be used to evade road tolls that use automated systems.

Wi-Fi Jamming

Wireless jamming attacks can use dedicated jamming devices or specially configured or compromised Wi-Fi-enabled devices such as laptops or smartphones.

A Wi-Fi jamming attack could be used to flood a wireless network with a constant disruption signal, resulting in slow speeds or a total lack of access for legitimate users. For example, security firms warn that wireless jammers can be used to disable Wi-Fi security cameras, by robbing them of the bandwidth they need to operate.

Consequences of Jamming Attacks

Disruption of Communication

Jamming attacks have the ability to disrupt or completely disable communication on networks such as Wi-Fi and Bluetooth. This can result in a loss of internet connectivity and the failure of the systems relying on it.

Data such as passwords and card details can also potentially be intercepted by a malicious actor as part of a jamming attack.

Inaccurate Navigation and Positioning

Above, we described how a GPS jamming attack can play a part in car theft or evading detection for traffic offenses. Various jamming attacks can also be used in modern military conflicts.

For example, it's been reported that GPS jamming attacks have taken place in Eastern Ukraine on a regular basis since Russia annexed Crimea in 2014. In war scenarios, jamming techniques can impact everything from unit positioning to the flow of information.

Financial Losses

Businesses of all kinds are increasingly reliant on wireless technology, for everything from service provision to payment processing. A retail store or restaurant that's unable to process card transactions due to a lack of internet access will immediately begin to lose money.

Jamming attacks can also play a part in other incidences of cybercrime, such as masquerade attacks, in which the interception of communications can lead to costly data leaks that compromise people's financial security.

How to Detect and Protect Against Jamming Attacks

a. Establish a way to monitor the strength of the wireless signal on the network. A sudden inconsistency in signal strength, or an increase in interference could be signs of a jamming attack in progress.

b. Use an intrusion detection system (IDS). Such a system can identify unusual traffic on the network and sometimes also take automatic steps to thwart an attack in progress. For example, an IDS can be used to shut down a frequency channel where suspicious activity is detected.

c. Educate yourself and other device users on cybersecurity principles. Encourage the use of virtual private networks (VPNs) and advise caution when using public Wi-Fi networks, such as those in cafes and hotels.

d. Use the strongest encryption available and practice good password hygiene.

Alongside these steps, remember that the best practices in cybersecurity may change over time, especially given the developing technology involved in jamming attacks. As such, point number c above bears repeating: Educate yourself about how to stay safe online with the most up-to-date research on jamming attacks and countermeasures.

Date: 01.10.2025

Volume 2 Issue 13

Cybersecurity Digest

Bi-Weekly by the CISO Section of Meghalaya Rural Bank

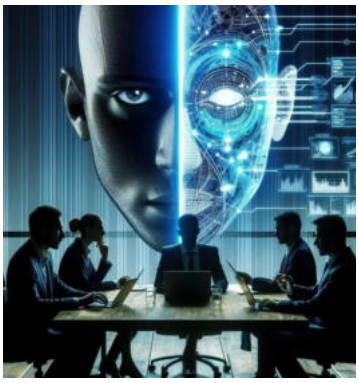
Dark AI

Dark AI is the malicious use of artificial intelligence to develop cyberattacks, commit fraud, or execute other illicit activities. It is also on the rise. Generative AI (GenAI) has lowered the barrier to entry, making it easier for cybercriminals to design and launch attacks.

At the same time, the rapid adoption of enterprise technologies, including AI, has expanded organizations' digital attack surface, introducing vulnerabilities that threat actors can exploit.

By 2025, cybercrime is expected to cost $10.5 trillion annually, and a growing share of that will be driven by dark AI.

Dark AI is not a specific technology; it's a set of tactics and behaviors that exploit AI's capabilities for harmful ends.



Key characteristics include:

Anonymity: Attackers operate in hidden online spaces, often using encryption, referrals, and cryptocurrencies to avoid detection.

Autonomy: Dark AI systems often run on autopilot with minimal human input, enabling attackers to launch large-scale attacks targeting multiple victims simultaneously.

Adaptability: Adversaries continuously adopt the latest AI innovations and adjust their methods to evade new detection systems.

Human-like behavior: From deepfakes to persuasive social engineering, dark AI mimics real human interactions to deceive and manipulate.

Whereas traditional AI is designed to improve productivity, decision-making, or quality of life, dark AI is built to infiltrate, mislead, and cause harm. It exploits trust and obscures intent, often with devastating consequences.

Dark AI challenges and cybersecurity threats

The rise of AI has made it faster and easier for attackers to launch sophisticated cyberattacks. What once required deep technical expertise is now accessible to a much wider range of threat actors, and many are using AI to sharpen their tactics and outpace traditional defenses. Understanding how dark AI accelerates risks can help teams stay proactive and resilient:

- **AI-powered cyberattacks:** Ready-to-use toolkits available on the dark web make it easy for attackers to launch phishing, malware, and ransomware campaigns. As a result, the volume and scale of attacks have surged.
- **Evasion capabilities:** Machine learning models help cybercriminals adapt to security systems in real time, making detection harder. Attack patterns can shift automatically to avoid known defenses.
- **Speed of attacks:** AI compresses the lifecycle of an attack. Breaches happen faster, and attackers can move across systems before security teams even spot the intrusion.

AI psychosis:

This term, inspired by the clinical definition of psychosis, describes a mental state where individuals develop delusional thoughts that are induced or amplified by AI. While humanity has experienced technology driven paranoia, since the times of Industrial Revolution of the 1800's, this recent sycophantic break with reality is unprecedented. The documented examples of this appalling behaviour include AI tools that glorify suicidal thoughts, push users to replace table salt with toxic chemicals, and provide fictional information that leads people to file lawsuits.

In extreme cases, individuals have proclaimed themselves to be on a messianic mission, develop fantasied romantic relationships with chatbots, mistake chatbot conversations for genuine love, and even treat the chatbots as sentient deities, believing that results from ChatGPT are god-like and beyond question. Such cognitive dissonance takes one's dependency (read addiction) on the AI tools to a whole new level, thereby resulting in the hallucinatory mental state aka AI psychosis.

Data privacy at risk

Dark AI threatens the very foundations of data privacy. Using sophisticated attacks, threat actors can access personal and sensitive data (e.g., credit card numbers, health records, and private communications). This data is then weaponized in secondary attacks, such as identity theft, extortion, and financial fraud.

Attackers also work hard to stay hidden, using tactics like spoofed IP addresses, VPNs, and proxy networks to avoid detection. These methods can make it harder to enforce even the strictest data protection frameworks, such as GDPR, HIPAA, and PCI-DSS.

Building strong, proactive data protection measures such as data encryption, access controls, and real-time monitoring is key to minimizing the impact if attackers manage to get through.

Exploiting social and communication platforms

Social media and communication platforms are increasingly being used as entry points for AI-driven scams. Attackers impersonate executives on LinkedIn and Twitter, mine Facebook and Instagram profiles for personal details, and even manipulate public discourse through deepfakes and AI bot activity.

By crafting more convincing messages and gathering more personalized data, AI helps attackers make scams harder to detect, and makes defending brand trust and user privacy even more important. Ongoing employee awareness, stronger identity verification processes, and smart monitoring of public-facing channels can help organizations reduce the risks tied to AI-powered social engineering.

How to protect against Dark AI

Staying protected from dark AI and other emerging cyber threats requires the integration of proactive, resilient security practices into every layer of your organization. By combining smart technology, ongoing education, and a strong security foundation, teams can reduce risks without slowing innovation. Here are some tips for staying ahead:

Track emerging threats

Stay informed about new AI-powered attack methods, tools, and tactics. Threat intelligence feeds, community updates, and industry reports can help your teams anticipate how attackers might use new technologies.

Train employees

Empower your teams to recognize and respond to AI-enhanced phishing attempts, deepfakes, and social engineering. Regular training builds a culture of security awareness and can turn employees into an effective first line of defense.

Enhance security with AI

While it is introducing new dangers, AI can also be a force for good. Use advanced detection tools that can spot anomalies, detect zero-day threats, and automate response actions. Security solutions can also help you shift left by embedding security into development workflows, so vulnerabilities are caught and fixed as early as possible.

AI red teaming

To counter these sophisticated threats, security teams can think like their adversaries. AI red teaming is a proactive security measure where ethical hackers use AI to simulate realistic attacks on an organization's systems, applications, and data. This goes beyond traditional red teaming by leveraging AI tools to automate reconnaissance, exploit vulnerabilities, and navigate complex networks, mirroring the tactics of modern attackers.

By using AI to probe for weaknesses, organizations can identify and patch vulnerabilities before malicious actors can exploit them. The insights gained from these simulations are critical for building more resilient defenses and ensuring a "secure by design" posture. It's a step in preparing for a future where AI-powered attacks are the norm.

Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Date : 16.10.2025

Volume 2 Issue 14

Cyber-Laundering

The rise of the internet and digital technologies has brought a lot of benefits and convenience to people's lives, from online shopping to social media. However, it has also opened the door to a new type of criminal activity known as cyber laundering.

Cyber laundering is a sophisticated form of money laundering that leverages the internet and other digital platforms to conceal and transfer illegally obtained funds. It involves the use of complex and advanced technologies, such as virtual currencies, encryption, and anonymization, to cover the tracks of criminal activities.

The process typically involves three stages: placement, layering, and integration, like traditional money laundering. In the placement stage, the illicit funds are introduced into the digital system, often through anonymous online transactions. In the layering stage, the funds are moved around and disguised through multiple transactions, often across different jurisdictions and currencies. In the integration stage, the funds are reintroduced into the legitimate financial system, usually through the purchase of assets or investments.

One of the most common methods of cyber laundering is through virtual currencies, such as Bitcoin, which allow for anonymous and untraceable transactions. Criminals can use these currencies to purchase goods and services online, transfer funds across borders, and convert the proceeds back into traditional currencies, all without leaving a digital trail. Another technique is through the use of anonymous communication and encryption tools, such as Tor and VPNs, which allow criminals to communicate and transfer funds without detection. They can also use sophisticated techniques, such as "mixing" services, which blend the funds of multiple transactions to make it difficult to trace the original source.

Cyber laundering poses a significant threat to the global financial system, as it allows criminals to conceal and use the proceeds of their illegal activities. It also creates a challenge for law enforcement agencies, who must adapt their methods to keep up with the constantly evolving digital landscape. To combat cyber laundering, governments, and financial institutions have introduced a range of measures, such as increased monitoring, stricter regulations, and the development of new technologies, such as blockchain, to enhance transparency and security. However, the battle is far from won, and it will require ongoing cooperation and innovation to stay ahead of the cybercriminals

Types of Cyber-laundering

Stay Alert

There are two types of cyber-laundering, each with its own unique characteristics and methods.

The first type is called "**instrumental digital laundering**." In this type of cyber-laundering, the criminal uses digital tools to carry out one or more constituent steps of the money laundering offense. These steps can include placement, layering, and integration. Placement is the process of introducing illegal funds into the financial system. Layering involves moving the money through various accounts and jurisdictions to disguise its origin. Integration is the final stage in which the laundered money is used to purchase legitimate assets.

Contd...

The second type of cyber-laundering is known as "**integral digital laundering**." In this type of money laundering, all three steps take place entirely and completely with the use of computers or digital tools. The cybercriminal will use digital currencies, such as Bitcoin, to transfer funds from one account to another. This type of cyber-laundering is more complex and difficult to detect as all transactions take place online, with no physical presence or paper trail.

Cyber-laundering typically operates on the internet, taking advantage of computer bugs and loopholes or using specific hardware and software systems to establish connections in anonymity and non-traceability of one's location. This method allows criminals to deceive law enforcement authorities and carry out their illicit activities without being detected.

In recent years, there have been numerous cases of cyber-laundering, with criminals using increasingly sophisticated methods to carry out their illegal activities. Law enforcement agencies have had to adapt to these changing circumstances and invest heavily in technology and training to keep up with the pace of technological advancement.

The Intersection of Cyber Crimes and Money Laundering

The connection between cyber crimes and money laundering is intricate and concerning. Cyber criminals often employ money laundering techniques to conceal their illicitly obtained funds. By funneling the money through various bank accounts and financial transactions, they aim to make it appear legitimate and remove any trace of its criminal origins.

Money laundering is a crucial component of the cyber crime ecosystem, enabling criminals to enjoy the financial benefits of their illegal activities without raising suspicion.

The unregulated nature of cryptocurrency also presents opportunities for cyber criminals to launder money, due to the difficulty in tracing transactions.

Cyber criminals continuously adapt their money laundering tactics to stay ahead of law enforcement efforts. They may use online gambling platforms, shell companies, or even legitimate businesses to obscure the origins of their funds. These tactics make it challenging for authorities to track and prosecute those involved in cyber crimes.

Moreover, the global nature of cyber crimes and money laundering poses significant challenges for international cooperation and coordination among law enforcement agencies. Criminals can exploit jurisdictional gaps and differences in regulations to move their illicit funds across borders swiftly, making it harder for authorities to apprehend them.

Future Trends in Cyber Crime and Money Laundering

The landscape of cyber crimes and money laundering is ever-evolving. As technology advances, cyber criminals will continue to adapt their tactics to exploit new vulnerabilities. One emerging trend is the use of artificial intelligence and machine learning by cyber criminals to automate their attacks and evade detection.

Furthermore, the increasing popularity of cryptocurrencies presents an ongoing challenge in combating money laundering. Governments and regulatory bodies are striving to establish stricter measures to monitor cryptocurrency transactions and ensure compliance with anti-money laundering regulations.

Another significant trend on the horizon is the rise of deepfake technology in cyber crimes. Deepfakes are hyper-realistic forgeries created using artificial intelligence, making it difficult to distinguish between real and manipulated content. Cyber criminals could potentially use deepfakes to impersonate individuals or create fraudulent videos to deceive individuals or organizations.

Moreover, the Internet of Things (IoT) devices are becoming more integrated into daily life, creating new opportunities for cyber criminals. These interconnected devices, such as smart home appliances and wearable technology, can be exploited to launch cyber attacks or facilitate money laundering schemes. As the number of IoT devices continues to grow, so does the potential attack surface for cyber criminals.

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

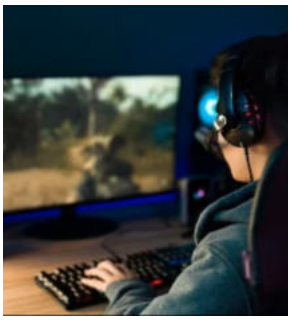
Volume 2 Issue 15 **Date: 01.11.2025**

Video games: A gateway to online money laundering

Online video games have become a popular pastime for people of all ages. However, the rise of the virtual economy and the increasing value of in-game items and currencies (in-game items and in-game currencies) have also made them a target for money launderers. Money laundering is the disguise of proceeds from illegal activities as legitimate funds, and criminals use virtual currencies and in -game items in online video games to launder their illicit funds. The anonymity and global reach of the Internet make it an attractive option for money launderers, as it allows them to move money across borders and through different financial systems with relative ease.

What are in-game currencies?

An in-game currency is a virtual currency created specifically for a video game to fuel its virtual economy. This type of currency can either be earned in-game by winning challenges or acquiring new abilities, converted into real funds or traded between players.

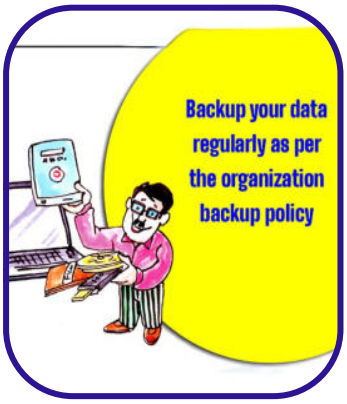


There are two common types of in-game currency: convertible and non-convertible. With the more convertible currency, a player can exchange real currency for in-game currency and then back again. Many of these types of currencies have a fluctuating exchange rate and a specific exchange platform. A player can use this type of currency to create, sell, or trade items with other players in the game, or to invest in the game's virtual properties or assets. With non-convertible currency, a player can exchange real money bills for in-game currency, but not back. This currency can only be used within the game to purchase skins, weapons, or power-ups for the player's avatar to personalize their in-game character, but cannot be traded with other players or officially invested.

Why cybercriminals use the video game industry for money laundering.

The video game industry, particularly the market for online multiplayer games, has seen a rise in nefarious activity in recent years due to the lack of regulation by local and international organizations, few to no customer identification rules, ease of transferring in-game currency, and crowded platforms that allow criminal transactions to get lost in the myriad of legitimate transactions.

For money launderers, traditional methods of money laundering pose higher risks than in the past as AML regulations become tighter. As a result, cybercriminals are looking for new avenues. The video game industry is one of those new avenues. The video game industry poses a money laundering risk due to in-game commerce, as game materials can be purchased with real money in some video games. The key factor that makes money laundering through online games possible is that virtual items in the game sometimes have real value outside the game. These include, for example, artifacts that give the game character additional powers (e.g., swords, armor, and potions) or "currencies" that can be used to purchase them.



Examples of money laundering in online games

The use of convertible and non-convertible virtual currencies in the video game industry and the anonymity offered to players have created an environment for criminal activity. When purchases are made for the game in online video games, users enter their credit card information into the system. Criminals can steal these credit card details and conduct money laundering activities through these accounts. In addition, cybercriminals typically log into accounts without two-factor authentication and use stolen credit card information to purchase in-app money. These game materials and purchased currency can then be sold on an online marketplace at a lower price. Game owners can only find a solution if they are aware of this event.

Some common methods are:

- Buying virtual currency or in-game items by illegal means and then selling them for profit on third-party marketplaces.
- Using virtual currency or game items to purchase real goods or services, such as weapons, drugs, or other illegal items.
- Creating multiple accounts in a game and using them to transfer virtual currency or game items between accounts.
- Gambling with virtual currency or game items in online games.
- Creating fake virtual items in a game and selling them to other players

How are values acquired?

The normal way to acquire new game values is to simply play the game. But the game is not fast enough for those who want to make money by trading values from the game. Criminals have found out that it is not difficult to gain access to a computer and the game using phishing, Trojans or simply hacking the PC. Once they gain access, there are several ways criminals can get game assets. Basically, it's not difficult using common phishing techniques, such as emails that entice people to click on a link that downloads malware, gaining access to the player's name and password. The criminals discovered that it was quite easy to take over a computer in this way and went one step further. They refined the malware so that it also gave access to bank and credit card information and even took over the player's access to the banking system. After that, the easiest way to empty the bank account was to make large or multiple purchases. However, they also discovered that they could use the account to transfer illegal funds. By buying game assets directly from the account and immediately reselling them to an exchange or RTM (real money trading) website, they could make the money virtually untraceable.

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Volume 2 Issue 16 **Date: 16.11.2025**

TOR Browser

The Tor network originated with research conducted by the United States Naval Research Laboratory in the mid-1990s, which developed the foundational technology behind onion routing. The project later released its code for public use, and in 2003 a publicly accessible version of the Onion Routing software—eventually known as Tor—became available. In 2006, The Tor Project, a nonprofit research and education organization, was established to oversee the network's development and maintenance.

According to Tor, its mission is to promote human rights and freedoms by creating and deploying free, open-source tools that enhance anonymity and privacy online. The Tor Browser embodies this mission by enabling users to browse the internet with a high level of confidentiality. It achieves this by routing traffic through multiple volunteer-run servers, or nodes, layering encryption in a way that resembles the many layers of an onion, which makes tracing user activity significantly more difficult.

Despite these privacy-focused intentions, Tor has become closely associated with the dark web, as the anonymity it provides is sometimes used for illicit activities. While the software itself is legal in many countries and was never designed to facilitate criminal behavior, some governments restrict or prohibit access to the network due to these concerns.

What is the Tor browser used for?

There are several questions worth asking about Tor, including "What does a Tor browser do?" and how its use differs from regular browsers. The Tor browser is primarily a way to browse the web anonymously. As such, the main reason it is used is to avoid surveillance and ensure privacy while online. However, many people also use Tor to access services that regular browsers cannot reach, such as .onion sites which only function on the onion network, such as DuckDuckGo, a privacy-enhanced search engine, which offers a .onion version of its search engine, which doesn't track user data, providing a more private search experience.

In addition, because Tor is closely linked with the dark web, some users use this for particular types of research, and also to carry out illegal activities.

How does a Tor browser work?

In its simplest form, a Tor browser use onion routing to direct and encrypt all traffic, offering users a high level of anonymity. The network transmits traffic through three layers of international network nodes called onion routers:

- Entry nodes, which form the first layer of encryption and enable the connection to the Tor network.
- A series of middle nodes fully encrypt web traffic to ensure anonymity.
- Exit nodes, which further encrypt data before it reaches the final server.

Because onion routing effectively encrypts and relays data through multiple network layers, the Tor browser is highly effective at protecting user data and concealing IP addresses.

Benefits of a Tor browser

The Tor browser does have several advantages, which is why some internet users can benefit from using it. However, not all of these will be relevant to regular internet users. Here are some of the main reasons why some users choose to use a Tor onion browser:

- The browser is a free, open-source program
- IP addresses and browsing history are masked
- Enjoy heightened network security because the Tor browser operates on secure, encrypted networks
- Easy access to non-indexed pages, especially through search engines.

Disadvantages of a Tor browser

Aside from security concerns and wondering "is the Tor browser safe," there are some other potential disadvantages of using this software. Below are a few things to keep in mind before deciding to use the Tor onion browser.

- Because of the way it routes traffic, Tor connections are very slow, especially when compared to VPNs, and downloading large files is not practical.
- Activity may not be completely anonymous, and it is possible to decrypt a user's identity
- Some countries and companies can block the Tor browser, and its usage can even be illegal in certain countries.
- The use of this browser can be suspicious, even if it is legal
- Not all websites function on Tor.

How to stay safe while using the Tor browser

Many users wonder "How to stay safe while using the Tor browser?" and this is indeed a fair question. As with anything else online, there is an inherent risk with using a Tor browser. However, users can take steps to mitigate these and be mindful of their online activities. Here are a few tips for safely using the Tor browser:

- Ensure that the Tor browser and any associated apps or extensions are always up to date.
- Use the Tor browser in conjunction with a VPN.
- Employ a firewall to protect the computer's network.
- Use antivirus software.
- Avoid logging into personal accounts, such as social media profiles or emails.
- Use the Tor browser randomly, so that it is hard to create identifiable patterns.
- Use the highest level of security available on the chosen Tor browser, so that it executes the least amount of browser code and helps protect devices from malware.
- Use an extension that protects your privacy and only accesses secure HTTPS websites, such as extensions that will automatically rewrite a URL to use HTTPS instead of HTTP.

DoT introduces new cybersecurity rules to combat cyber fraud

The Department of Telecommunications (DoT) has finalized new cybersecurity rules for the tech and telecom sectors, including major operators such as Airtel, BSNL, Jio, and Vi. These regulations aim to address the rapidly rising cases of cyber fraud. A central feature of the new framework is the **Mobile Number Validation (MNV) platform**, developed by the DoT to verify whether a mobile number is correctly linked to its user as per the telecom operators' KYC records. This platform will enable banks, financial institutions, and insurance companies to authenticate a customer's mobile number during account opening, strengthening safeguards against fraud. By allowing secure, direct verification of phone numbers between financial institutions and telecom operators, the MNV platform fills a critical security gap and plays a key role in preventing cybercrime.

NATIONAL CYBERCRIME REPORTING PORTAL
IF YOU ARE A VICTIM OF FINANCIAL CYBER FRAUD VISIT cybercrime.gov.in OR DIAL HELPLINE NUMBER 1930
HELPLINE NUMBER 1930

Volume 2 Issue 17

Date: 01.12.2025

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Stuxnet

Stuxnet is a highly sophisticated computer worm that became widely known in 2010. It exploited previously-unknown Windows zero-day vulnerabilities to infect target systems and spread to other systems. Stuxnet was mainly targeted at the centrifuges of Iran's uranium enrichment facilities, with the intention of covertly derailing Iran's then-emerging nuclear program. However, Stuxnet was modified over time to enable it to target other infrastructure such as gas pipes, power plants, and water treatment plants.

Whilst Stuxnet made global headlines in 2010, it's believed that development on it began in 2005. It is considered the world's first cyber weapon and for that reason, generated significant media attention. Reportedly, the worm destroyed almost one-fifth of

Iran's nuclear centrifuges, infected over 200,000 computers, and caused 1,000 machines to physically degrade.

Who created Stuxnet?

Whilst no-one officially claimed responsibility for Stuxnet, it is widely accepted that it was a joint creation between the intelligence agencies of the US and Israel. Reportedly, the classified program to develop the worm was code-named '**Olympic Games**' which began under President George W Bush and then continued under President Obama. The program's objective was to derail or at least delay Iran's emerging nuclear program.

Initially, agents planted the Stuxnet malware in four engineering firms associated with Natanz – a key location in Iran for its nuclear program – relying on careless use of USB thumb drives to transport the attack within the facility.

Is Stuxnet a virus?

Stuxnet is often referred to as a virus but in fact, it is a computer worm. Although viruses and worms are both types of malware, worms are more sophisticated because they don't require human interaction to activate – instead, they can self-propagate once they have entered a system.

Besides deleting data, a computer worm can overload networks, consume bandwidth, open a backdoor, diminish hard drive space, and deliver other dangerous malware like rootkits, spyware, and ransomware.

WhatsApp Screen Mirroring Fraud

In this type of scam, fraudsters trick a person into enabling screen-sharing via WhatsApp. This way, the fraudsters gain access to the person's sensitive information such as OTPs, bank details, passwords, personal messages, etc. As a result, the person can fall prey to financial losses, account takeovers and even identify theft.

How to stay Safe?

Verify the caller's identity through official channels before engaging.

Avoid screen-sharing unless absolutely necessary and only with trusted contacts.

Enable two-factor authentication on all financial and messaging apps.

Keep your phone's operating system and apps updated to close security gaps.

Notify your bank to freeze or secure your accounts.

Why is Stuxnet so famous?

Stuxnet generated extensive media interest and was the subject of documentaries and books. To this day, it remains one of the most advanced malware attacks in history. Stuxnet was significant for a number of reasons:

- It was the world's first digital weapon. Rather than just hijacking targeted computers or stealing information from them, Stuxnet escaped the digital realm to wreak physical destruction on equipment the computers controlled. It set a precedent that attacking another country's infrastructure through malware was possible.
- It was created at nation state level, and while Stuxnet was not the first cyberwar attack in history, it was considered the most sophisticated at the time.
- It was highly effective: Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.
- It used four different zero-day vulnerabilities to spread, which was very unusual in 2010 and is still uncommon today. Among those exploits was one so dangerous that it simply required having an icon visible on the screen – no interaction was necessary.
- Stuxnet highlighted the fact that air-gapped networks can be breached – in this case, via infected USB drives. Once Stuxnet was on a system, it spread rapidly, searching out computers with control over Siemens software and PLCs.

Cybersecurity for industrial/organizational networks

In the real world, advanced nation state attacks like Stuxnet are rare compared to common, opportunistic disruptions caused by things like ransomware. But Stuxnet highlights the importance of cyber security for any organization. Whether it's ransomware, computer worms, phishing, business email compromise (BEC), or other cyber threats, steps you can take to protect your organization include:

1. Apply a strict Bring Your Own Device (BYOD) policy that prevents employees and contractors from introducing potential threats onto your network.
2. Implement a strong and technically-enforced password policy with two-factor authentication that hinders brute force attacks and prevents stolen passwords from becoming threat vectors.
3. Secure computers and networks with the latest patches. Keeping up-to-date will ensure you benefit from the latest security fixes.
4. Apply easy backup and restore at every level to minimize disruption, especially for critical systems.
5. Constantly monitor processors and servers for anomalies.
6. Ensure all your devices are protected by comprehensive antivirus. A good antivirus will work 24/7 to protect you against hackers and the latest viruses, ransomware, and spyware.

Password change email from 'rnicrosoft.com' is a phishing scam

Heads up! There's a new phishing scheme targeting Microsoft users with fake password reset emails. Scammers have set up a website similar to Microsoft's, using 'rnicrosoft.com' to lure you in. This could lead to serious security breaches for your account. Make it a habit to scrutinize email addresses and links closely. For password resets, go straight to the Microsoft homepage.

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Volume 2 Issue 18 **Date: 16.12.2025**

Bank Drop

A bank drop refers to a bank account controlled by a criminal, used as a pivot in financial system conceived to launder illicit gains. It is either created through fake credentials or stolen to an unsuspecting victim. In some cases, money mules can also be used.

A bank drop is essential in money laundering schemes, as it is often used to legitimize and conceal the proceeds of illegal activities. It can support cybercriminals engaged in layering and structuring activities, as part of their money laundering process. Financial systems are now strongly monitored against money laundering activities. Therefore, elaborated financial structures are developed to wash out the proceedings of their activities.

In the very beginning, bank drops involved physical manipulation, such as forgery. With the rise of Internet, cybercriminals shifted gear and were able to carry their operations remotely. Although there are plenty of methods to obtain one, more advanced techniques such as breaching into banks' information systems or spear phishing made their appearance. Automation bank drops' networks also allowed organized crime to streamline their financial operations.

As cybercriminals continue to exploit the digital landscape, the connection between bank drops and cybercrime is very intricated. Because digitization and automation made a huge impact on financial systems, cybercrime also took the opportunity to become more sophisticated electronically. Moreover, cyber-enabled crime now represents an increasing part of the puzzle. Ransomware is now a looming threat over companies, and individuals face waves after waves of phishing attacks and account takeovers.

Alongside bank drops, cybercriminals have also evolved in their money laundering techniques. They now operate complex schemes involving shell companies, countless accounts and international transfers to obfuscate the origin of their illicit funds.

How do bank drops work

Bank drops usually follow a series of coordinated steps:

- **Credential collection:** At first, the cybercriminal will usually gather identity information to create a bank drop, either by stealing or purchasing someone's credentials or even creating a synthetic identity. To make it legitimate, it may also create a comprehensive ecosystem with an email address, burner phone, and IP address to replicate the victim's environment;
- **Selecting a bank:** Once the identity is well-crafted, the cybercriminal will find an appropriate bank to open an account. It may leverage a money mule to do it on his behalf and further protect itself from detection. The bank selected would have preferably weaker controls over identity information;
- **Legitimizing the account:** After the account is opened, few legitimate transactions will be conducted to give it a clean state, and avoid raising any red flags;
- **Operating the bank drop:** If all goes well, the bank drop will then be used to receive the money from illicit activities. This will be combined with money laundering techniques to distance the funds from their illegal origins;
- **Withdrawing the funds:** Finally, after the funds have been laundered or moved to different accounts, the perpetrators proceed to withdraw the money as cash, transfer it to offshore accounts, or utilize it for personal gain. This step aims to obscure the trail and make it challenging for authorities to link the funds back to the initial illegal activities.

Why bank drops are so nefarious?

Even though bank drop aids and abets the money laundering of criminal activities, it is also the result of other crimes such as impersonation, identity theft, or penetration of information systems. Since bank drops often serve as a gateway to other criminal activities, funds laundered through them may be used to finance and facilitate additional illegal operations, such as drug trafficking or terrorism.

Given the bank drop's key role in money laundering schemes, it can cause tremendous damage and deeply undermine the trust in financial institutions. On the other hand, banks that fail to prevent those activities may face important fines from regulators, but also administrative sanctions.

Victims of identity theft can also suffer the consequences of bank drops and put them at risk as their identity can be used to conduct additional illegal activities. As it also relies on the recruitment of money mules, lured by promises of easy money, bank drops can put them at risk of becoming accomplices to criminal activities.

What measures can be taken to tackle bank drops

Given the severe consequences of bank drops, comprehensive for the civil society as a whole, measures to tackle it are necessary. While everybody can play a role from law enforcement to individuals, financial institutions are the key players in combatting bank drops. As technological advancements are now allowing cybercriminals to automate the creation of bank drops, financial institutions need to implement different measures to mitigate this risk:

- **Raise awareness among employees and customers**: Employees are sometimes the first line of defense. Training employees to detect such threats, but also raising awareness among customers can prove to be powerful to detect and limit bank drops;
- **Ask for customer information:** Thorough checks make for full-proof financial environments. When in doubt, operators should always ask for more information, to determine origin of funds or customer's identity;
- **Establish risk-based transaction monitoring systems:** Detecting suspicious transactions is essential to identify bank drops. Between behavioral analysis using algorithms to analyze patterns, deviations alerts and risk scores, robust transaction monitoring system can prove as a useful ally against bank drops;
- **Implement comprehensive anti-money laundering (AML) programs:** By developing adequate deterrence policies based on customer account usage, enforcing strong due diligence processes to obtain relevant information on the customer, a comprehensive AML program not only allow financial institutions to comply with current regulations, but also empowers them against multiple threats;
- **Cyber security measures:** Enforcing robust two-factor authentication (2FA), but also implementing advanced threat detection can boost how financial institutions deter bank drops.

Prevention of Cybercrime

- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- To prevent cyber stalking avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public places.
- Never send your credit card number to any site that is not secured, to guard against frauds.

Vol 2 Issue 19 Date: 01.01.2026

MEGHALAYA RURAL BANK

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Harvest Now Decrypt Later Attack

We have entered a new era in cybersecurity, and concerns that seemed settled long ago now loom large. Previously effective cryptography practices, in particular, will no longer provide the same level of reassurance they once did. It's time for enterprises to up their cybersecurity game—and this means acknowledging (and addressing) shifts in cryptography best practices.

Many sophisticated attacks now leave even seemingly well-protected websites and organizations at risk. Among the most worrisome? The harvest now, decrypt later (HNDL) strategy. Also referred to as harvest and decrypt, this is the purview of patient cybercriminals, who are willing to wait as long as it takes for quantum computing to shake up the cryptography scene

Also referred to as "retrospective decryption" or "store now, decrypt later," HNDL involves a unique approach to cybercrime: threat actors seek currently encrypted data, even if they are unable to access it yet.

From there, sophisticated cybercriminals can bide their time until quantum computing tactics become readily available. This is the ultimate form of playing the long game, and attackers anticipate that it will pay off.

Once quantum computing enters the picture, previously effective encryption algorithms will no longer keep the stored data these cybercriminals collected safe. Unfortunately, quantum computers will have the power to break widely used encryption algorithms like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC).

How the harvest now, decrypt later attack works

The central strategy of harvest now, decrypt later is simple: gather as much data as possible and prepare to decrypt it in the future. This is a purpose-driven strategy, and cybercriminals are far from haphazard in their efforts; they go to great lengths to ensure that they can access information that will be easiest to leverage and that will cause the most damage once decrypted.

Data harvest stage

It's widely accepted that we are already in the midst of the data harvest stage, as many sophisticated attackers are well aware of the upcoming availability of quantum computing and eager to leverage enhanced computing power as soon as possible. Threat actors are preparing right now, and potential victims should be as well. Critical components of data harvesting include:

- **Identifying targets**. This strategy begins with the careful selection of targets. Typically, threat actors focus on data that will remain relevant over time. This could include anything from personal data (such as financial information) to intellectual property. A lot depends on how the cybercriminals intend to use that information once decrypted. Adversaries may also examine encryption strength, targeting data if it's thought likely to become vulnerable in the next few years. Cybercriminals tend to seek out vast quantities of data, with the assumption that at least some of it will prove useful later on.
- **Capturing encrypted data**. Once targets have been identified and thoroughly researched, the next step involves obtaining the desired data. Yes, it may be encrypted at this point, but that will not stop threat actors from seeking access. Through numerous attack mechanisms, cybercriminals can pinpoint vulnerabilities, breach servers or databases, and capture data without initially decrypting it.
- **Monitoring**. The 'harvest' portion of HNDL attacks may not necessarily represent a one-time pursuit. If vulnerabilities are detected, threat actors may monitor these over time and continue to capture data as it becomes available. Those targeted may never realize that they are being monitored and their data is being harvested.

Data storage and management

After obtaining encrypted data, cybercriminals enter an uncertain stage that could potentially last several years: storing and managing a wealth of illicitly obtained information. Many rely on cloud storage and fraudulent accounts, although some may look to physical storage solutions for enhanced security and obfuscation.

Techniques such as fragmentation or misnaming of files may make it more difficult to detect bad actors. Over time, these cybercriminals will continue to verify that harvested data remains accessible (only to them, of course) and that it is properly concealed. They may also take steps to limit the risk of data loss or obsolescence.

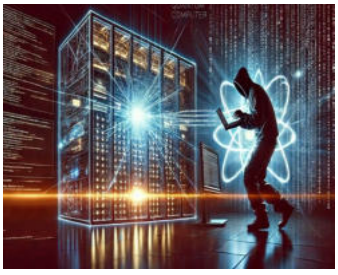
Future decryption with quantum computers

While quantum computing is not yet available, all signs indicate that this will soon change. When this unmatched computing power is unleashed, bad actors—who have patiently waited for years—will have the ability to decrypt previously protected data. At this point, they will be able to break algorithms such as RSA and ECC.

This devastating final stage will begin with gaining access to quantum computing resources and then centralizing data, which may have been stored in numerous locations through the years. From there, the strongest quantum algorithms (capable of breaking the most powerful encryption schemes) can be applied.

Key discovery will play heavily into this stage and could leave targeted organizations at risk. Following successful decryption, cybercriminals may have access to passwords, financial information, and other sensitive data that can be used for malicious purposes.

The importance of addressing this type of threat now



The quantum age is closer than most people think; experts anticipate that by 2030 conventional asymmetric cryptography will no longer provide sufficient protection. This is only a few short years away, and already threat actors could potentially be gathering sensitive data to be used for ill purposes later on.

With threats such as HNDL coming to light, it is increasingly clear that quantum concerns need to be addressed as soon as possible. The term "quantum threat" describes the urgency that this situation requires—and underscores that, although quantum computing could present some unique opportunities, we cannot fully realize them unless we promptly address the accompanying security concerns.

Developing and implementing a strong post-quantum framework (including quantum-resistant algorithms) takes years, and although the field has made great progress in recent years, most organizations remain far from sufficiently protected.

Banking Cybersecurity: Investment, Not Expense

For now, one shouldn't think of cybersecurity in banking as an expense. It's an investment in client trust, in reputation, in preserving assets. One successful attack can cost more than years of spending on security.

The trends of 2025 show that protection must be built in at all levels. From technology to processes, from people to organizational culture. It's not a simple path, but it's the right one.

Banks that take cybersecurity in banking seriously, that invest in technology, train people, and constantly adapt to new threats, will be leaders in both resilience and client trust. This will be the most important competitive advantage of the next decade.

The future of the banking system depends not on one-time solutions, but on constant, deliberate readiness. And the time to start has come long ago.

It is not enough to protect your data, you need to protect your customers' data too

MEGHALAYA RURAL BANK

Cybersecurity Digest

Bi–Weekly Update by the O/o CISO of Meghalaya Rural Bank

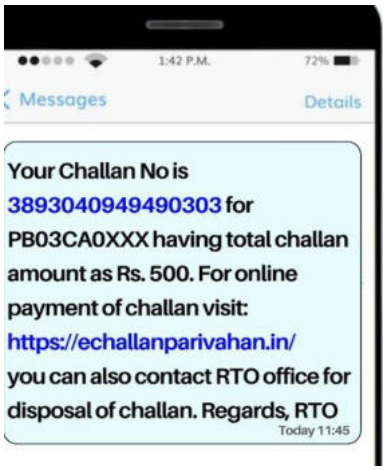
Vol 2 Issue 20 **Date: 16.01.2026**

E-Challan Scams

This is a new cyber fraud where scammers pose as traffic authority and make people download a fake app for paying challans. This app is actually malware that steals sensitive information from mobile like SMS, banking apps, OTP and passwords.

In this scam, cyber criminals pose as traffic police or government agency officials and send fake challan messages through WhatsApp, SMS or email. It states that your vehicle has violated traffic rules and you need to pay a fine. Along with this, an APK file (like e-parivahan.apk) or link is provided, which claims to install this app to view challan details or make payment.

When the user downloads this file and installs the app, it requests access to sensitive information from the phone such as SMS, contacts, banking apps, passwords and OTPs. Once this access is granted, scammers steal money from accounts through mobile banking or UPI.



How to differentiate between real and fake e-challan messages?

Real challan messages come from government's official SMS IDs (like VK-MORTH, CH-TRAFF etc.) and do not mention any APK files or suspicious links. For genuine challan information, you need to visit government websites like https://echallan.parivahan.gov.in and enter RC number or driving license number. Whereas fake challan messages contain fear-inducing language and pressure to download APK files or click on links.

What to do if you have downloaded a fake app?

- Uninstall the app immediately.
- Go to mobile settings and remove all permissions.
- Change passwords for your bank, UPI and social media accounts.
- If money has been withdrawn or you are being blackmailed, file a complaint at the nearest cyber crime cell.
- Additionally, you can file an online complaint on the cyber crime portal.

The official mParivahan app is only available on Google Play Store or Apple App Store. Its developer is 'NIC eGov Mobile Apps'. Additionally, you can verify its official link by visiting https://parivahan.gov.in.

What precautions should be taken to avoid such fake apps ?

Scammers take advantage of fear and urgency to make users make mistakes. You can protect yourself from such fraud by following the measures given below.

- Never install any app from an APK file.
- Do not click on any link provided in the challan message.
- When you receive a challan message, first check it on the official government website.
- Before downloading any app, check the app developer's details and ratings on the playstore.
- Always verify the URL carefully before clicking on any link.
- Keep your banking SMS and UPI apps secured with an app lock.
- If in doubt, verify on the official website of the traffic police.

Can antivirus or security apps stop such fake apps?

Some mobile security apps do scan APK files and give warnings, but they don't guarantee 100% security. The best approach is to download apps only from Google Play Store or Apple App Store. Also, never install APK files received through messages or websites.

Volume 2 Issue 21

Date: 01.02.2026

Cybersecurity Digest

Bi-Weekly update by O/o CISO of Meghalaya Rural Bank

URL Poisoning

In today's hostile Internet, URL poisoning poses a significant threat to web users, their computers, and their data. This malicious technique—also known as URL manipulation attack, URL redirection attack, or URL interpretation attack—allows attackers to deceive users to the true destination of a URL by altering that URL to redirect them to harmful websites. By understanding how URL poisoning works, its impact on businesses, and preventive measures, you can safeguard yourself and your user population against a wide variety of impacts.

Most URLs are human-readable because they begin with a fully-qualified domain name (FQDN) such as "search.google.com." Even to an inexperienced reader, this FQDN is mostly understandable as being the Google search page. As such, we might ignore the rest of the URL and simply trust it based on the domain or FQDN.

URL poisoning is a cyberattack method where attackers modify URLs to manipulate user behaviour or access unauthorized resources. By changing parameters, fragments, or domain names, attackers can redirect users to phishing sites, install malware, or steal sensitive information. This technique exploits the trust users place in familiar web addresses, making it difficult to detect and prevent.

A variation of URL poisoning is search engine poisoning, or SEO poisoning. Cybercriminals optimize their malware-laden pages to get them to the top of search engine results where users can only see the beginning of the URL and not the query strings.

How Does URL Poisoning Happen?

URL poisoning often begins with attackers identifying vulnerabilities or predictable patterns within web applications. By exploiting these weaknesses, attackers can modify URL parameters to bypass security mechanisms or inject malicious code.

For instance, if a URL carries user data or session information as part of its structure, altering these details might grant unauthorized access to service areas or confidential data. Attackers may employ social engineering tactics, sending doctored links under the guise of trusted sources. This manipulation may include altering path segments, query strings, or exploiting poorly configured URL shorteners, making their malicious intent hidden or seemingly benign.

Techniques such as URL encoding or obfuscation tools might also be used to disguise the true nature of the changes, leaving users unaware of the impending danger.

Contd...

Small URL Changes, Big Cybersecurity Impacts

Understanding URL poisoning and its implications is crucial for maintaining a secure online environment. By addressing vulnerabilities, businesses can protect their data, reputation, and customers from the damaging effects of URL manipulation

How URL Poisoning Impacts Your Business

URL poisoning via phishing inside email, SMS, or other messaging application is frequently used as the initial exploit to gain access inside of a larger attack campaign. As such, it can lead to severe consequences for businesses. It compromises user trust, damages brand reputation, and exposes sensitive information. Customers may fall victim to phishing attacks, leading to financial losses and identity theft. Furthermore, businesses may face legal repercussions and regulatory fines for failing to protect user data. The financial and reputational damage caused by compromises that are aided by URL poisoning can be devastating, underscoring the need for proactive measures.

Without proper awareness and defense mechanisms, businesses and individuals are left vulnerable to the myriad threats URL poisoning introduces.

URL redirection attacks can also be a form of URL poisoning. Sometimes, web applications are built as a redirect URL to collect user metrics with the real destination in a query string field. The user is then redirected on to the real destination. This is very common in marketing campaigns.

Examples of URL Poisoning

URL shortening services are widely used and very popular. Users can submit a URL and receive a shorter version that is easier to share in messaging applications. However, they use URL poisoning by design. When someone clicks on the shortened URL, the service redirects them to the original destination. However, recipients cannot determine the final destination from the shortened URL alone, which can allow malicious URLs to be concealed.

In a different scenario, an attacker registers a domain that closely resembles a well-known website. They then design a URL that appears authentic but directs unsuspecting users to a phishing page. By altering parameters, such as usernames or account numbers in URLs, attackers can access confidential user data or administrative controls.

Preventing URL Poisoning

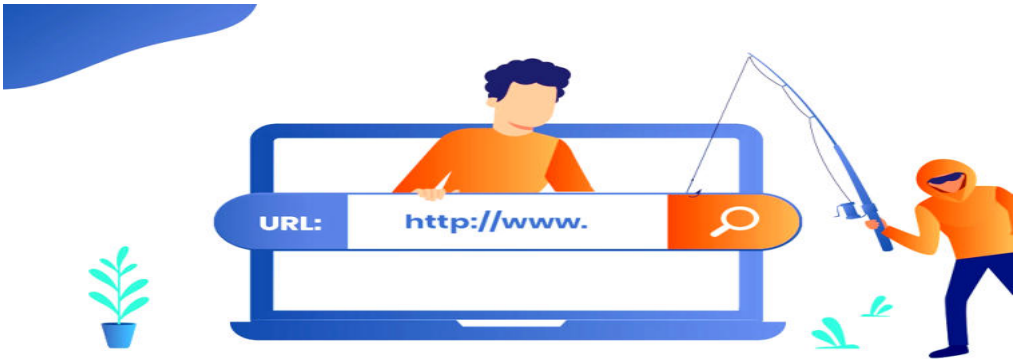
Preventing URL poisoning involves a comprehensive approach to web and messaging security.

Implementing Protective DNS (Domain Name System) is a robust strategy to safeguard against URL poisoning to protect endpoints such as desktops, laptops, and mobile devices. Protective DNS helps mitigate threats by filtering out malicious domains and preventing users from inadvertently connecting to harmful websites. This is accomplished by monitoring DNS queries and applying security policies in real-time, thereby thwarting access to potentially dangerous sites before any damage can occur.

It is essential to implement strong input validation and output encoding practices in web applications to ensure that URLs and the inputs inside of them are properly sanitized and cannot be altered or used in redirects. This reduces the risk that your web applications could be used in URL poisoning attacks.

Educating employees and users on the risks associated with URL manipulation is also vital. Encouraging vigilance when interacting with unfamiliar URLs or operating system popups can prevent potential threats.

By employing these strategies, organizations can significantly reduce the risk of URL poisoning



Cybersecurity Digest

Bi-Weekly Update by O/o CISO of Meghalaya Rural Bank

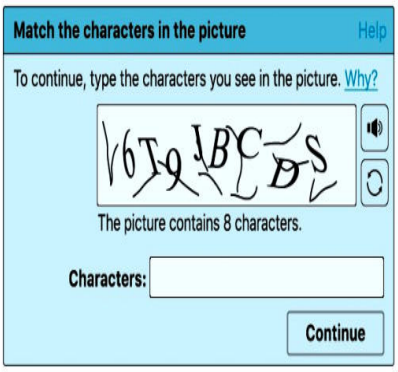
Volume 2 Issue 22

Date: 16-02-2026

CAPTCHA

A CAPTCHA test is designed to determine if an online user is really a human and not a bot. CAPTCHA is an acronym that stands for "**Completely Automated Public Turing test to tell Computers and Humans Apart.**" Users often encounter CAPTCHA and reCAPTCHA tests on the Internet. Such tests are one way of managing bot activity, although the approach has its drawbacks.

Although CAPTCHAs are designed to block automated bots, CAPTCHAs are themselves automated. They're programmed to pop up in certain places on a website, and they automatically pass or fail users.



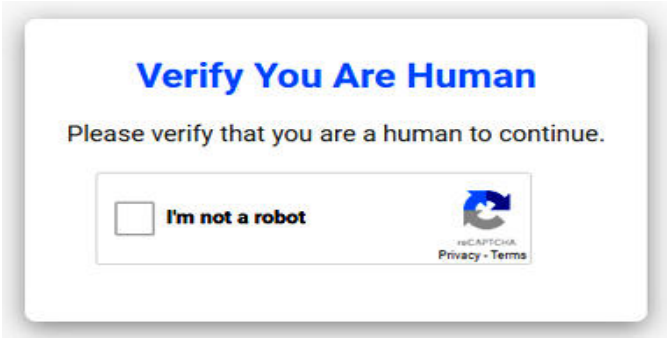
Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again.

Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.

The idea is that a computer program such as a bot will be unable to interpret the distorted letters, while a human being, who is used to seeing and interpreting letters in all kinds of contexts – different fonts, different handwritings, etc. – will usually be able to identify them.

CAPTCHA ATTACK

Fake CAPTCHA attacks often begin with deceptive emails containing malicious links, misleading social media ads leading to fraudulent websites, compromised links on legitimate sites, or manipulated search engine results, and then the user is presented with a CAPTCHA, such as the one below.



Once users engage with the fake CAPTCHA, they may be prompted to copy and paste commands that seem harmless, but these can utilize PowerShell to run scripts in the background and execute malicious code, compromising their systems. Awareness of these tactics is vital for maintaining online security and avoiding these sophisticated attacks.

Socially engineered

The attack leverages our inherent trust in CAPTCHA challenges, exploiting the widespread assumption that CAPTCHAs are a security measure designed to protect us. This familiarity can lead people to let their guard down, blindly following instructions without critically evaluating the situation. Attackers also use tricks like adding harmless-looking text at the start of the command to hide the real code that does the damage

How to Spot Fake CAPTCHA

This is the classic CAPTCHA widget you've probably checked hundreds of times. But beware – a fake version may look identical. At first glance, the fake CAPTCHA may look identical to the real thing, and you'll be asked to check a box and confirm you're not a robot, just like you would with a legitimate CAPTCHA. But once you click through, instead of being presented with a challenge like identifying distorted text or selecting images, you'll be instructed to copy and paste a command into the Run dialog or a Command terminal; That's when you know you're dealing with a fake, as shown in fig.1.

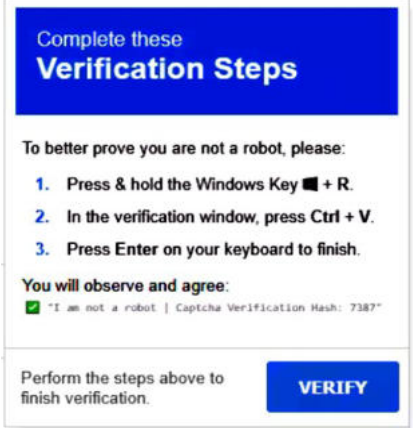


Fig. 1

Legitimate CAPTCHAs will never ask you to copy and paste commands, and if you do, you'll be executing a harmful command that could compromise your machine's security. The fake CAPTCHA wants to appear legitimate by showing you a preview of the command that you are being instructed to copy and paste, but this is a ruse. The real command being executed is obfuscated and is actually malicious, and may be hidden from view outside of the text field (as seen in fig.2, where the command appears to be a harmless verification ID).

As seen in fig.2, if the user pastes the command into the Run dialog and clicks OK, the malicious command is executed, potentially allowing attackers to access and control the user's system, install malware, or steal sensitive information, often without the user's knowledge or visible indication of compromise .

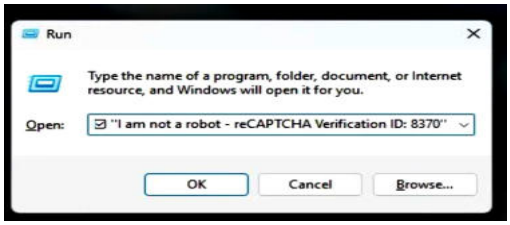


Fig. 2

Key Takeaways

Here are some ways to protect yourself:

- **Be aware of the Fake CAPTCHA technique:** Fake CAPTCHAs exploit trust of a familiar interface.
- **Never copy and paste commands from a website.** Legitimate verification processes will never ask you to run code on your computer.
- **Be wary of prompts to open Run or PowerShell:** These are not normal actions for everyday tasks, and could be a sign of a security threat.

What To Do If You're Affected

If you think you may have followed these steps and pasted a malicious command:

1. **Disconnect from the internet:** Immediately disconnect your device from the internet to prevent further communication with the attacker's server.
2. **Do not continue using the device** until it has been checked by your departmental IT staff.
3. **Notify your departmental IT staff or contact IT Helpdesk** to report the incident. Provide as much detail as you can about what happened.

Date : 01.03.2026

Vol 2 Issue 23

MEGHALAYA RURAL BANK

Cybersecurity Digest

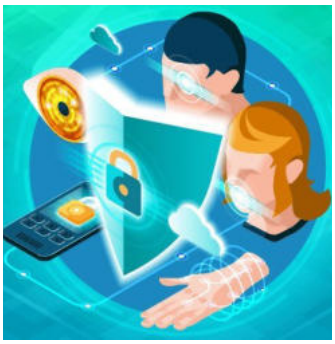
Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

Claude Code Security

Claude Code Security is an AI-assisted vulnerability detection system embedded within Claude Code, an AI programming assistant developed by Anthropic. The core idea is to use AI reasoning rather than traditional pattern matching to scan codebases and surface potential security flaws that could be exploited in software applications.

Unlike conventional static analysis or signature-based scanners that look for known patterns of insecure code, Claude Code Security uses large language models to reason about how data flows through a codebase and how different parts of a program interact. This can help in identifying more complex issues such as logic errors, insecure data handling and configuration weaknesses

AI Based-Biometric Scam



A new tactic by cybercriminals has emerged where fraudsters are targeting not only financial assets but also citizens' biometric identity data. Experts have warned that AI-based biometric scams are spreading rapidly, with criminals attempting to steal sensitive identity information such as facial and voice data.

Fraudsters often approach people in crowded public places such as malls, metro stations, or markets. They may pretend to need help and request mobile phones under the pretext of checking pension status, government benefits, or technical settings in an app. During such interactions, the victim's photograph, voice, or other biometric data may be secretly recorded.

In some cases, criminals may use video calls or screen recording techniques to capture biometric information. If a person unknowingly grants camera or microphone permissions, biometric data can be stolen within seconds.

The stolen biometric data can be used to create AI-generated fake identities. Criminals may conduct social engineering attacks and attempt to bypass verification systems by generating synthetic voice or facial imitations. Such misuse of technology is increasingly associated with financial fraud and identity theft.

Security experts advise citizens not to hand over their mobile phones to unknown persons and to avoid keeping their face visible for long periods during unknown video calls. In crowded places, people should remain cautious if strangers ask for quick assistance and avoid sharing screen or camera access.

Parents are also advised to educate children and elderly family members about such cyber threats, as criminals often target individuals who are less familiar with digital security practices.

Cybersecurity specialists believe that biometric data theft cases may increase in the future as deepfake technology is being misused. Fraudsters can generate fake videos and voices to deceive people using advanced AI tools.

Citizens are advised to disable unnecessary app permissions on their mobile devices and immediately report suspicious activities to cyber helpline numbers. Special caution is recommended during digital interactions with strangers in public spaces.

Experts say that biometric data protection is no longer limited to financial security but has become an essential part of personal safety. Awareness and vigilance are considered the most effective measures to prevent such emerging digital threats.

Deepfakes and Digital Safety: A Citizen's Guide to AI Scams

Introduction: The Double-Edged Sword of AI

India is one of the world's fastest-growing digital economies. While AI is driving progress in healthcare and agriculture, it has also given rise to a new breed of cybercrime: Synthetic Media Fraud, commonly known as "Deepfakes."

Deepfakes are realistic-looking images, videos, or audio recordings created by AI algorithms. Scammers use these to impersonate family members, bank officials, or government authorities. To stay safe in the Digital India era, every citizen must practice "Cyber Hygiene."

The "Voice Clone" Scam (The Emergency Call)

The Threat: Scammers can now clone a person's voice using just 3 to 10 seconds of audio taken from social media (Instagram Reels or Facebook videos). They use this AI-generated voice to call parents or spouses, claiming to be in an emergency (kidnapping, accident, or arrest) and demanding an immediate money transfer.

How to Spot It:

- **Urgency:** The caller will always demand immediate action to panic you.
- **Audio Quality:** Listen for robotic pauses or unnatural background noise

The "Family Password" Defense:

- **Action:** Establish a secret "Code Word" with your family members today.
- If you receive a distress call from a loved one, ask for the code word. An AI bot cannot know your family secret.
- Always disconnect and call the person's original mobile number to verify.

Video KYC and Deepfake Calls

The Threat: With the rise of Video-KYC for banking, fraudsters use Deepfake videos to impersonate bank officials or law enforcement officers. They may claim your account is "blocked" and ask you to reveal OTPs over a video call.

How to Spot a Deepfake Video:

- **Unnatural Blinking:** AI models often struggle to replicate natural eye blinking patterns.
- **Blurry Edges:** Look at the edges of the face or hair; deepfakes often look "glitchy" or blurry around the borders.

The "Hand Wave" Test:

- **Action:** If you suspect a video caller is fake, ask them to wave their hand in front of their face or turn their head side-to-side.
- Deepfake filters usually "break" or glitch when an object (like a hand) passes over the face.

The "Zero Trust" Rule for UPI & Aadhaar

AI can automate attacks, but it cannot bypass the fundamental rules of banking if users are alert.

A. UPI Safety (The Golden Rule)

- **Fact:** You never need to enter your UPI PIN to receive money.
- If a caller asks you to scan a QR code or enter a PIN to "receive a refund" or "win a prize," it is 100% a scam.

B. Aadhaar Biometric Lock

- **Fact:** Scammers use silicon fingerprints to breach Aadhaar-enabled Payment Systems (AePS).
- **Action:** Download the official **mAadhaar App** or visit the UIDAI website and enable "**Biometric Lock**". Unlock it only when you need to perform a verification. This creates a hard shield against identity theft.

SANCHAR SAATHI

The Government of India has launched specific portals to help citizens fight these threats:

Sanchar Saathi (Chakshu Facility): *Visit* ***sancharsaathi.gov.in to report suspected fraud communications (calls or SMS) received on your mobile.***

CyberCrime.gov.in: ***Use this portal or dial 1930 immediately if you have lost money to a financial scam. The "Golden Hour"*** *(reporting within 1 hour) increases the chances of recovering lost funds.*

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

MEGHALAYA RURAL BANK

Vol 2 Issue 24
Date: 16-03-2026

Cybersecurity is a shared responsibility

Risks associated with inadequate cybersecurity measures:

1. Reputational Damage
2. Data Breaches
3. Financial Losses
4. Disruption of Business Operations
5. Legal and Regulatory Consequences

Data Breach

A data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information).

The terms "data breach" and "breach" are often used interchangeably with "cyberattack." However, not all cyberattacks are data breaches. Data breaches include only those security breaches where someone gains unauthorized access to data.

For example, a distributed denial of service (DDoS) attack that overwhelms a website is not a data breach. A ransomware attack that locks up a company's customer data and threatens to

leak the stolen data unless the company pays a ransom is a data breach. The physical theft of hard drives, USB flash drives or even paper files containing sensitive information is also a data breach.

Why data breaches happen

Data breaches are caused by:

- **Innocent mistakes**, such as an employee emailing confidential information to the wrong person.
- **Malicious insiders**, including angry or laid-off employees who want to hurt the company or cause reputational damage, and greedy employees who want to profit off the company's data.
- **Hackers**, malicious outsiders who commit intentional cybercrimes to steal data. Hackers can act as lone operators or part of an organized ring.

Financial gain is the primary motivation for most malicious data breaches. Hackers steal credit card numbers, bank accounts or other financial information to directly drain funds from people and companies.

Some attackers steal personally identifiable information (PII)—such as Social Security numbers and phone numbers—for identity theft, taking out loans and opening credit cards in their victims' names. Cybercriminals can also sell stolen PII and account information on the dark web, where they can fetch as much as USD 500 for bank login credentials.

A data breach can also be the first phase of a larger attack. For example, hackers might steal the email account passwords of corporate executives and use those accounts to conduct business email compromise scams.

Data breaches might have objectives other than personal enrichment. Unscrupulous organizations might steal trade secrets from competitors, and nation-state actors might breach government systems to steal information about sensitive political dealings, military operations or national infrastructure.

How data breaches happen

Most intentional data breaches caused by internal or external threat actors follow the same basic pattern:

1. **Research**: The threat actor identifies a target and looks for weaknesses that they can use to break into the target's system. These weaknesses can be technical, such as inadequate security controls, or human, such as employees susceptible to social engineering.
2. **Attack**: The threat actor starts an attack on the target by using their chosen method. The attacker might send a spear-phishing email, directly exploit vulnerabilities in the system, use stolen login credentials to take over an account or leverage other common data breach attack vectors.
3. **Compromise data**: Inside the system, the attacker locates the data they want and does what they came to do. Common tactics include exfiltrating data for sale or use, destroying the data or locking up data to demand a ransom.

Data breach prevention and mitigation

According to the *Cost of a Data Breach 2025* report, it takes an average of 241 days to identify and contain an active breach across all industries. Deploying the right security solutions can help organizations detect and respond to these breaches faster.

Standard risk management measures, such as regular vulnerability assessments, scheduled backups, timely patching and proper database configurations, can help prevent some breaches and soften the blow of those that occur.

However, many organizations today implement more advanced controls and best practices to stop more breaches and significantly mitigate the damage they cause.

Data security tools

Organizations can deploy specialized data security solutions to automatically discover and classify sensitive data, apply encryption and other protections and gain real-time insight into data usage.

AI and Automation

Organizations that extensively integrate artificial intelligence (AI) and automation into security operations resolve breaches 80 days faster than those that don't, according to the *Cost of a Data Breach 2025* report. The report also found that security AI and automation reduce the cost of an average breach by USD 1.9 million or a savings of over 34% (as compared to organizations that don't use security AI and automation).

Many data security, data loss prevention and identity and access management tools now incorporate AI and automation.

Employee training

Because social engineering and phishing attacks are leading causes of breaches, training employees to recognize and avoid these attacks can reduce a company's risk of a data breach. In addition, training employees to handle data properly can help prevent accidental data breaches and data leaks.

Identity and access management (IAM)

Password managers, two-factor authentication (2FA) or multifactor authentication (MFA), single sign-on (SSO) and other identity and access management (IAM) tools can protect employee accounts, VPNs and credentials from theft.

Organizations can also enforce role-based access controls and the principle of least privilege to limit employee access to only the data that they need for their roles. These policies can help stop both insider threats and hackers who hijack legitimate accounts.