



Cybersecurity Digest

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

Date: 16-01-2025

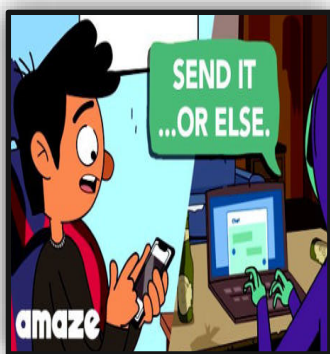
Volume 1, Issue 9

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 fil-

ters 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 send-



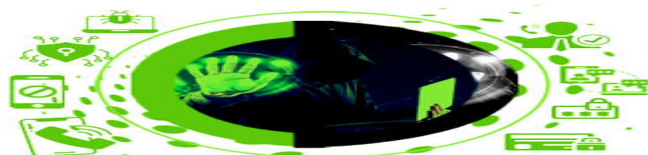
Spam Traps

er's reputation and email deliverability. Spam traps can cause the sender's domain list or Internet Protocol (IP) address to be denied.

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