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.

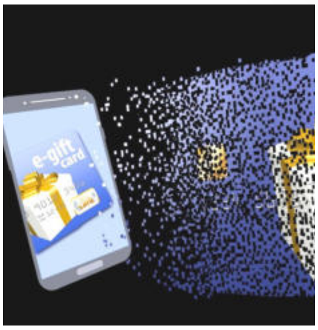
Buying and Using Gift Cards

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.