FINANCIAL FRAUD consortium

Industry Insight

Protecting Your Employees From Rising Gift Card Scams

Gift card scams have been ongoing for a decade. However, with the rise in remote working, growing technology usage in business settings, many people fearful of COVID-19, and growing financial strain with a recession looming, scammers are ever ready to take advantage of you or your employees.

Photo by Blake Wisz

What Are Gift Card Scams and How Do They Work?

Gift card scams involve a person (or group of people) impersonating another employee, or a third-party company or organization they are not part of in an email or text message. Typically, they will make representations for the purpose of creating a sense of authority, trust and urgency. For example, a scammer may say you need to act immediately because your boss needs you to do this, you have hackers on your PC, this offer is only available for a short time, or you have committed tax fraud and will go to jail if you don't do X. Some employees, anxious to please, too busy to be skeptical, or not very risk adverse, may be more vulnerable than others.

The gift card part of the scam involves the scammer telling the employee that it must buy $X in gift cards, scan them, and email a copy back to the scammer. In some cases, the scammer will take a step further, asking for information that would enable them to gain access to the employee's computer or asking them to click a link to complete the process. As we all know, once the scammer has acquired the gift card codes from the employee, they will immediately deplete the gift card funds or sell the gift cards on a third-party marketplace, typically at a discounted value off of the retail value. If the scammer gains access to the employer's access credentials, scammers may remotely connect to the employee's computer to spy on them, delete important files, lock someone out of their computer via syskey, and/or steal personal information. If workers fall victim to a scam of this nature, they could end up compromising the entire company.

How To Protect Yourself From Gift Card Scams

First, beware of suspicious communications, e.g., emails and texts from outside the organization, from someone you don't know, or that require an urgent response, you to buy something and send it to the emailer, or require information from you that you typically would provide to anyone except a trusted person.

Connect with the Financial Fraud Consortium:
info@fraudconsortium.org
(405) 676-1067

How To Protect Yourself From Gift Card Scams

If you receive a suspicious communication,

- Confirm that the email address appears to be accurate, e.g., check the “from” email address for suspicious domain names that may be close to your company's email but may be off by one letter, have an extra dot, switched .com to .net, etc.
- Read the communication to look for spelling, grammatical, and formatting errors;
- If you receive any urgent-sounding or suspicious requests, or a communication from someone you don’t know and that is unexpected, always contact the IT Department directly to verify it is a legitimate communication;
- If the communication is from outside of your company, scrutinize it even more carefully;
- Do not click on any links when you receive messages. Instead, go directly to the website to see if it appears legitimate;
- If you log into a website, do it from the website not from a link provided;
- Never give your sensitive information via email or over the phone, including your social security number, credit card details, gift card details and so on;
- Remember that your employer generally will not ask you to pay for something out of your own monies, especially an expensive purchase; and
- Remember that government agencies don’t send text messages or emails to alert you to an issue.

Understand that all communication channels may be subject to spam messages, including (but not limited to) your work phone and business email.

What To Do When You Get a Scam Call or Message

If you have already given away your information or clicked on a link, contact your IT Department and, if it involves your financial information, contact your bank, credit card company, and finance department to freeze and cancel any cards that may have been compromised. If you find out that you’ve been subjected to a scam that may affect your employer (for example, if you were contacted via a work phone or email), it’s important to let your employer know so they can take action.

Employers can contact us, the Financial Fraud Consortium, for help with fraud intervention and recovery resources and education.

Conclusion

Scammers are constantly adapting their processes based on the political, financial, or social climate to prey on individuals at any level. It can feel overwhelming to keep up with these types of scams to protect your employer and its employees.

If you or your employer want to learn about different types of financial fraud, consider a membership with the Financial Fraud Consortium and join our growing membership base! Each tier of membership provides growing value including access to closed webinars, white papers, alerts, and member-specific communication.

Connect with the Financial Fraud Consortium:
info@fraudconsortium.org
(405) 676-1067