McGriff | Executive Risk Advisors
Client Advisory

September 2022

Social Engineering Attacks are on the Rise

98% of cyber attacks involve some form of social engineering.[1] A disturbing social engineering trend is the rise in threat actors impersonating a client or vendor in an attempt to bypass organizational controls to obtain sensitive information or steal funds. One of the most common ploys occurs when criminals email an Insured advising that future payments should be made to a new bank account.

In one of our recent cases reported to McGriff, an Insured was tricked into sending about $1.5 million to a fraudulent account. After the Insured called our Claims Team, we helped them obtain reimbursement from the insurance company, according to the terms of their policy. Having the right policy and coverage in place is key to a prompt recovery from an incident like this.

What is Social Engineering?

Kroll, an international cyber risk consulting firm, describes social engineering as a security incident whereby malicious actors attempt to win the trust of a potential victim to exploit them for sensitive information, or a large sum of money.

Telltale Signs

Threat actors use many different manipulation tactics to trick victims into providing sensitive information. Here are a few:

- A warning that induces fear or concern about an item/situation
- An unexpected request for personal information from a seemingly trusted source
- A sense of urgency or time sensitivity
- An attempt to appear official by providing information under the guise of authority that ultimately cannot be verified

Examples of Social Engineering Methods

Types of social engineering include:

- Smishing and vishing are two types of fraud that use SMS (smishing) and voice (vishing) to trick people into giving up money or personal information. Baiting, where a scammer uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware.
- Whaling, a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email. Whaling is digitally enabled fraud through social engineering, designed to encourage victims to perform a secondary action, such as initiating a wire transfer of funds.
- Spoofing, a type of scam in which a criminal disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source.
- Pretexting, a certain type of social engineering technique that manipulates victims into divulging information. A pretext is a made-up scenario developed by threat actors for the purpose of stealing a victim's personal data.
- Business Email Compromise (BEC)—also known as email account compromise (EAC) is one of the most financially damaging online crimes. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request.

A whopping 90% of data breaches take place because of phishing, according to the CISCO 2021 Cybersecurity Threat Trends report.

A report from the Anti-Phishing Working Group recorded 1,025,968 phishing attacks for the first quarter of 2022. That was a 15% increase (137,383) from the 888,585 attacks in the fourth quarter of 2021.[2] According to the FBI, phishing attacks are now rising by 400% a year.[3]

(continued)

Insurance Protection

Since both money and confidential data or systems are at play, social engineering fraud coverage is available as a part of both cyber and crime policies.

Insurance should be a major part of your company's defense strategy against social engineering fraud. Both cyber and crime coverages could provide protection for social engineering fraud. Be sure to discuss social engineering fraud coverage with your McGriff producer.

How to Protect Against Social Engineering Fraud

There are several best practices to help protect your organization and employees against social engineering fraud schemes, including:

- **Train your staff.** With ongoing training your employees should be able to identify social engineering attacks and take the following steps to mitigate risk:
  - Stay alert when receiving texts or phone calls from a random number. Avoid clicking on links.
  - Check phone numbers from the actual store, bank, or delivery website. In addition, verify a suspicious caller by hanging up and calling a number from the website of the supposed organization.
  - Address questions or concerns regarding orders or deliveries by calling the phone number on the company website or an order confirmation email.
- **Implement internal controls**. For example, consider a policy whereby multiple employees must verify and authorize the transfer.
- **Vet your vendors**. Thoroughly vet any vendors or partners to ensure their security protocols are up to date.
- **Restrict access to sensitive data**. By limiting the number of employees at your company who have access to certain files, you'll be reducing the risk of that data being compromised.

Ten Essential Security Controls

Kroll evaluated dozens of questionnaires requested by cyber insurance carriers and compiled a list of the most essential security controls for improving your organization's security. You can view this list here.

Has Your Company Been Compromised?

Take immediate action:

- Immediately contact the originating bank and request a recall of the transfer if a wire is involved;
- Through your legal team, you might need to file a complaint with the FBI at www.ic3.gov. This reporting triggers the FBI's Recovery Asset Team.
- Preserve records of the incident, including emails sent and received in their original electronic state. Correspondence and forensic information contained in these electronic files help investigators find the perpetrator(s), and parties who may be responsible for the incident.
- Contact your McGriff broker for assistance filing a claim with your insurance carrier as per the terms of your policy.
- You might need to conduct a forensic investigation to determine the root cause and ensure your systems are safe.

Conclusion

70% to 90% of malicious data breaches involve social engineering and this trend will remain.[4] Threat actors continue to update their tactics to trick unsuspecting victims, so it's important to stay vigilant and safeguard your information. If you believe your company is the victim of a social engineering attack or for any questions regarding coverage and/or available policies, please contact your McGriff broker.

McGriff

Executive Risk Advisors

Client Advisory

September 2022

If you have questions about this advisory or cyber insurance, please contact:

Natalie Santiago, JD
Sr. Vice President, Claims Manager
McGriff Executive Risk Advisors
NSantiago@McGriff.com
(713) 402-1410

Suzanne Gladle, ARM
Sr. Vice President, Cyber Insurance Practice Leader
McGriff Executive Risk Advisors
SGladle@McGriff.com
(315) 750-6010

For more general cybersecurity information from Kroll, visit http://kroll.com/cyberblog or contact:

Cristin Sinnott
Vice President, Cyber Risk
Kroll, LLC
55 East 52nd Street
New York, NY 10055
cristin.sinnott@kroll.com
(212) 833-3373

www.McGriff.com

[1] https://purplesec.us/resources/cyber-security-statistics/

[2] https://apwg.org/apwg-1q-2022-phishing-reaches-record-high-apwg-observes-one-million-attacks-within-the-quarter-for-the-first-time-in-the-first-quarter-of-2022)

[3] https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

[4] https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks