AmWINS Group, Inc.

UNDERSTANDING SOCIAL ENGINEERING SCHEMES TO MITIGATE RISKS

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker.

LEGAL DISCLAIMER

Courtesy of AmWINS Group, Inc.

ABOUT THE AUTHOR

This article as co-authored by Lisa Block, vice president and national commercial crime product manager for AXIS Insurance Company, and Scott Schmookler, Esq, a partner in the Chicago office of Gordon Rees Scully Manuskhani, LLP. Scott counsels clients on insurance issues relating to commercial crime policies, cyber crime, and data breaches.

ON YOUR TEAM.

In part one of our series on Social Engineering, we discussed how cyber criminals have shifted their focus away from pure technological attacks to attacking employees through the use of social engineering, a collection of techniques used to manipulate people into performing actions or divulging confidential information. We also reviewed recent court rulings to illustrate that computer fraud and funds transfer insuring agreements in traditional crime policies may not provide coverage in the event of a social engineering claim.

In the second part of our series, we identify examples of schemes employed by social engineers and how to design and implement comprehensive security practices to mitigate the risk of a loss.

SOCIAL ENGINEERS PREY ON INNATE HUMAN EMOTIONS

Social engineers use technology to swindle people and manipulate them into disclosing passwords, revealing banking information or granting access to their computer. Understanding how these social engineers work and the schemes that they employ is key to implementing successful internal controls that minimize risk.

The success of social engineering schemes does not always rely upon sophisticated software or hacking technology. Social engineers exploit human emotions – such as fear, curiosity, the natural desire to help, the tendency to trust, and laziness – to bypass the most iron-clad security measures. Social engineering schemes, therefore, remain one of the most foolproof and commonly used methods to breach secure systems.

In the cyber world, the weakest link in the security chain is the employee who accepts a person or scenario at face value. Social engineers target this vulnerability. A few common examples illustrate how social engineers take advantage of human emotion.

Messages from Trustworthy Sources:

Social engineers cleverly manipulate the natural human tendency to trust and accept representations at face value. Human nature is to trust others until they prove that they are not trustworthy. If someone tells us that they are a certain person, we usually accept that statement.

Seizing upon this trait, cyber criminals commonly hack email accounts to gain access to the owner's contact list. Once access to an email account has been obtained, the cyber criminal can send messages to all the owner's contacts. These messages prey on trust and curiosity. For example, the social engineer may send:

(continued on next page)

(continued from previous page)

- A link that you "just have to check out." Because the link comes from a friend, and humans are naturally curious, the recipient is likely to click on the link. As a result, the system becomes infected with malware that the criminal can use to take over the machine and collect information.
- A file to download (disguised as pictures, music, movie, document, etc.) that is embedded with malicious software. Once downloaded, the system is infected. Now, the criminal has access to the system.

Phishing Schemes:

Phishers seize on fear and gullibility to obtain private information. Phishers send e-mails, instant messages, or text messages that appear to derive from a legitimate or popular company, bank, school, or institution. These messages explain that there is a problem that requires you to "verify" information by clicking on the displayed link and entering information into a form. The link location may look legitimate (often containing the correct logos and content copied from a legitimate website). The spoofed site closely resembles a legitimate site and tricks the user into entering his credentials, thereby enabling the social engineer to implant malicious programs or spy on the user's computer activity.

Baiting scenarios:

Social engineers also use greed to manipulate human operators. Often found on peer-to-peer sites offering a download of a hot new movie or music, social engineers dangle something people want and wait for people to take the bait. Once people take the bait, the cyber criminal uses malicious software to corrupt secure systems and steal confidential information or banking details.

Impersonating Superiors:

Impersonation is one of the most common social engineering techniques. Impersonation can occur over the phone or online. For example, a social engineer may obtain the name of someone in the organization who has the authority to grant access to confidential information. Using that information, they call the target and claim that a senior official authorized the disclosure of information or transmission of funds. Similarly, a social engineer may impersonate a network administrator or help desk member and ask an employee for his/her username and password (so they can ostensibly troubleshoot a network problem and/or trace a problem).

These schemes prey upon the desire to be helpful and fear of being reprimanded. Many employees receive a negative reaction from superiors if they do not act promptly and/or take too long to complete a project. Fearing reprimand, many employees want to be helpful and follow directions – which can lead to giving away too much information.

GUARDING AGAINST SOCIAL ENGINEERING

Social engineering is one of the most difficult crimes to prevent, as it cannot be defended against through hardware or software. In order to build defenses against social engineering attacks, organizations need to design and implement comprehensive security practices:

- **Risk Assessment:** A risk assessment helps management understand risk factors that may adversely affect the company and track existing (and upcoming) threats. Determining security risks helps enterprises to build defenses against them.
- **Policies and Procedures:** Policies and procedures must be clear and concise. They should be aimed toward mitigating social engineering attacks. Well-defined policies and procedures provide guidelines for employees on how to go about protecting company resources from a potential cyber attack. Strong policies should address proper password management, access control, and handling of sensitive user information.

(continued on next page)

(continued from previous page)

- **Security Incident Management:** When a social engineering event occurs, a company must have a written, comprehensive protocol for managing such incidents. To manage the incident, the help desk must be trained to track (among other things) the target, their department, and nature of the scheme. Such protocols will enable a company to actively manage the risk of the breach to mitigate potential losses.*(continued on next page)*
- **Training Programs:** Companies should invest in security training programs and update their employees on security threats. Because companies are composed of various departments, training and awareness must be customized to the needs and requirements of each department. Such practices help employees recognize and handle security attacks effectively.

Despite the best vendor background screenings, fraud detection systems, segregation of duties, and education, companies still face an uncertain risk of loss from social engineering schemes. As a result, strong consideration should be given to purchasing coverage tailored to social engineering risks.

The Professional Lines specialists at AmWINS, in partnership with AXIS Insurance Company, a leading Crime insurance carrier, have developed a solution specifically tailored to address losses from social engineering attacks. In recognition of the fact that a client's cost of risk includes more than just the insurance premium, the AmWINS Social Engineering Crime solution provides free social engineering training for employees, as well as a significant discount for advanced training from KnowBe4, the world's largest security awareness training provider. Avoiding a loss through proper training is more cost effective and less disruptive to a business than insurance alone.