Risk Control

Social Engineering Fraud – Exploiting the Psychology of the Pandemic

The COVID-19 pandemic has had a profound impact on daily life. The way people work has changed considerably, with many employees logging in remotely instead of working in a physical workspace. In fact, by April more than 50% of employees in the U.S. were working remotely.[1] Unfortunately, the pivot to remote work wasn't the result of a careful plan. Rather, it was done hastily in response to COVID-19, and many employers might not have had the time to ensure that sufficient protocols were in place to protect against cybercrime. Although the pandemic has stopped many things, it has not stopped cybercriminals from exploiting the situation.

Increase in Social Engineering Schemes During the Pandemic

"Coinciding with the increase in remote working during the second quarter, … global data has shown employees have been more likely to fall for social engineering scams, with organizations in the middle market most likely to be victimized."[2] There has been a substantial increase in cybercrime during the pandemic, and social engineering is one method of fraud which has rapidly increased. In these schemes, the fraudster intentionally misleads an employee by using a communication that purports to be from someone such as a client, vendor, employee or owner, but is actually from the fraudster. Social engineering schemes try to manipulate employees with fraudulent telephone calls, email, text messages, social media posts and other internet resources to convince those employees to divulge confidential information, send money or otherwise disregard security protocols. Sometimes, the perpetrator even gains access to the company's systems.

For example, a perpetrator might pose as a vendor with which the company does business, sending an email to an employee which appears to be from the actual vendor and uses an email address nearly identical to one known and trusted by the victim, complete with the vendor's logo. The email states that it is "urgent" that money be wired to the vendor for goods that were purchased and received by the company. The email instructs the recipient to send the money immediately to a new account in order to keep the vendor's business afloat during the pandemic. Because of the urgency and time sensitivity conveyed in the email, as well as the fact that the employee is working remotely, it may be difficult for the employee to contact someone to verify the transaction. The fraudster preys on this heightened sense of urgency, fear and isolation. The employee, believing they are doing the right thing, bypasses security protocols and wires the money to the new account. Unbeknownst to the employee, the money goes to the fraudster's account, not the vendor's.

[1] COVID-19 and Remote Work: An Update, 10/13/20, at https://news.gallup.com/poll/321800/covid-remote-work-update.aspx

[2] Attacks on Mid-Markets Soar, https://www.infosecurity-magazine.com/news/attacks-on-midmarket-organizations/. Middle market is defined as over $35 million in annual revenue.

A real-world example of a COVID-19 scam occurred when a company employee received an email, allegedly from the CEO of another company, about a previously scheduled $1 million transfer. The fraudster's email address was identical to the CEO's actual email address, except for one changed letter. The email requested that the transfer be made at an earlier date and that it be made to a different account "due to the Coronavirus outbreak and quarantine processes and precautions."[3]

If hackers gain access to company email systems, they might issue an internal email, supposedly from an executive, instructing a subordinate employee to wire money, make a payment, or make a purchase. If the fraudsters cannot access the company's internal email systems, they might create an email that appears to be from an internal company source to perpetuate the fraud. Recent social engineering schemes have been "linked to demand for personal protective equipment (PPE) such as masks, particularly through fake stores, fake 'cures' or telephone scams that are a variation of medical injury scams where family members are said to be unwell and requiring funds to pay for treatment."[4]

Mitigating the Risk of Social Engineering

Social engineering schemes are dangerous and difficult to prevent. This is especially true during a pandemic when the majority of employees are working remotely. However, there are steps that a company can take to help mitigate the risk:

1. Continually train employees regarding social engineering schemes.
   - Train employees to be able to distinguish between a fraudulent, targeted phishing email and a legitimate email, and provide clear instructions for what they should do if they suspect an email is fraudulent.
   - Train employees to avoid clicking on links from unknown senders or that appear suspicious.
2. Implement multifactor authentication for computer systems. This helps to protect computer systems from remote attacks, even if access credentials have been stolen, by providing an additional layer of security.
3. Consider using a spam filter to detect and divert suspicious emails.
4. Establish strong vendor and customers controls.
   - Maintain a master list of all approved vendors and customers.
   - Consider limiting the number of employees who are able to transfer money, make purchases or payments and change customer or vendor accounts.
   - Create policies and procedures to verify the receipt of inventory, supplies, goods or services against an invoice prior to making payment to a vendor.
   - Confirm all money transfers and requests to change vendor and customer account information by a direct call to the vendor or customer using only an authenticated phone number previously provided by the vendor before the transfer or change request was received.
   - Confirm that an individual representative is affiliated with the company by using an independent means other than the contact information provided by the representative, such as contacting another individual at the company.
   - Consider providing, in advance, a code specific to the customer or vendor, which must be provided to effectuate money transfers or account changes.
   - In order to ensure that an email sender is who they purport to be, consider typing the name of the recipient of an email instead of hitting "reply."
   - Be skeptical of last minute changes in wiring instructions or recipient account information.[5]

The Right Insurance Coverage for Your Business

Because social engineering crimes may involve the release of company funds by a person within your company, standard liability policies may not cover your losses. Your policy should explicitly state coverage for social engineering – if it doesn't, your claim may not be covered.

Even a business with thorough preventative protocols can fall victim to social engineering fraud. To help protect your company against these scams, talk with your insurance agent or broker to ensure that your business has the right insurance coverage for this exposure.

[3] Federal Bureau of Investigation (FBI), COVID-19 Fraud Law Enforcement's Response to Those Exploiting the Pandemic, 6/9/20 at https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic

[4] BCOVID-19 and the effects on Fraud Prevention - Part 3 - Social Engineering, FinExtra blog at https://www.finextra.com/blogposting/19475/covid-19-and-the-effects-on-fraud-prevention---part-3---social-engineering

[5] For more resources regarding the mitigation of social engineering and other forms of cybercrime while telecommuting, see https://www.cna.com/web/user/cna/about/listofauthors/authorbio/blogdetails/SA-Dominic-Senese/CT-Protect-Your-Business-Social-Engineering-Scams and https://www.cna.com/web/guest/cna/about/listofauthors/authorbio/blogdetails/SA-Author2/managing-a-remote-workforce?