Social Engineering's Attack On Your Business

Nowadays every company has some sort of cyber and crime exposure. And it's no longer a matter of if, but rather when. In November 2017, the FBI noted a 2,370% increase in such incidents in the last two years and more than $5 billion in related losses over the last four years worldwide." The increasing prevalence of "social engineering" or "business email compromise" schemes has forced courts to answer this question: "Is a financial loss connected to an email "spoof" covered by standard Computer Fraud or Funds Transfer Fraud insuring clauses found in commercial crime policies or financial institution bonds?"

Social engineering is a method of tricking people into giving out sensitive and personal information such as passwords and other credentials in order to gain access to the computer systems. Here are the most common social engineering techniques used:

- Phishing is the most common social engineering technique used by cybercriminals today. Phishing uses a fake email from a third party the victim would trust to trick them into providing sensitive information. The email appears to be their bank or Paypal for example, asking them to log in to the website. The reasons are varied. You could be told that your account was compromised and you need to update your password; or that the bank is updating its privacy policy and you need to log in to confirm that you agree. Once the login is complete, the hacker receives the credentials and you've been socially engineered!

  Another familiar way method is sending a fake message from a "friend," "coworker" or a person you might trust. This message will ask you to open an attachment. Once you opened the attachment or clicked on the link, malware finds its way into your computer system and now your computer data is at the mercy of the hacker.

- Vishing is like phishing, just over the phone. One scam that has been used for several years is from a hacker posing as Microsoft solutions architect. The hacker calls a business's employee informing them "their computer has been infected with a virus." The employee is directed to download software from "Microsoft's" website to fix the situation. The unsuspecting employee doesn't know that she is really downloading a malware.

- Pretexting is yet another technique that is similar to phishing. Where phishing preys on the victim's fear or urgency to do something, pretexting capitalizes on human's desire to trust. The hacker builds a false sense of security and trust with their victim. Pretexting scam requires a lot of research on the part of a scammer, concocting a story that leaves little doubt that it's safe to give them the information requested.

  "For example, a scammer will exploit the fact that employees from different locations don't know employees from other locations. The 'employee' says they are CFO's assistant. They have the right story, say all the right words, know all the right facts about the CFO and the company. You have no reason to not believe them" and "might not think twice about providing them the financial reports they 'need' for their branch. Now the scammer has your company's sensitive financial data and to make it worse you have been conned to willingly provide it to them.

- Baiting promises a free good, like a song or ebook download, in exchange for your information. Once you provide the sensitive data the hackers are after, the virus is downloaded onto your computer.

- Quid Pro Quo involves a promise of service in exchange for sensitive information. The most common Quid Pro Quo scheme is s scammer pretending he is an IT consultant or a customer support representative calling the employee back. Eventually, he'll hit on the employee that really does have a problem. The "fix" will usually involve revealing sensitive data like a password and other credentials. Other less sophisticated Quid Pro Quo schemes might involve a workplace contest or a survey.

- Make sure your insurance program is broad enough to cover any type of cyber attack regardless of the method or what was stolen. The best way to do that is purchase both a cyber and crime with social engineering policy.

(Sources: https://www.propertycasualty360.com/2018/02/05/fool-me-once-insurance-coverage-for-social-enginee/ ; https://foundershield.com/top-6-forms-of-social-engineering/)