Cyberliability Tips: Watch Out for Holiday Scams!

As companies dash toward year-end, scammers are also hard at work. In one common scam, known as "spoofing," an employee receives an email that appears to be from within an organization in order to trick the recipient into sending the scammer money, sensitive information, or other materials of value.

These emails are typically addressed from an executive of the company and will usually contain a simple request like, "Can you help me with an important project right now?" The scammer's goal is to create a sense of urgency so that the recipient will reply quickly and without questioning the legitimacy of the request. Once the recipient responds, the scammer will typically ask the recipient to wire money or divulge sensitive information.

This time of year, for example, the request may ask the recipient to provide a company credit card number to buy gift cards for the company's employees or customers. Once the scammer has the number, he or she can quickly spend hundreds or thousands of dollars. It is also common for scammers to ask an employee to buy gift cards and send the redemption codes to the scammer via email, allowing the scammer to redeem the gift cards online without being traced. A request to purchase gift cards a week before Christmas may not seem so unusual, but any urgent request for funds should be treated as suspicious, no matter the time of year.

The best protection is to make sure to train all company personnel on the warning signs and proper procedure for confirming a sender's identity before responding to any suspicious emails. Most spoofed email addresses will appear similar, but not identical, to the sender's real email address. If an employee has any doubt about the legitimacy of an email, the recipient should double-check the source email address.

If, after double-checking, the recipient still isn't sure whether or not the request is legitimate, he or she should call the purported sender (at a known telephone number, not the number in the email) or send a new email to a known email address asking if the first email is legitimate (the recipient should never respond directly to the suspect email). There should also be a procedure for reporting suspicious emails. Many organizations also set their email settings to automatically flag emails from external sources, which makes detecting spoofed emails easier.

Scammers know that the end of the year is hectic for businesses and that some employees will let their guard down. If you have policies in place to address these types of risks, it is a good time to remind your team to be extra vigilant. If your policies could use some refreshing or you would like to discuss ways to help prevent becoming the victim of a scam, please contact us and we would be happy to help.

Date Created
December 18, 2018