Division *of* Risk Management

Business Email Compromises – A Social Engineering Attack

In 2021, the Federal Bureau of Investigation received over 20k complaints of business email compromise (BECs) in which companies lost approximately $2.4 billion. A BEC is a type of social engineering attack where scammers use emails to impersonate employees or trusted vendors and clients. They use fake emails to trick companies into sending payments, changing payroll, directing deposit information, or acquiring sensitive information. The emails often look legitimate. These schemes can cost tens of thousands of dollars. Here are some tips to avoid these scams.

How to Avoid Social Engineering Business Email Compromises

Many agencies and schools are aware of cyber attacks and have often spent a lot of time and money investing in security measures to reduce these threats. Even with all of that in place, the human element still remains. Scammers are taking advantage of human errors and trust to bypass the information technology loss control. This is known as social engineering.

Social engineering attacks are when scammers email various employees in the finance or accounting department with legitimate-looking invoices from known vendors and contractors. They will request an invoice be paid and electronically sent for promised or completed work. To prevent falling victim to these scams, it is critical that accounting controls be implemented to confirm initial payment terms (bank accounts for electronic payments and addresses for physical payments) and to change payment terms. If any aspect of the payments is changed in any way, verification should be done via telephone to ensure you are directly working with the contractor and confirm why the payment method has changed. Accounting or invoicing departments should also implement controls based on authority levels and dollar amounts, such as requiring a supervisor to confirm payments over a certain dollar amount.

Social engineering scams via email often look like they come from a legitimate source and changes submitted by email should not be trusted at face value. Always verify the email sender's identity by placing a phone call to the claimed sender. Also, always remember that legitimate banks will not ask for your authorized credentials or confidential information via email. These scammers often identify which large construction projects your agency is working on and whom the contractor(s) are doing the work. With these large contracts, be careful about who, where, and when you send payments. It is wise to make a couple of extra phone calls to verify a payment amount and the vendor that is supposed to receive it. It will save a lot of money and headache by avoiding a scam.