TIPS FOR EMPLOYEES TO MITIGATE EMAIL-BASED SOCIAL ENGINEERING FRAUD

While social engineering fraud is certainly increasing in sophistication and frequency, implementing the following basic controls will help mitigate the fraudster's chance of success:

1 SLOW DOWN AND BE APPROPRIATELY SKEPTICAL

One of the most common themes in social engineering fraud is that the fraudster creates a sense of urgency. The target is often asked to move quickly in order to avoid missing a deadline or upsetting a client/vendor/manager/executive.

When it comes to transferring funds or sharing information, there is always a case for moving at a measured pace.

It isn't required that you look through life expecting the worst of people, but a healthy level of skepticism is a good thing.

2 CHECK THE ADDRESS AND AVOID USING 'REPLY' TO ACCEPT OR RELAY SENSITIVE INFORMATION

More and more social engineering frauds are taking place through forged or altered email addresses – amended to look very similar to authentic addresses. When responding to requests that ask for confidential or sensitive information to be disclosed or altered, closely verify the address and start a new email chain to the known address to carry on the communication. You should, however, whenever possible, avoid using email to complete these types of transactions. Remember though, if the email address is correct, it doesn't mean it is a legitimate email. Continue to be vigilant.

3 VERIFY WITH A KNOWN SOURCE

Given that fraudulent emails may originate from a legitimate email address (the account may have been hacked) whenever you are asked to make changes that involve sensitive or confidential information (payment/banking info, contact information, primary contact person, mailing address etc.) always verify with a known contact that the person who contacted you is authorized to make those changes or is who they say they are. Pick up the phone or when possible meet in person to confirm.

4 BE UP FRONT IF YOU THINK YOU'VE BEEN A VICTIM

It happens more than we'd like. If you think you may have been the target of a social engineering attack, successful or not, tell your manager so that they can act early. Sometimes it is only through hindsight when you may realize something was off. Often a quick response can minimize the damage. Hiding it, avoiding it or hoping it goes away will only ensure that the potential loss is bigger and/or harder to recover.

5 CREATE AN ENVIRONMENT THAT PROMOTES CAUTION AND HAVE ESTABLISHED PROTOCOLS

If you are in a position where you give instructions to others or have people report to you, encourage them to verify important or atypical requests and offer praise when they do. Often people don't verify because they don't want to risk upsetting a busy manager or executive within the company.

Create internal protocols that address making changes to or disclosing sensitive or confidential information, so that employees don't have to make it up as they go. Give them the tools to protect themselves and the company.

Visit **theguarantee.com/corporateinsurance** to learn more about our Corporate Insurance products and services.