Anyone who is tasked with purchasing supplies or making payments to vendors could be at risk of receiving falsified payment instructions. These fraudsters are smart; it is important to stay vigilant and cautious to avoid sending money to someone who is attempting to trick you in order to receive funds through fraudulent methods. Three common scenarios are listed below.

**SCENARIO 1**

*Your system has been breached and someone’s email account has been hacked*

In this scenario, a hacker has gained access to your systems in order to hijack your email accounts. This means that they have an employee’s login credentials and can communicate with you without the employee knowing. The hacker can also make it appear as if an actual employee is sending an email with instructions on how to distribute funds. Oftentimes, the attackers will monitor your communications, and use the information they gather to send a more convincing e-mail.

**SCENARIO 2**

*The vendor’s system has been hacked*

In this scenario, one of your vendors has been hacked, and the attacker sends you an email from the vendor’s account asking for you to make a payment. As in the first scenario, the email will be from a legitimate account of someone you have communicated with in the past. The attacker will also likely monitor communications and jump in after legitimate emails have been sent back and forth, so that it looks like a continuation of a real conversation with the vendor.

**SCENARIO 3**

*Vendor’s email is spoofed*

This scenario is different from the first two because no one has actually been “hacked.” Instead, the attacker makes it appear as if they are one of your vendors. These attackers are smart, so the email will look similar to a real email from your vendor. They may copy the logo and the email address will likely be off by only one or two characters. An example is CEO@company_xyz.com vs. CEO@company-xyz.com.

westernalliancebank.com | (800) 764-7619