Cyber Criminals Taking Advantage of COVID-19

Preventative Actions You Should Take

Since the start of the 2020, Cyber criminals have registered over 4,000 domain names containing the phrases "Corona" and/or "Covid". These domains are being used to execute phishing and ransomware attacks disguised as Coronavirus related emails. Fraudulent emails may come in the form of a message from the Center for Disease Control & Prevention (CDC), health advice from a medical specialist, or even internal workplace policy notifications.

From mom-and-pop shops to multinational corporations, all businesses are susceptible to social engineering. Here are some helpful tips that your company can utilize to avoid being the victim of a social engineering incident:

1. Multi Factor Authentication (MFA or 2FA)

Most complex social engineering attacks begin with hackers breaching email accounts to obtain a better sense of how businesses communicate and interact. Once the hacker is comfortable with a company's procedures, they will create their own funds transfer request email that appears strikingly like that of an employee, senior executive officer, or vendor, thus increasing the chances of tricking an employee into sending money to a fraudulent bank account.

In order to prevent hackers from obtaining access to emails, we highly recommend utilizing Multi-Factor Authentication (MFA) when logging into email related accounts and applications that require a username and password. MFA will send a text / alert to the user's cell phone with an authorization code, which will be used to confirm the person logging into the email account is in fact them. This is one of the most successful methods of preventing hackers from using brute force attacks, in which they run a program that rallies through a series of passwords until one works.

2. Call Back Procedure

One of the most impactful practices that a business can implement when wiring money is picking up the phone and calling (over a verified telephone number) the company or person requesting the funds transfer to confirm that the request is legitimate.

Verified telephone number does not include numbers found in the email containing the request, but rather the phone number listed on the vendor's website, or a number that is confirmed via an internal resource.

3. 2 Person Authorization

If your business is required to transfer money over a certain threshold, we recommend having a two-signature verification process with two senior executive officers involved.

For example, if you are performing a wire transfer over $10,000, then two assigned officers must review and sign off on it before further action is taken.

There is insurance to protect you in the event one of these attacks affects your business. If you don't have cyber coverage, or have questions about the coverage you have, please contact our office at 303-442-1484.