QUESTCO

Cyber Security Awareness

An Information Technology Update from Questco – August 8th, 2020

As the global health crisis of COVID-19 continues, many organizations have experienced a rise in cyber-attacks, including PEOs. Questco has found that one of the most effective tools in the prevention of cyber-attacks is to increase employee awareness of the existence of these actions. To assist in your own employee education process, we have highlighted below several common attack schemes and best practices to follow to avoid falling prey to these schemes.

"Phishing" is the most common type of cyber-attack. There are many forms of phishing, but they share a common goal: to get the recipient to share sensitive information, such as credit card information, log-in credentials, or bank account information. Not only is this a risk to PEOs, but it is also a risk to all employers. Due to the unintended error of an employee, malware can be delivered to a company computer, potentially infiltrating your internal computer systems. Many of us have tools in place to counter these attacks, such as spam filters, but the first line of defense is with our employees.

Below are a few different types of phishing attacks that all employees should be aware of and watching for:

- ***Business Email Compromise or CEO Fraud:*** Occurs when the CEO or other C-level executive appears to send an email to a lower-level employee with the goal to transfer funds to a fake account or vendor; however, the sender is actually a cybercriminal.
- ***Spear Phishing:*** Is a sophisticated form of phishing that targets an audience and appears to come from a legitimate source. The cybercriminal will tailor the information to the specific target by personalizing the email, with the intent to trick the recipient into clicking on links or attachments.
- ***Clone Phishing:*** Takes advantage of a legitimate message that the recipient previously received and creates a malicious version of it. It sends a message from an email address that looks legitimate but the links or attachments in the original email are swapped for malicious ones. The cybercriminal will use an excuse that they are resending the original message, because there was a problem with the first link or attachment.
- ***Domain Spoofing:*** This occurs when a cybercriminal "spoofs" an organization or company's domain. They can make their emails look like they are coming from the official domain or make a fake website look like the real deal by using a similar URL. As an example, the spoofed domain could be "Microsoft.co" vs the real domain of "Microsoft.com".

There are many types of phishing, but you as an employer can avoid these phishing schemes by following a few best practices:

- Provide regular training and education to employees about the various types of schemes and clear instructions on how to avoid falling prey, including:

- ✓ Do not click on links or attachments from senders that you do not recognize. Be especially cautious of .zip or other executable file types.
- ✓ Never enter sensitive information in a pop window. This is usually a tool used by cybercriminals.
- ✓ Inspect URLs carefully to make sure they are legitimate and not imposter sites.
- ✓ Watch for email senders that use suspicious or misleading domain names.
- ✓ If asked to provide sensitive information via email from an unknown source, independently confirm the legitimacy of the sender.

- ➢ Ensure you have communicated a clear process for how to report phishing should your employee ever feel they are a target. Encourage all "questionable" emails to be forwarded to the appropriate technology resource in your company for further investigation and potential "blacklisting" of sender.
- ➢ Install and maintain a reliable firewall, anti-spam, and anti-virus software.
- ➢ Set-up multi-factor authentication on devices and programs where possible. This allows the user to authenticate their log-in by requiring two or more credentials. As an example, a code will be sent via text or email for the user to provide in addition to their log-in password.

IMPORTANT

Questco will never send your employees links that require them to fill in personal data, such as banking or credit card information, in a pop-up window. All requests for confidential information will require the employee to log-in to our secure Questco Employee Self Service (ESS) Portal or involve direct communication with Questco via encrypted email. Please communicate this practice to all your employees.

The above list of potential phishing attacks and best practices is not all inclusive. Cybercriminals continue to refine their fraudulent tactics for stealing data; however, remaining vigilant towards the prevention of these types of scams is essential.