WHIPCORD

How to Strengthen Your Cyber Security

It's important to have a set of security practices that all employees adhere to that strengthen your company's security. Your plan should include awareness of potential threats and a designated person your employees can go to for help. It can also be helpful to put together a presentation and include it in your new employee orientation. Two areas of concern for businesses are phishing scams and password security, which this download will address so you can be prepared to talk to your employees about it.

Phishing Scams

These types of scams target your employees usually through email. It comes in the form of a fraudulent message that baits victims into clicking a link. Once the link is clicked, it redirects you to a page resembling a trusted company and prompts you to fill out a form or download a file. Once the action is completed, a trojan is installed that contains malware – like a key logger. The goal of this scam is to gain confidential information like credit card details, which are then sold online and used for identify theft.

Mitigate the Risk

Although these types of scams are targeted more at individuals than organizations, it's no secret that most employees have and will at some point use company equipment for personal use.

How to Tell If an Email Is a Scam

- Requests personal information
- Deceptive domain names
- Generic Salutations
- URLs that don't match the link (hover your mouse over the link to see where it goes)
- Emails with executable file attachments (such as file types like exe)
- Unexpected email attachments
- Messages that elicit heightened emotions (Congrats you've won xyz!)
- An unfamiliar sender

Your employees should not only be aware of these potential threats but also know who they should talk to and what they should do if they become a target of a phishing scam.

Strong Passwords

It's suggested that you have a different password for every different device and site you log in to. A password manager is the best way to achieve that because you will only need to remember the log in for the manager app you're using. To further protect yourself, create a passphrase to use for logging into the manager, which is more complex and includes the recommended amount of characters and symbols. You should also utilize two factor authentication when available.

Mitigate the Risk

If you're using a password manager, a good starting point to creating a passphrase is to think of a phrase you will remember, such as "I had a lemonade stand at 542 First Street, I charged $1.23 per drink." Then use the first digit of each word to form a passphrase. Your new passphrase: Ihalsa542fsIc$1.23pd

How to Create a Strong Password

- Minimum of 12-14 characters
- Mix of symbols, numbers, capitals and lower-case letters
- Isn't a legitimate word or combination of words
- Doesn't have common substitutions, example using a 3 for an E
- Changed every 30-60 days

Two Factor Authentication

This is easy to use and is important because it provides another layer of security that is used to confirm your identity is legitimate. The first authentication step is with a username and password and the second reconfirms your identity, an example is either through a verification code sent by text or scanning your fingerprint.