Seven Ways to Keep Your Business Safe

1 Be Suspicious of Emails and Phone Calls

Social engineering attacks, typically through phishing emails, continue to be credited as the primary attack method used by bad actors to gain access to systems. According to a survey conducted by CoNetrix, phishing attacks were identified as the number one security incident experienced by financial institutions in 2018. If an email in your inbox seems suspicious, don't be afraid to report it or contact the sender using other means to verify the email is genuine.

2 Strong Passwords = Less Stress

Almost every device or profile we use in our daily lives requires a password of some sort. The more profiles you manage, the harder it is to keep track of passwords. It can also be easier for someone else to figure out your password, especially if you make it something easy to remember. Consider using song lyrics or a quote to make the password longer and more complex. Whatever you do, do not write passwords down where someone else can find them.

3 Don't Use the Same Password

It is important to not use the same password for different accounts. If one of your accounts is compromised using a "recycled" password, you run the risk of other accounts being compromised, as well.

4 Use MFA for high risk systems

Multi-Factor Authentication (MFA) is a powerful authentication control. Instead of just providing the typical password (something you know), when MFA is implemented, you must use more than one factor to verify your identity. There are three different types or factors for identification; something you know (password), something you have (token), and something you are (fingerprint). Many applications today offer the ability to add a second factor for authentication, usually in the form of a push notification from an app, an SMS message, or an email.

5 Check, Double Check, and Check Again

Have you ever sent an email in a rush only to find out later you sent it to the wrong person? These kinds of simple mistakes can happen easily, especially when we are busy. It is important for us to be diligent and double check our work. As an example, any time you need to send an email that may contain sensitive data, always check the "To" field to ensure you have selected the correct person to whom the email will be sent.

6 Unsafe Connections Lead to Compromised Devices

With recent advances in technology, it's easy to connect our personal devices to Bluetooth enabled devices. Many of you have your mobile device connected to your car, a pair of headphones, or a smart watch. While Bluetooth connections are meant to make our lives easier, we must be cautious when pairing devices over Bluetooth. If you pair with a Bluetooth device and plan not to use it again, be sure to remove the connection when you're done, or if you prefer to not use Bluetooth at all, turn off the connection on your device to help keep your data safe from unwanted connections.

7 You're Never too Old to Learn Something New

While many of us have heard tips and tricks like the ones in this article, it never hurts to keep ourselves up to date with the latest list of "best practices." The cybersecurity industry is ever changing, and new techniques to steal information are put into action every day. Keep up with the growing threats by following reputable sources like CoNetrix Updates.

CoNetrix
A Family of Technology Companies