WV Executive Branch Privacy Tip

This week's tip is brought to you from the Identity Theft Resource Center (https://www.idtheftcenter.org/) for a reminder of the dangers of phishing.

"All I Did Was Click this Link…"

There's no shortage of scams, fraud attempts, data breaches, and hacking. Sadly, it doesn't matter who the victim is: personal tech users, companies of every size, senior citizens, even school children. Criminals who are after your identifying information or your money have no moral compass when it comes to stealing.

But all too often, victims end up doing the dirty work for the criminals. Whether it's falling for a scam, handing over their information, or installing a virus on the network, if a criminal can trick you into doing his bidding, you're making his job easier.

One of the common strategies scammers use is known by several different names, depending on how it played out. Spoofing, phishing, smishing, and boss phishing are just a few of the labels used to identify the same kind of attack, which involves getting you to comply with their message. Many of these attacks originate in phishing emails, but smishing (from the term "SMS phishing") comes through your text messages, while spoofing and boss phishing come from someone you think you know.

What's the common denominator in these kinds of attacks? A link. Once you click it, you're either redirected to a fake website where you are told to input your sensitive information, or more often, you just downloaded a virus to your computer or mobile device. The virus will then root around in your device for information, and can even send itself to everyone in your contacts list by pretending to come from you.

A number of major data breaches have already been traced back to a phishing email. The Target data breach, for example, was tied to a third-party vendor whose employee clicked a malicious link in an email. Phishing attacks are so rampant, in fact, that Verizon's annual data breach investigation showed that 89% of security breaches in 2015 came about as a result of phishing attempts by organized criminals.

Even more alarming is the fact that between 70% and 90% of the malicious software that infects a company through a phishing attack is unique to that company. That means criminals are rewriting the code each time to make the virus appear unique in order to bypass anti-virus protocols. This helps them avoid the "red flags" that would prevent it from coming through in an email.

But that's all in the corporate world. How does phishing impact you as an individual citizen? In much the same way. Scammers send out phishing attempts through automated emails, sometimes thousands at a time, hoping someone falls for it and clicks the link. Once the individual follows through and the virus is installed, it only becomes a matter of gathering up the victim's personal data.

In order to prevent this kind of attack on your personal computer or mobile device, make sure you keep your anti-virus and anti-malware software up-to-date. More importantly, engage in safe internet behaviors. Never click a link you weren't expecting, even if it appears to come from someone you know.

At work, the steps are pretty much the same. Make sure your company has current software installed that will prevent the installation of malicious software, but more importantly, make sure your company is educating all of its employees—from the CEO to the custodian—on the dangers of phishing emails, boss phishing scams, and harmful links. Establish a policy that not only prevents employees from doing the legwork for hackers, but also leaves the door open for them to safely report it immediately if they accidentally cause a breach.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.