First Neighborhood Bank
216 Market Street
Spencer, WV 25276
(304) 927-1750 (phone)
firstneighborhoodbank.com

April
2018

Mobile Phishing Attacks Are on the Rise

Oftentimes, we think phishing attacks happen only on desktops or laptops, forgetting that our mobile devices are just as vulnerable. And although some may argue that mobile devices can sometimes be more powerful and more flexible than our desktops and laptops, protecting these devices is sometimes an afterthought. But recent reports have shown that mobile phishing attacks are on the rise, and everyone needs to take the same precautions we do for desktops and laptops.

Did you know more than half of all web traffic goes to cell phones? Mobile devices have become the "go-to" method for a lot of people. Even though not all major tasks can be performed on a mobile device, it's fair to say that a great number of them can. Employees can conduct business transactions and other forms of communicating using their mobile device anytime, anywhere. App developers for mobile devices are hard at work creating new and faster capabilities, increasing the likelihood of users reaching for their mobile devices first versus their laptop or desktop. But with all good things in technology, there is great risk.

Lookout recently put out a report stating between 2011 and 2016, mobile phishing attacks have grown a whopping 85%. Cybercriminals have been paying close attention to the increase of mobile device use and know targeting these devices can be extremely lucrative. Traditionally, email was the entry point for cybercriminals via a laptop or desktop, but over the years mobile devices have introduced a number of different ways of communicating, such as instant messaging apps, social media apps, and texting, providing cyber criminals with several different avenues to perform malicious phishing activities.

Inside this issue:

Detecting phishing attacks on a mobile device is difficult. One of the major problems reported is being unable to hover over a link prior to it being clicked on. The size and small print on the devices sometimes prohibit seeing full link details that might expose discrepancies or questionable information. We are more inclined to click on a message received via social media or text without even thinking twice about it. Some of that comes from being distracted. Our mobile devices are with us 24/7 and while performing daily tasks, we simultaneously receive messages on our mobile device causing our attention to shift. This means users are more susceptible to clicking on a link that could possibly be dangerous. In fact, it has been shown that mobile users are 18 times more likely to get duped by phishing scams.

Also, mobile devices are often used for both personal and work, so although a work email account can be protected through the company's network, there are still security gaps because there are non-protected applications being used on that same device as well.

While networks are able to protect desktops and laptops using firewalls and endpoint protections, mobile devices have some challenges in that area. Most of the time, mobile devices are connected outside traditional firewalls and typically do not have endpoint protection in place. They also have access to lots of different platforms that are not used on desktops or laptops.

The fact of the matter is mobile phishing attacks have become easy for cybercriminals. Bad actors are able to find vulnerabilities and take advantage. Here are some ways to protect mobile devices from phishing attacks:

- Make sure your device has malware protection.
- Be careful of links received via email, text or any other form.
- Make sure your device's operating system is updated regularly, as well as updates for apps. Developers are constantly finding loopholes, bugs or other vulnerabilities and make updates to their apps to protect users.
- It is good practice to only use the Google Play Store or Apple App Store to download apps instead of third parties. For the most part, apps that are in the official app stores are monitored, therefore helping to eliminate the threat of possibly downloading something malicious.
- Think about encryption or use of VPNs to connect to secure networks.
- Continue to have security awareness training for employees that incorporates mobile device use and protection tactics. Sometimes having policies and the best software are not enough. Making sure that employees understand and follow guidelines are crucial in protecting data from phishing attacks.

Sources:
https://www.bankinfosecurity.com/phishing-attacks-on-rise-a-3080
https://www.securityweek.com/mobile.
https://blog.lookout.com/mobile-phishing-content-protection