Smartphone Phishing Attacks Escalate, Bedeviling Law Firms

by Sharon D. Nelson, Esq. and John W. Simek

Just When You Thought You Had Perfected Your Cybersecurity Training for Law Firm Employees . . .

Time to think again. It's no secret that cybercriminals have increased all kinds of phishing activity since the pandemic. More people utilizing consumer grade equipment in a less secure work-at-home environment creates a fertile ground for phishing attack victims.

According to a ZDNet report, phishing attacks are shifting to mobile devices. That's not surprising since mobile devices are the primary computing technology for more than 50% of users. The goal of the attackers is to obtain usernames and passwords that could be used for accessing cloud services or other sections of the enterprise network. The goal of the cybercriminal is to gain network access. Attacking a smartphone means a greater success rate for getting that access.

So Why Are Phishing Attacks on Smartphones so Successful?

Spotting a phishing attack on a smartphone is much harder than on a computer. Think about it. When you get an email on a computer, determining the originating email address is pretty easy even if the display name is familiar. On a smartphone, typically you just see the display name and not the actual email address. It takes a lot more work and jumping through hoops to expose the actual originating email address.

As ZDNet states, "Tailoring phishing emails towards mobile devices can make them more difficult to spot because the smaller screen provides fewer opportunities to double check that links in messages are legitimate, while smartphones and tablets might not be secured as comprehensively as laptops and desktop PCs, providing attackers with a useful means of attempting to compromise networks."

Multiple Attack Vectors Multiply the Problem

Multiple attack vectors make mobile devices particularly vulnerable to phishing attacks. There are a lot of vectors for cybercriminals to exploit on a smartphone. Some of the attack channels include the various social media platforms, messaging apps and plain old SMS text messages. In fact, according to a report from security provider Proofpoint, SMS text phishing (also called smishing) increased by almost 700% in the first half of 2021 as compared to the last six months of 2020.

Some of the more recent smishing campaigns revolve around impersonating delivery companies. This is particularly effective this time of year as we are all anxious about our holiday deliveries in light of the global supply chain issue. Imagine a text message impersonating UPS advising that there is a change in a scheduled delivery with a link prompting for your confirmation of some personal information. The webform that you are sent to is controlled by the cybercriminal and looks exactly like one you are familiar with. Mimicking PayPal and Amazon login pages are perennial favorite gambits.

Besides impersonating delivery services, expect to see smishing campaigns thanking you for a recent payment to your AT&T or Verizon account or something similar. The messages contain a link for you to "redeem" your special thank you gift by just completing a form. Again, the webform is identical to one you are used to seeing, but it is hosted on a malicious website. Sorry, but no thanks.

We would also suggest avoiding shortened URLs and QR codes. You really don't have any idea where they are going to send you unless you do a little bit of advanced research and investigation. Employees cheerfully simply click away.

Defending Those Vulnerable Smartphones

Cybercriminals will continue to target mobile devices as firms continue to embrace a work-from-home environment. To make matters worse, the security of mobile devices is typically left in the hands of the remote user and not the enterprise. That's another reason to seriously reconsider a BYOD (Bring Your Own Device) strategy and instead issue firm smartphones to end-users.

Train your employees to be particularly vigilant, especially if they use a mobile device to access corporate resources. Don't reply to suspicious text messages and by no means click on any of the links.

Proofpoint operates the 7726 text message system on behalf of the mobile carriers. To report a suspicious or fraudulent text message, forward it to the short code **7726** (SPAM) so that it can be investigated by your cellular carrier. Just like computers, make sure that your smartphone is up to date and fully patched with the latest software versions. Security firm Lookout reported that "56% of Android users were exposed to nearly three hundred exploitable vulnerabilities by running out-of-date versions of Android OS." Yikes.

In addition, you should be running some sort of security software on your smartphone (including iPhones) just like you do on your computer. After all, smartphones are really nothing more than small, hand-held computers that happen to be able to make phone calls.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com