LEXINGTON™
FINANCIAL/LIFE MANAGEMENT

Phone Phishing: Attackers Turn Their Attention to Mobile Devices

As smartphones are used more in business and even government settings, phishing attacks designed for these devices are more common—and the stakes are higher.

You may think of phishing attacks targeting your phone as a nuisance, obviously bogus text messages that you delete without a second thought. But according to research from cybersecurity firm Dragos, several newer hacking groups are specifically targeting employees of firms in such crucial sectors as utilities, manufacturing, and government.

Indeed, according to another report from Lookout, the energy sector has seen a massive 161% increase in mobile phishing attacks targeting the energy sector since the second half of 2020.

Why do newer attacks often focus on mobile devices rather than email inboxes? Experts point to two major reasons:

- Most large organizations now have in place solid anti-phishing technology that prevents many attacks from reaching employees.
- Multiple studies show that while workers have become accustomed to email phishing threats, and are thus on their guard when working through new messages, they are far more trusting when they receive text messages on their phone.

What you can do

At their core, mobile phishing attacks—like their email- or voice-based counterparts—are social engineering scams. That means you can take several precautions to avoid putting company data at risk:

- Reset your expectations. Understand that even a legitimate-looking text message that appears to have come from your manager or another co-worker could be a scam.
- Take your time. Any phishing gambit, especially one that arrives on your smartphone, will attempt to rush you to take some action without thinking it through. Instead, pause, take a deep breath, and consider calling the supposed sender to confirm.
- Consider a helper app. There are several anti-malware apps that can spot potential incoming spam and malware. They're no substitute for using your head, but you may find them helpful.

LEXINGTON™

FINANCIAL/LIFE MANAGEMENT

2022 Security Resolutions

While you're promising to get to the gym more often in 2022, or maybe contribute a bit more to your 401(k), here are a few security resolutions to add to your list:

- **I resolve to** go through all my passwords and change them, making them longer, stronger, and unique. After all, many of them are old or mild variants of other passwords.
- In fact, **I resolve to** finally explore these digital password managers that create super-strong passwords and remember them for you. I have so many accounts that now may be the time.
- **I resolve to** save a few trees and boost my security by going online-only for my bank and investment account statements.
- **I resolve to** procure all three (Equifax, Experian, and TransUnion) of my free credit reports—and to do so for my children while I'm at it. These reports can serve as early indicators of fraud.
- **I resolve to** stop emailing work to my private email account. It's a convenient way to get some work done overnight or on weekends, but it's a breach waiting to happen.
- **I resolve to** change my passwords at work and stop letting colleagues log in as me.
- Speaking of colleagues, **I resolve to** be alert to signs of insider threat (people working weird hours, seeking access to new projects, etc.) and to report these red flags when I see them.
- **I resolve to** examine my social media accounts to make sure I'm not "oversharing" in a way that could help hackers guess my login info.
- **I resolve to** start using two-factor authentication wherever I can.
- It never hurts to be tidy, so **I resolve to** neaten up my work areas—both in the office and at home—and securely store any sensitive hardcopy documents.