Beware: Cybervillains Lurk on LinkedIn

BY STEVE THOMAS

ISTOCK

HARDLY A DAY GOES BY WITHOUT NEWS of another data breach, online scam, new malware threat, or other success story from the annals of organized cybercrime. A March 6 article from International Business Times reported that more than 1 million decrypted Gmail and Yahoo accounts from prior breaches had gone up for sale on the Dark Web, including user names, passwords and email addresses, with the converted Bitcoin prices ranging from $10 to $28 per account. Malevolent shoppers need merely browse the contraband inventory and add to their criminal cart, like eBay for bad guys.

The sources for reaping ill-gotten gains have expanded to virtually every corner of the internet, including what might seem an unlikely hunting ground at first glance—LinkedIn. Although the professional network offers no platform for money to change hands, crooks still see gold in profile pages, endorsements, InMails and connection requests. Consequently, scams abound, despite LinkedIn's continual efforts to weed them out.

Since virtually all online scammers are con artists at heart, they often begin on LinkedIn with a fake profile page, frequently using a photo of an attractive female or the logo of a well-known brand. In November 2016, KnowBe4 reported a fake Wells Fargo LinkedIn profile being used to contact LinkedIn subscribers with InMails (LinkedIn's internal emails) telling them that their "Personal Security Key for your Wells Fargo Account has expired" and urging them to click a link to reactivate the key. The link led to a fake Wells Fargo page asking for credentials—a fairly standard "credentials phish."

To boost credibility, the miscreants often will send out very real connection requests from their fake profile pages, duping those who automatically accept connection requests into supporting the criminal enterprise by making it appear more legitimate. Of course, those connections often will be the first targets for later scams. The best approach is to disregard connection requests unless the sender is known or separately validated.

Once a credible fake profile page has been established, the scamming can begin. Fake job offers, romantic ruses, and Spanish-Prisoner-like cons set up marks to divulge data or pay advance fees. The same approaches used by legitimate recruiters to find potential recruits for open positions can be used by criminals to seduce job seekers into giving up valuable information. Data extracted from victims can be incorporated into spear-phishing or whaling attacks designed to trick employees into wiring funds because they believe their boss is the person telling them to do so.

Sometimes, the bogus communication purports to come from LinkedIn itself, using faked support notices and the LinkedIn logo to lure users into divulging their LinkedIn credentials and other personal information. A simple request to "confirm your email address" on an authentic-looking LinkedIn message could reward a click with ransomware.

Even connection requests can be a trap. After all, a LinkedIn user learns about a connection request from an email, which could be a spoof carrying

a link to malware instead of a potential contact.

Be suspicious of anything claiming that your account might be blocked for inactivity, or inviting you to click on a link or attachment. Since connection requests and other communications in email format can be spoofed, generally it's better to double-check them by logging in to LinkedIn before clicking any link or opening any document.

The best approach is to spot the scam up front, and there are some common indicators. As mentioned above, fake profiles or connection requests often use images of attractive young women or commercial logos lifted from other places on the internet. When uncertain, drop the image or logo into Google's reverse image search and see whether it matches the purported source.

Check the text. If it sounds full of SEO terms normal people would rarely use, or if there are frequent misspellings or grammatical gaffes, proceed with caution.

LinkedIn has been vigilant about finding and shutting down scammers, so quite often fake profiles have very few connections. Like a restaurant with only two customers at lunch hour, be wary of profiles having only a few connections, especially when they ask to connect or seek information.

Professionals eager to grow their networks generally are diligent about developing a relatively complete and attractive profile, so it's a red flag when a connection request comes from a profile that has entire sections blank or that has text that reads as if it was pasted from somewhere else.

A lot of these issues of vulnerability to potential scammers can be addressed by modifying the privacy settings in LinkedIn, but locking down your LinkedIn profile reduces exposure and your ability to connect with others, which undermines the purpose for joining the network in the first place.

At day's end, being careful beats hiding. LinkedIn offers valuable opportunities for professionals to develop relationships and build their networks. In every legitimate institution, there are always lawbreakers lurking in the shadows—con artists have a long tradition of associating with churches and charities. Like with any other online gathering place, LinkedIn users should weigh the benefits but watch their step.

Steve Thomas is a shareholder with McGuire, Craddock & Strother in Dallas. He serves on the firm's technology committee. His practice includes commercial litigation in state and federal courts. His email is sthomas@mcslaw.com.