Staying Safe and Secure On Social Media

By Sid Kirchheimer

Get wise to these 5 ways your data is at risk

Fifty-plus and on Facebook? You're in great company—64 percent of online adults ages 50 to 64 use Facebook, as do almost half of those 65 and older. But among social media fans and followers, there is fraud. "Phishing" scams—in which criminals try to collect your credit card numbers, log-in credentials and other information in order to steal your identity—have more than doubled in the past year, reports social media security company Proofpoint.

Watch out for these ruses.

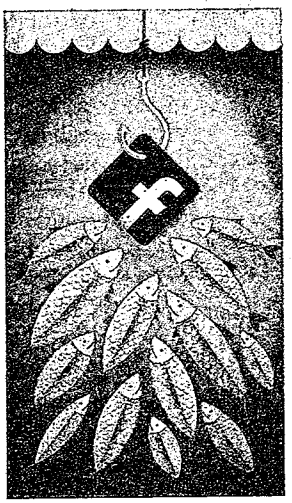
1. Twitter tricks With keystroke tweaks—such as adding an extra character to a corporate name—cybercrooks create fake social media accounts to pose as customer-care reps.

The phishing mission: to intercept messages sent to legitimate companies. You tweet a question to a bank's customer service Twitter account, for example, and a scammer—who is monitoring these tweets—responds from a Twitter account with a slightly different name. The crook then provides a link to a fake website that requests your log-in code and account number.

"The customer not only expects the response, he or she welcomes it, and has incentive to follow the link," explains Devin Redmond, vice president of social media security and compliance at Proofpoint.

2. Live-stream lies Taking a cue from media companies that stream their TV shows and movies online, crooks offer their own programming—typically, they promise free viewing of a big game, hot concert or other popular event.

The phishing mission: With tempting comments on social media pages (say, the page of a sports team), scammers post links promising free access to a live stream. Click and you'll land on a website that demands credit card and personal details before any stream is provided, often under the guise of a free trial that can be canceled any time. Provide the info and you may see nothing; the promised stream often doesn't exist. But after the "free trial" expires, look for a monthly charge on your credit card.



ERIC NYFFELER

3. Fake freebies and discounts Scammers set up bogus social media pages that look like those of legit companies—and claim to offer free or dirt-cheap products and services.

The phishing mission: to collect your name, address, phone numbers, email address and other information to be used for identity theft or sold to other crooks on the black market. The thieves also collect credit card numbers, which are supposedly required for shipping and handling of the faux freebies.

4. Contest cons and survey swindles In these schemes, crooks promise a prize for completing an online survey.

The phishing mission: Getting you to fill out a survey lets the bad guys mine deeper for your personal information, including occupation, income and spending habits.

5. Gossip gotchas Celebrity names, coupled with terms such as "video" and "picture," have long been among the internet's most-typed search terms—and most dangerous. That's true on social media as well.

The phishing mission: Your curiosity about Hollywood's elite, sports superstars and other household names is used to tease you into clicking on links promising scandalous video and reports about these folks, for which you provide your credit card info.

Whatever the con, many of these pages look so realistic and the responses seem so convincing that it's easy to fall for them. Your best protection is common sense. Go to the manufacturer's official website for freebies, for instance. Be careful what you click on. All in all, don't be *too* social on social media—hang on to your personal information. □

GO TO aarp.org/fraudwatch network to learn more about identity theft and avoiding scams.

Sid Kirchheimer is the author of *Scam-Proof Your Life*, published by AARP Books/Sterling.