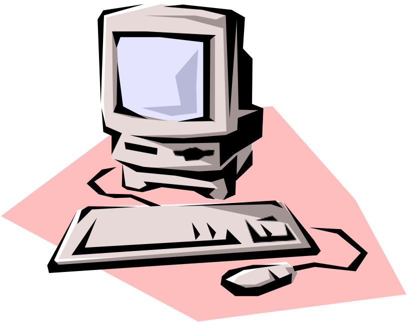
COMPUTER CORNER



Spoofing and Phishing and Fraud, Oh My!

by Michael Wilson

We are all at risk of various types of scams, whether in person, by phone, or by email. Our own past-president, John Farris, was recently tricked into giving his email password to an unauthorized party. He was lucky enough not to suffer financial loss as a result, but still had to spend many hours holding for and talking with tech support in order to get the resulting mess cleaned up.

The annual reports of the FBI's Internet Crime Complaint Center (*www.ic3.gov*) show that internet-based crimes are increasing rapidly, from 288,000 complaints and $1.1 billion in losses in 2015 to 467,000 complaints and $3.5 billion in losses in 2019. The largest category of losses ($1.8 billion worth in 2019) is compromise of email accounts to conduct unauthorized fund transfers. These losses are probably largely to businesses, but many individuals are affected as well. The largest number of complaints in 2019 (115,000 of them) were related to "phishing" scams, which the FBI defines as "Unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials." Another 25,000 complaints involved the closely-related "spoofing," in which contact information is falsified and appears to be from a legitimate source. This can occur by phone, email, or website.

Here you can begin to see the danger if someone is able to gain access to your email account. By reading messages that you send and receive, they can learn enough about you and your friends and family to be able to fool you with a fake message. If you are careless with your email, scammers might even be able to learn credit-card numbers or financial account numbers and passwords that can enable them to make unauthorized purchases, withdrawals, or transfers. Less drastically, using information from the emails they might be able to convince you to give them money or further information (maybe by pretending to be a friend or relative who needs help, for example). Or you might be subjected to "identity theft." A scammer can potentially open new bank accounts in your name, order credit cards, or any number of other things. By the time you find out what's going on, it can be a very big job to clean it all up. Let's be blunt here: you can never be sure that email is private. Even aside from hacking into your email account, it's always possible that a message or messages could be intercepted *en route*. So don't ever put things like credit-card numbers in email! It's also worth noting that older people in particular are often targeted for scams. In 2019, the FBI received 68,000 complaints from victims over the age of 60, with losses of over $800 million.

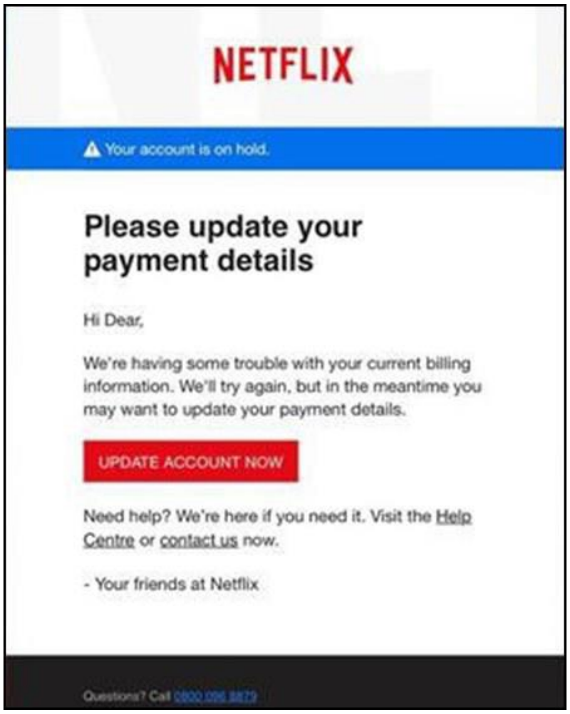
So, what should you do to reduce your chances of becoming a victim of these types of fraud?

First, be careful about emails, especially from unknown senders. Don’t open attachments or click on web links unless you’re pretty sure they are from someone you trust. And even if it is from someone you trust, it’s possible that their email account has been hacked, so watch out for anything that seems off. If you have any suspicions, contact the sender directly and confirm that the email is legitimate.

If an email is from a business or government agency, it’s best to go to their website or call them directly rather than following a link or calling a phone number in the email. For example, I will occasionally get an email from my credit-card company asking me to confirm some charges that they think are questionable for some reason. Even though the email is probably perfectly legitimate, I call the number on the back of my credit card and ask to speak to their fraud department rather than clicking on the web link in the email, just to be sure.

It’s definitely a red flag if an email is asking for money or personal information like your social-security number, whether it be for a Nigerian prince or the IRS, or even a grandchild in trouble. Call the IRS or your grandchild directly! (Just ignore the Nigerian prince.) This goes for phone calls as well. Lots of scams involve trying to scare you into thinking that you or someone you know are in trouble. It’s an extra big red flag if they are asking for payment by some untraceable method such as a pre-paid credit card. Something like that is almost certainly a scam.

An email from a company or agency can look official simply by incorporating logos, typefaces, colors, and such that could have been copied from an actual email or a website. The FTC’s Consumer Information website has an example of a fake message from Netflix (see figure), which looks very convincing (except for the “Hi Dear”—keep your eyes open for things that don’t look quite right). If you get a message like that, don’t click on its links or call its phone numbers—log into your Netflix account or look up their phone number in a directory. And remember that a personal message can also look legitimate if someone’s email has been hacked.


NETFLIX

⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 8879

Legitimate companies or agencies will not request personal information, financial information, etc. by email or phone unless it’s part of some ongoing interaction with them. If the IRS has something official to tell you, they will send you a letter, not call you on the phone. (Watch out there, too, because letters can be fraudulent as well.)

If you do receive a fraudulent message from a company or agency, you can look for a phone number or website to report it to them, or even report it to the police, the FTC, or the FBI. If you think a scammer has actually obtained your information, the FTC has a website, IdentityTheft.gov, which can get you started on what to do about it. There are also companies now that offer “identity theft” protection. They will keep a watch on the dark corners of the internet for you, watching for your private information to pop up where it shouldn’t, and helping you to recover if your information should be compromised, including insurance to cover financial losses. It’s especially a good idea to sign up for a service like that if you know that your information might have been exposed in one of the big hacks like those of Target and the Office of Personnel Management.

Another step you can take is to be careful with the passwords you use to access various websites, especially financial ones. It’s not a good idea to use the same password everywhere because if one company’s website is compromised and your login ID and password are stolen, the hackers can try that information on other websites. A way to protect against this is to use a password manager to keep track of all your passwords, which enables you to use long, complicated passwords that are different on every site. I had been thinking about doing that for a while, and finally signed up with one recently when my identity-theft service notified me that my email address and a password had been detected on the “dark web.” That seemed like a good reason to start being more careful. I still use simple, rememberable passwords for a lot of websites that don’t really matter, but have cranked up the security for the ones that do matter.

You can also have your credit reports locked at the three credit bureaus at no cost. This prevents anyone from taking out a loan or getting a new credit card using your information. When you need to do something like that, you just have your credit unlocked temporarily.

Finally, protect yourself by making regular backups of your computer(s). Then, if something happens and you lose data, at least you can recover everything up to the last time you backed up. It’s a good idea to keep a copy of your backup data separate from your computer and another copy in a completely separate location. The first protects you if your computer is stolen or is compromised by a hacker or a disk crash, and the second can protect you if your house burns down! There are several services that can allow you to back up your computer to “the cloud.” Just make sure your information gets encrypted and the company has good security.