COMPUTER GURU

by Don Benjamin

Technology Lab Programs sponsored by: Stark & Stark Attorneys at Law

Phone and Text Scams

You just received a call from Verizon that your computer is infected with a virus. The voice on the far end offers to remove the malware and provide a security service for $799 for life (not sure who's life). "The service will cover all your computers, tablets, and smartphones." But he needs access to your hard drive to install the special security application.

You agree to a five-year plan and give him your credit card information. He then hangs up without doing anything. Or, if you let him access your computer, he may add a password or encrypt your files and demand payment to restore your hard drive.

Of course, it's a scam.

So is the text message you received from your bank that they froze your account, but if you call a special number you can regain access. So is the phone call from Amazon that someone in Moline, Iowa, has charged an item to your account and "… please press '1' so we can reverse the charges on your credit card." Nope. Not legit.

Latrina kvetches after she realized she'd been scammed.

We've noticed an increase in phone, email, and text scams that sound and look official but can cost you hundreds or thousands of dollars or render your computer unusable. The scammers aren't trying to get your information, just your money. Most of the scammers work from call centers in India and use fake American names, like "Bob Jones" or "Kevin Wilson," or Mary-Lou Philips." (None of my many friends from India are named Bob or Kevin or Mary-Lou.)

Here are some general facts to keep in mind:

1. Internet service providers, such as Verizon and Xfinity, don't monitor your computer and will not call to tell you that you have a computer virus.
2. Computer companies, like Apple or Microsoft, won't call you, either. None of these companies monitor your equipment.
3. Webpage pop-ups that warn you've been infected are usually bogus. Just close your browser.
4. Your bank will not text you that your checking account has been locked, and if you want to unlock it, "simply enter your account number." If you're worried, call your bank.
5. The Social Security Administration will not call you to report that your social security number has been found in an abandoned Toyota Corolla near El Paso along with twenty-two pounds of illicit drugs.
6. PSE&G will not call you demanding immediate payment in Walmart gift cards. Nor will American Water or the IRS.
7. Your credit card company may send you a text to confirm that recent purchases are legitimate. Those are OK—you usually answer with a Y or N. But don't click any links. Call your bank if you're concerned.

Randy is the victim of a scammer who installed a small thermonuclear device on his laptop.

And here are some tips to keep you safe:

1. If you are uncertain of a phone caller's integrity, hang up.
2. Don't give anyone you don't know access to your computer.
3. Never click on links in emails or text messages that ask you to confirm your account information, ID, or password. Call the company from the phone numbers you already have or check your account from their website.
4. If you're worried about suspicious messages, webpages that warn you that you've been hacked, or phone calls from Kevin, contact our Tech Resources webpage **princetonsenior.org/psrc-tech-resources/** for help.