Password Protected?

Stop cyber criminals from trying to take a byte of your personal and private data.

BY MARK WARD, SR., PHD

A newcomer to today's digital devices, "Pat" didn't grow up in the generation that is connected 24/7. But now, with interest in making some extra money from home, Pat was ready to explore the vast possibilities available along the Information Superhighway and headed online, checking out one site after another. Requesting additional information was so easy. Just a few clicks!

One company started calling—several times a day—wanting to sell Pat its services. Only a small investment was needed. Pat got an ego boost from all the attention and the promise of "inside" information about how businesses worked. A profit was guaranteed or the upfront money would be refunded. All Pat had to do was provide some identification and a processing fee. The company would take care of setting up a legal business in Pat's name.

About this time, Pat noticed the computer was running slower and locking up. When a pop-up ad for a computer "cleaning" service appeared, Pat phoned the number and soon was getting repeated calls from a technician for a "major" software corporation. Pat trusted the name and, with the man on the phone providing guidance, let him remotely control the computer in order to fix the problems. But the computer got worse, not better.

Pat grew worried—and too embarrassed to tell family and friends. After a year, the truth couldn't be avoided. The scam had cost several thousand dollars. And Pat had to junk the computer, change all bank accounts and credit cards, get a new phone number, engage a legal adviser, write the IRS—and cope with ongoing psychological strain and shame. That Information Superhighway no longer looked so attractive.

SNAPSHOT

- Each year, cybercrime costs the U.S. economy $140 billion and half a million jobs.
- Use an updated antivirus/antispyware program on all devices so spammers can't insert "malware" that tracks you online or remotely controls your computer.
- The consequences of a lost smartphone, tablet or laptop can be as bad as losing your wallet or purse!

Though the name has been changed, this tale is true—and, frighteningly, it's all too common. Every day, some 800 reports of cyber fraud are received by the Internet Crime Complaint Center, a joint project of the FBI and U.S. Department of Justice. That number likely is a drop in the bucket, because most cybercrime goes unreported or even undetected. A 2013 study by the Center for Strategic and International Studies estimates that cybercrime annually costs the U.S. economy $140 billion and half a million jobs.

The statistics are alarming in the aggregate. But the danger really hits home on a personal level. Pat's story is a good illustration. Not being "streetwise" to the Internet, Pat became prey to what the Federal Trade Commission (FTC) labels the "work-at-home scam," as well as the"tech-support scam." Both scams sought to steal Pat's money *and* identity. And the FTC lists more than a dozen common cyber scams related to weight loss, sweepstakes, mystery shoppers, online dating, online auctions, debt relief, investment, bogus apartment rentals and others. More threats lie in wait as Americans increasingly incorporate mobile devices into their daily lives—and opportunities for credit card fraud are on the rise.

How to make sense of it all? Think of the threats in three broad categories: **privacy, security and identity.** You want to protect yourself against unwanted *messages*, *intrusions* and *access*. Thieves can wreak havoc in all three ways: fooling you into giving away your information, infecting your device with "malware" that spies on your online activities and accessing your data while you're connected to a network. Let's take a look at what you can do to reduce your risk of becoming a victim.

Maintaining Your Privacy

Mail Call

Solicitations have become omnipresent in daily life. You check the "snail" mailbox and find it crammed with pre-approvals and offers. As you sit down to dinner with the family, the phone rings; a telemarketer is on the line. After dinner, you check your personal e-mail and discover a dozen spam messages. And now, a new wrinkle: text messaging spam. (While snail mail and the telephone aren't literal players in cyberspace, you can adopt an overall strategy to protect your privacy against *all* forms of unwanted communication. For more details, check out our online story at www.schoolnutrition.org/snmagazinebonuscontent.)

In cyberspace, you can limit unsolicited e-mail by using filters in your e-mail software and routing suspect messages to the "Bulk" or "Spam" folder. Moreover, before you provide your e-mail address to a website, you always should read its privacy policy. If you do decide to provide your address, consider unchecking the pre-checked boxes that give the company—and its marketing partners—permission to send you updates, offers and so on. Consider creating an e-mail address that's separate from your personal e-mail and is designated specifically for such uses.

Spam Artists

Spam is a particularly pernicious type of unsolicited e-mail. If your device isn't protected by an updated antivirus and antispyware program, spammers can insert "malware" to spy on your online activities and even remotely control your computer to send out even more spam.

Spammers connect hacked computers into networks, or "botnets," that send countless e-mails. According to the FTC, millions of home computers have become parts of botnets, and most spam is generated in this fashion. You can lessen the likelihood of being hacked by and into a botnet if you install security software from a reputable provider, set the software to update automatically and disconnect from the Internet when you are away from your computer. If downloading free software (such as games and toolbars), make sure it's from a source you trust—and, as a rule, *never* open unknown e-mail attachments or undefined "click here" links.

"Phishing" e-mails are a type of spam that requests your personal information. These often claim to come from a reputable source and may even have a graphic design that mimics a legitimate organization. Usually, "phishing" consists of an alarming message—your bank account is being closed, your credit card account shows an unauthorized transaction charge, your unpaid invoice will be sent to a debt collector, your sweepstakes award is forfeit—along with a request for prompt verification of your identity. Report phishing attacks and all other spam to the FTC by forwarding the messages to spam@uce.gov.

Beware, too, those pop-up and banner ads that appear on your computer with alarming messages ("Your computer is in danger! Click here for a free PC scan!") or with offers that seem too good to be true ("Congratulations! You've been chosen to receive a free . . ."). The safest course is to ignore them. If you must, look up the name of the company or product on your favorite search engine, along with the keyword "complaint," "scam" or "review." Ads can appear on websites you trust without the site endorsing the ad or even knowing about it. Many scammers buy ads that look legit, but direct you to a bogus service; if you click the link, you might start getting unsolicited pop-up ads that pressure you further.

The latest target for spammers is your cell phone. Just as many Americans are moving toward text messaging as a preferred communication method, so are spammers. Many use auto-dialers to randomly or sequentially generate phone numbers and send offers of free gifts or discounted service if you provide personal details. Even clicking the link makes your phone vulnerable to malware that transmits your phone account data to the spammers, who in turn sell the information to marketers or identity thieves. Like telemarketing and robocalls, most unsolicited text messages are illegal unless you give the sender written permission.

Shield Yourself

Since malware can infect both your computer and your cell phone, you need to know how to fight back. As already noted, keep your security software up to date and don't click any links, open any attachments or download any software from unfamiliar sources. Set your web browser to block pop-up ads and detect unauthorized downloads.

Is your computer or mobile device slowing down, draining power too quickly, crashing repeatedly, refusing to boot up or shut down or displaying unfamiliar web content? Consider the possibility that you've been hacked. If you suspect your unit has been compromised, then immediately stop any online banking, shopping and other activities that require the exchange of personal information. Otherwise, the scammers' spyware may access your logins, passwords, bank accounts, credit card numbers and other sensitive personal data.

Next, update your security software, activate a scan for viruses and spyware, delete any identified threats and restart the unit. If your computer or mobile device is still under warranty, note the model and serial number and then contact the manufacturer or retailer for additional technical support.

Securing Your Devices

Keep a Watchful Eye

It can be a complicated, expensive and time-consuming process, but installing—and updating—security software on *all* your devices is an essential step in protecting yourself against cyber predators. Such software should provide protection against computer viruses and spyware, plus a "firewall" to stop downloads from unknown or risky sources.

Another vital security measure is your choice of passwords for logging into the computer, connecting to your Internet service and accessing specific websites. In general, the strongest passwords are those that are longer (10 to 12 characters are recommended) and feature a mix of numbers, letters and special characters (such as @#$%^&). Avoid predictable combinations featuring names, common words and birthdates. Don't share your passwords, avoid using the same or similar ones for every account and be sure to store them in a secure place—never on the actual device.

Laptops, tablets, smartphones and other mobile devices allow you to access the Internet on the go—so these also require updated security software and secure passwords. But unlike desktop computers, they can be misplaced, lost or stolen—and the consequences can be as bad as losing your wallet or purse! Use common sense to minimize the danger:

- Know where your laptop and mobile devices are at all times.
- Avoid leaving these in the car; but if you must, put them out of sight and lock the doors.
- When you travel, don't leave your laptop and mobile devices in checked luggage.
- Pay attention as your items emerge from a security metal detector.
- At a hotel, store your laptop or tablet in the room safe.
- When using portable devices at a meeting, never leave them unattended.
- Consider buying a laptop alarm triggered by sudden motion or when the unit is taken out of a specified range.
- Don't store passwords on the device or in the pocket of its case.

Keeping your computer and mobile devices secure also applies to their eventual disposal. Desktop and laptop computers have hard drives that may store everything from your address book to your tax returns. Even when you delete a file, the data itself remains on the drive; only the links for reassembling the data have been deleted. Unless the data itself is wiped clean, anyone who acquires your old computer can reconstruct the files through a recovery program. For details on how to manage the destruction process, visit www.schoolnutrition.org/snmagazinebonuscontent.

Protecting Your Identity

Cookie Monsters

The very nature of the Internet—the ability for computers to exchange information—brings a final threat that comes in the form of exchanging some account data about your own computer or mobile device usage. Much of this sharing is benign and is designed to make your Internet experience more efficient, convenient and enjoyable. For example, a website uses "first-party cookies" to record your login, the pages you visited, the content you searched, the items in your shopping cart, the highest game score you attained, the ads you clicked and so on. When you return for a different visit, the site "remembers" you and your activity so you can continue where you left off.

However, the same site may allow "third-party cookies" by which *advertisers* can recognize your activity and deliver new ads tailored to your interests. If this proves bothersome, most web browsers provide privacy settings that can delete or limit cookies, while some web advertisers now alert visitors on how to "opt-out" of cookies.

The websites of the Digital Advertising Alliance (www.aboutads.info) and the Network Advertising Initiative (www.networkadvertising.org) feature general information for opting out of targeted web ads. The industry also has developed a Do Not Track service—now supported by some web browsers—which is similar in concept to the government's Do Not Call registry. Companies that have signed onto the service are legally required to honor your preference.

Careless Whispers

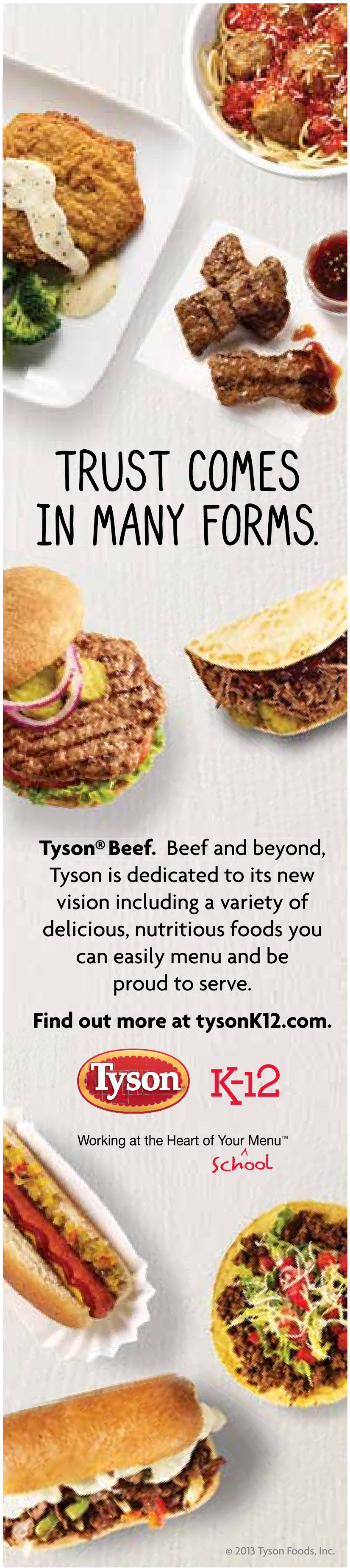
While *some* data must be exchanged to use the Internet, don't ever take it for granted, because today, the risk is only heightened as more users access the Internet via wireless networks. These send your data where thieves can victimize the negligent user.

At home, accessing the Internet with a wireless router is fairly commonplace today. The router provides the freedom of portability around the house. But when you set up the router, choose a strong password for logging into your home network—then be sure to activate the router's encryption feature.

Through encryption, any information you send over the Internet is put into a code that outsiders can't access. The latest wireless routers employ WPA2 (WiFi Protected Access 2) encryption. Older routers with WEP (Wireless Equivalent Privacy) encryption may leave you vulnerable to hackers' newest tricks.

When accessing the Internet via a WiFi hotspot—perhaps a hotel or a coffee shop—remember that most public networks are unsecured. Information you send over a laptop or mobile device is not encrypted. But even if you can't avoid public networks, you can use common sense. Choose a secured network if one is available. If not, make sure that when you're done, you log out. And adjust the settings on your devices so that they don't automatically connect to a WiFi access point just because one comes in range. Three more precautions can help:

- Check with a VPN (Virtual Private Network) provider about how to obtain an account. Even when you log into a public network, you can route your information



through an encrypted VPN.

- If using a mobile device in a WiFi hotspot, connect to the Internet via your phone's web browser rather than a mobile app.
- When on the Internet using public WiFi—or really, whenever you're online—only share personal data with websites that encrypt information sent to and from that site. You can tell if a site and its pages are encrypted if the address begins with *https*; the "s" stands for "secure."

Social networking today is all the rage. You've probably heard how many companies now check a prospective employee's Facebook page and Twitter account for disturbing information. Identity thieves do the same. Never ever post your contact information or Social Security number. Guard other personal information—your hometown, your mother's maiden name, your favorite schoolteacher—that can allow thieves to answer the "challenge" questions that protect your bank accounts and credit files.

Fight Back

If you suspect your identity has been stolen, don't hesitate in taking several critical steps:

- Contact *one* of the national credit report companies and place a free, 90-day initial fraud alert.
- Contact all *three* credit reporting companies to obtain your credit reports and check these for unauthorized charges. Dispute any with the reporting companies, even as you contact the individual creditors involved and follow-up with certified return-receipt letters.
- Go to the FTC's web pages and file an Identity Theft Affidavit.
- Use this document when you report the theft to your local police, office of the state attorney general, the credit reporting companies, individual creditors and debt collectors.
- Contact the three credit reporting companies again, place extended fraud alerts or credit freezes on your files, and ask that disputed charges be blocked on your credit reports.

Just as the Internet is now a fact of life, so are the dangers that come with it. As this article was going to press, technology experts were warning about a new and particularly vicious virus that can turns encryption against you—locking you out of your own files, and demanding a financial ransom to release them. (And paying the ransom doesn't guarantee your data will be unlocked.)

The Internet Superhighway can be a "fun" road, connecting you to more resources, information, people and convenience. Don't take its safety for granted. Like much else in life, with privilege comes responsibility. Don't let ignorance, confusion or laziness be a gateway to becoming a victim. SN

Mark Ward *is a freelance writer based in Victoria, Texas. Photography by* **www.istockphoto.com** *and* **www.jiunlimited.com.**

BONUS
WEB CONTENT

Take steps to protect your personal data and your privacy. Visit www.schoolnutrition.org/snmagazinebonuscontent for exclusive online articles offering tips on limiting telemarketing and robocalls, as well as advice on how to scrub clean your electronic devices when you are ready for an upgrade.

TO YOUR CREDIT: For CEUs toward SNA certification, complete the "To Your Credit" test on page 42.