AVID® Weekly
Decades of College Dreams

Online exposure increases risk of identity theft

By Claudia Buck

When it comes to online identity theft, it's a minefield out there. Every day, some cyber crook is devising new ways to sneak into our online accounts and pilfer money, or just our sanity.

And computer hackers are getting better at it, becoming increasingly sophisticated in their methods and targets.

"In the last five years, the bad guys have gotten as good as or better than the good guys," said Robert Siciliano, security expert with McAfee, the Santa Clara, Calif.-based online security company.

Since 2005, about 560 million consumer medical, financial and personal records have been breached by hackers who broke into databases of numerous government agencies, hospitals and companies, from General Motors to Twitter. That's according to the San Diego-based Privacy Rights Clearinghouse.

No one is entirely safe, say online security experts.

"Based on the massive amount of information that people give away (online) and the staggering number of security breaches that occur each year, it's inevitable you're going to become a victim," said Adam Levin, founder of IdentityTheft911, a security breach consulting firm.

But there are ways to toughen up our defenses against online identity theft. Here's some advice:

BEEF UP PASSWORDS: Too many of us use the same, wimpy passwords, whether it's for banking, shopping or socializing. If just one account gets hacked, they're instantly all vulnerable.

Passwords should never be: a dictionary word, a sequence of numbers/letters (i.e. 45678 or abcdef) or anything that's personal (your kid's name, dog's name, anniversary).

Instead, they should be: at least 8 characters, a mix of upper-/lower-case letters, a combination of letters and symbols (#, &, $, etc.)

Try to make it something you can easily remember. Use the first letter of each word in a favorite phrase or song title, for instance. If you're on a site like Amazon.com, suggests Levin, include the letters AZ.

Too many passwords to remember? Use a password manager, which stores multiple passwords in an "online safe" where you only need one password for access. "They let you randomly generate strong passwords for all your accounts and store them securely," says Joanne McNabb, chief of California's privacy protection office.

McNabb said there are free versions: KeePass (for Windows, OS X, Linux, Android and iOS), Password Safe (Windows) and Keychain (Mac).

SKIP THE QUIZZES: "What dog are you?" "What Michael Jackson dance move are you?" "Could you survive the Hunger Games?"

All those trivia quizzes, polls, surveys and personality tests that populate the online universe may be perfectly benign. Or they could be a cyber crook trying to assemble puzzle pieces of your identity.

"You have to look at the information elicited through those quizzes as components to a nuclear weapon," said IdentityTheft911's Levin. "Many of these personal factoids are harmless on their own but when combined, they create a mosaic of your life" that can be used by hackers.

His advice: Don't indulge.

ANSWER WITH CAUTION: When signing up for online accounts, we're often required to answer selected security questions: your first pet, favorite color, mother's maiden name, high school mascot. But if someone wants to break into your online accounts, every answer they need could already be out there via social media.

Instead, use fake answers that you'll remember or repeat the same answer to every question: "Dog," for instance.

DON'T CLICK: You get an email from a friend, who wants to share a link to a cute video, political commentary or an intriguing story.

Problem is: It might not really be your friend, but an impostor. Or your friend may unwittingly be sharing an infected link that could worm its way into your computer.

"Don't click links in the body of an email. Ever,"

Online exposure increases risk of identity theft

By Claudia Buck

(continued)

---

said McAfee's Siciliano.

If it's a work colleague who said she's sending a link or if a company you've signed up for is sending a confirmation link, it's probably OK. For everything else, "just hit 'Delete.' "

SOCIAL MEDIA SAVVY: There are ways to reduce your risks while still enjoying online socializing, notes McNabb. Among them: never post your email address or your full birth date (especially the year). Lock down your account so it's viewable to "friends only." Don't accept friend requests from people you don't know.

And while Facebook isn't the only social media venue, its 800-plus million users make it a giant target for hackers. Facebook itself has a "Bug Bounty" that pays $500 and up to anyone who pinpoints security holes before they're used by hackers.

Facebook's website has security notes for parents, teens and everyone else on how to report hacked accounts and other online mischief, such as "Please send money" scams.

PALM OF YOUR HAND: Your mobile phone can be a source of cyber intrusions, either by downloading apps infected with viruses or clicking on texts/links that try to con you into disclosing financial or personal information.

At the very least, McNabb says, everyone should use a password on mobile phones.

And don't click on the "Save my Password" feature, says Levin. If your mobile device lands in the wrong hands, that feature could provide instant access to everything stored on your phone.

CHECK YOUR ACCOUNTS: Although he freely uses his credit card online, Siciliano says he carefully scrutinizes his monthly credit card statements. "If you're not looking at your statement frequently, the next thing you know you're paying for dinner of a cyber-thief."

Same for your credit reports. Every adult is entitled to a free, annual credit report from each of the three credit reporting bureaus (Experian, TransUnion and Equifax). Check yours to ensure that no fraudulent accounts have been set up in your name.

"Monitor what's going on; either pay for a monitoring service or look (online) at your bank and credit card accounts every day for fraudulent activity," said Levin.

If your financial institutions offer it, sign up for online or text alerts of suspicious account activity.

GET SECURITY PATCHES: Update your computer with the most current anti-virus and anti-spyware security.

Most newer PCs will do automatic updates, but if you have an older PC that requires manual updates, it may be time to upgrade. "You should be in at least Windows 7 or the latest version of Mac software. … You shouldn't be driving a Ford Pinto," Siciliano said, noting that older browsers and operating systems are often targets of hacker attacks.

———

Distributed by MCT Information Services

———

Claudia Buck is a writer for McClatchy Newspapers.