# Keep Your Data From Prying Eyes

## Eight tips to keep information protected.

**BY CLAIRE VATH**

Ever notice how, after you search for a product or service online, related ads pop up on future web pages you visit? Do you utilize an iPhone or other mobile smartphone device on a day-to-day basis? As you scroll the Web, cookies and tracking software embed ads into subsequent pages you visit. That phone you carry in your pocket features GPS software that easily determines where you live and your travel habits.

Technology is still a new frontier in terms of regulation and susceptibility. Massive amounts of data have been compromised from the FBI, major medical centers and big-box retail stores. These glaring security holes exposed in agencies known for security expertise shed light on the fact we're still at the advent of cybersecurity, and even the experts have a long way to go before fully understanding how best to protect data.

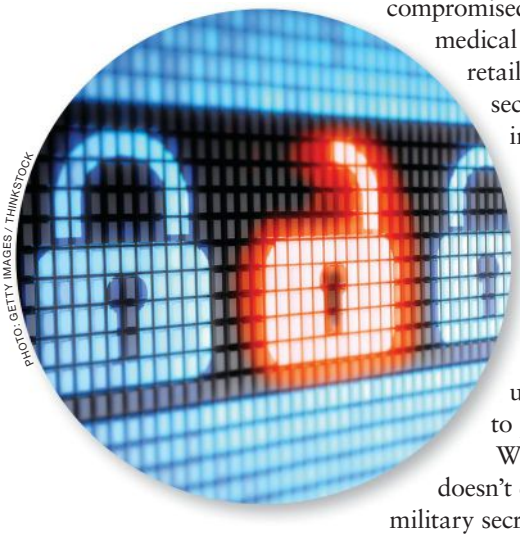

PHOTO: GETTY IMAGES / THINKSTOCK

While your data likely doesn't contain top-level military secrets, it does hold your finances and farm and operational information. So, how can you protect your information?

Scott Brown is author of the recently released "Essential IT Concepts for Small Business" and owner of security and managed services IT firm Ryan Creek Technology Associates, in Madison, Alabama. He offers the following simple steps for farmers and agribusiness owners looking to minimize personal data risk.

**1 SET STRONG PASSWORDS, AND CONSIDER A PASSWORD MANAGER.** A solid password, Brown says, "consists of 12 to 15 characters with a mix of uppercase and lowercase letters, numbers and special characters." Don't reuse the same password over and over. Instead, change up your passwords, and use a password manager, such as LastPass, Tiny Password, Dashlane or KeePass. Once you input all your passwords into the application, a manager encrypts them keeping them more secure. "And don't ever store your passwords in a document on your computer," Brown warns.

**2 CREATE REGULAR DATA BACKUPS.** The easiest way to create a backup involves keeping an external hard drive and keeping it hooked up to your computer, creating a constant backup. Prefer the Cloud? Brown recommends Carbonite or CrashPlan to protect data.

**3 BEWARE FREE SERVICES.** You know those pop-ups that appear on your screen offering free virus protection and free computer hard-drive cleanups? "Purchase, do not use, free antivirus products for phones, tablets, PCs, Macs, etc.," Brown says. "If the service is free, then your personal information is likely the product they're selling."

**4 WATCH WHAT YOU DOWNLOAD.** Never click a link in an email or an attachment. "Always retype the link in the URL bar, or hover over the link to make sure it goes where it says it is going," Brown says. Before opening an attachment you've downloaded, open your antivirus software and scan the file. Clicking a link is one of the easiest ways to quickly load a virus onto your system, potentially destroying critical data, he adds.

**5 MINIMIZE RISK OF CREDIT CARD HACKING.** Credit cards have been hacked online time and time again. How do you minimize your risk? Brown actually recommends getting a prepaid VISA card. "Use it exclusively for online purchases limiting your exposure to the amount deposited on the card," he says.

Otherwise, consider using a third-party encrypted payment method such as PayPal or Apple Pay for an extra layer of security, but link them to a credit card, not your bank account. And be sure to check your bank and credit card statements often, scanning for any suspicious activity.

**6 WATCH OUT FOR BOGUS TECH SUPPORT.** "Never, ever, ever believe the person on the phone that says they have detected a problem with your machine and would like to access it remotely to fix it unless you initiated the call, and it is to someone you know," Brown says. And never, ever give out personal information over the phone unless you initiated the call.

**7 BE STINGY WITH PERSONAL INFORMATION.** Never enter sensitive data—your contact information, credit numbers, etc.—into a form on a website or in an email unless you manually typed in the address in your browser, and it's a trusted site. "Never enter any personal information into a website where the URL does not begin with HTTPS:// and a lock icon is present," Brown says. The "S" in HTTPS denotes a more secure connection.

**8 USE A FIREWALL.** "Do not rely on your Windows firewall. Make sure you have a physical firewall device," Brown advises. Think of a firewall as a literal wall keeping your data safe on one side and hackers on the other. You generally have a software firewall that helps keep people from stealing your data, but a physical firewall adds another level of protection. Most internet routers include a firewall, including brands like SonicWALL, Cisco, Netgear and ZyXEL. ●