LOWDOWN

What You Need to Know About Getting Hacked

Cyber crooks are becoming more brazen. But you can take simple, effective steps to fend off attacks. BY DEANNA PAN

1. IT COULD HAPPEN TO YOU. The Web is rife with anonymous crooks who thrive in an online underground where they peddle stolen personal data. This year alone, according to the Privacy Rights Clearinghouse, hackers stole more than 13 million records containing sensitive information, such as Social Security, financial-account and driver's license numbers. "Companies don't always know what's been taken," says Christopher Boyd, who researches cyber threats at GFI Software. "They have to assume everything was compromised even if there's a good probability it wasn't."

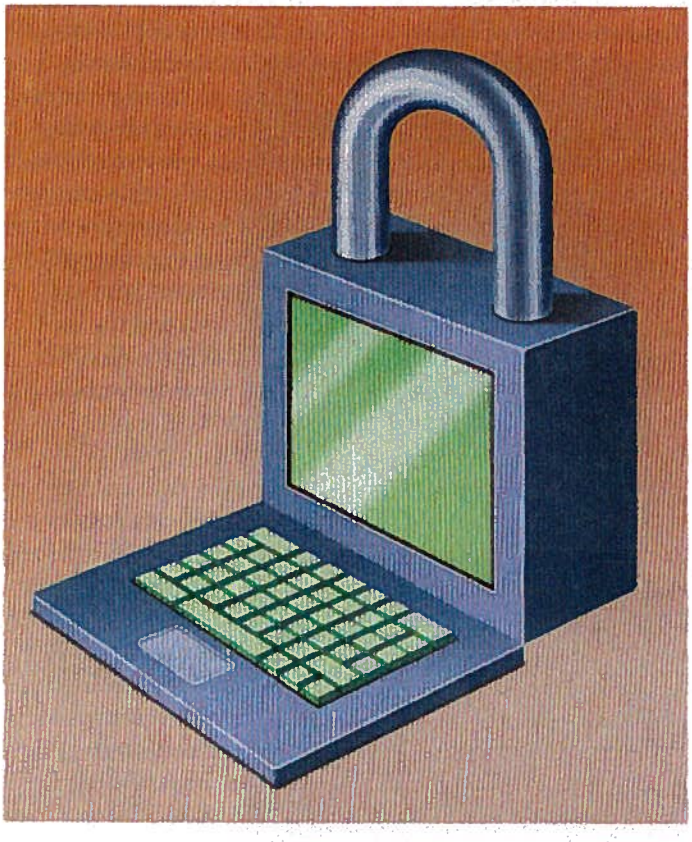
2. DEFEND YOUR PC. Hackers can wreak havoc using PCs they've infected with rogue software, says Matthew Prince, a Web security expert and founder of CloudFlare. Install the latest firewall, anti-malware and antivirus software on your home machine, and always download the recommended security updates for your programs and browsers. Secunia Personal Software Inspector (www.secunia.com/products) is a free download that identifies vulnerabilities in applications such as Adobe Reader and Adobe Flash.

3. PICK YOUR PASSWORDS WISELY. And use a unique password for each of your online accounts. "A lot of people don't change their password for different sites," says Jacques Erasmus, of Webroot Software, who prowls hacker forums in search of the latest cyber-threat trends. "Hackers exploit this by using stolen passwords to log in to other sites to steal your money or identity." A strong password has both upper- and lowercase letters, as well as numbers, punctuation marks and symbols; never use common names or dictionary words. KeePass (http://keepass.info), a free password-management program, can generate, store and protect all of your log-in credentials on your desktop and sync the data with your smart phone.

4. MINIMIZE THE DAMAGE. If one of your online accounts has been breached, assume your data has been disclosed. If your credit or debit card numbers could have been leaked, cancel your compromised cards and compare your online statements with your credit card or ATM receipts. If your Social Security number is exposed, place a security freeze on your credit report, which locks your file so that only you and existing creditors can access your account. Visit Privacyrights.org for more recommendations on dealing with security breaches.

5. SURF RESPONSIBLY. If you're entering confidential information into a Web page, look for *https://* in the URL bar to ensure your data is safe from meddlers. Never use a public Wi-Fi network to log in to your sensitive accounts. Instead, choose wireless connections that are password-protected. Better yet, sign up for a personal virtual private network service, such as Open VPN Shield Exchange (www.shieldexchange.com).

6. THINK BEFORE YOU CLICK. Malicious code often lurks in sketchy downloads, pop-ups, links such as shortened URLs and sites your grandmother wouldn't approve of. According to Symantec's most recent Internet Security Threat report, 49% of search terms that resulted in visits to infected Web sites were seeking "adult entertainment." ■



LLOYD MILLER