

SmartGuard Newsletter

The Ghost in the Machine

Tech-savvy identity thieves troll the Internet for information

Paper? You shred it. Credit and Social Security cards? You keep them private. Release personal information to a random caller, no matter what company they say they're from? No way. By now, most people are aware of the growing threat of identity theft and take the time to properly dispose of receipts and other private documents as well as monitor their credit either by requesting annual reports through the three main bureaus or utilizing the added protection a service such as Privacy Solutions offers.

But are we—not to mention our children—protecting ourselves as well as we could be online? While everyone knows not to email a bank account number to the guy who says he will share his million dollar lottery ticket with you, there are much more subtle, insidious ways for criminals to glean your personal details through the computer. Here's what to watch out for—and how to safeguard yourself online.

When Sharing Can Be Bad

Do you or your kids like to swap files, songs, or movies over Napster, LimeWire, Grokster or other peer-to-peer network? If so, you could be literally handing over your personal data to people across the globe. Though there are measures you can take when downloading peer-to-peer networking programs to block access to your most private files, many of us don't have the know-how to take advantage of these protection measures.

What's worse, if you are using P2P networks on your work computer, you could be exposing not just your own private information to the world, but that of your clients as well. Within the past year, Pfizer, ABN Amro Mortgage Group, and Wagner Resource Group have all fallen victim to security breaches because an employee was using a P2P network during work time. A supreme court judge even had his personal information exposed this way!

Mums the Word

With the advent of online banking, trading, filing of tax returns, and the like, more of your personal information is out there in cyberspace than ever. Of course, financial institutions and the government all use secure servers, but the bottom line is that you also have a responsibility in keeping your accounts protected. That means using different passwords for each important account, changing passwords regularly, and taking care not to set any system—private or public—to remember passwords.

Wireless Worries

Many people now have wireless networks set up in their homes so several computers can connect to the Internet through a single access point, or make use of wi-fi networks at coffee shops, airports, and other public locations. Though quite convenient, wireless networks can expose private information quite easily. At home, make sure you set your connection as secure and password protect it; in public, take care not to reveal personal details via email or on web sites. Also be aware of a scam called "shoulder surfing," where someone in close proximity watches as you input PIN numbers and passwords, then uses them to access your information and accounts later on.

And the Answer Is...

And the Answer Is...

<http://www.staysafeonline.info/basics/quiz.html>

SmartGuard Newsletter

A service of Privacy Solutions.™ The power to protect your identity.

Social Blunders

While it's nice to have online friends through social networking sites such as myspace, facebook, twitter and bebo, know that not everyone there is looking for camaraderie—they may be looking to steal your identity instead. So take care to set your profile as private, and do not post (or let your children post) private details of your life that might allow a thief to steal your identity.

Staying Safe in Cyberspace

Here are some additional tips to staying protected online:

- Install firewalls and anti-virus software to help keep personal computers bug- and hacker-free.
- Don't bite for phishers if you are sent an email asking you to update your account or reveal other private information, even if it appears to be from a company with which you do business. If you have any doubt at all that such an email is legitimate, do not input information over the web and call the company instead. Most firms would not require an Internet update of sensitive personal data.
- Shop securely. When you are making online purchases, be sure you are directed to a secure server that will keep your credit card and other information private. To check, just look at the URL. You will see an "s" after the http (like this https://) as well as a closed lock icon if the site is secure and encrypted.
- Keep careful records by backing up sensitive files and data regularly. In the event your computer stops functioning due to viruses or other cyber threats, you will still have access to important information.
- Educate your family so your children—especially tweens and teens—know the potential hazards posed by peer-to-peer networks and social networking sites.

Related Links

<http://www.tamingthebeast.net/articles/creditcardfraudidentitytheft.htm>

http://blogs.pcmag.com/securitywatch/2008/07/us_supreme_court_judge_among_t.php

<http://www.bbbonline.org/IDtheft/virtual.asp>

<http://www.staysafeonline.info/practices/index.html>