

SmartGuard Newsletter

Computers and the Internet

When It Comes to Identity Computer Technology can be Both Your Friend and Foe

There's no doubt about it. Computers and the Internet have changed our lives. They have positively impacted the way we shop, find, store and use information, and manage our personal and professional business. Unfortunately the important advantages computers and the Internet provide don't come without a clearly defined and an unfortunately well demonstrated element of risk...risk to our personal information.

Identity theft is running ramped with technology playing a key role. You see it in the news almost daily – “Stolen UC Berkeley laptop exposes personal data of nearly 100,000” or “FBI seeks stolen personal data on 26 million vets.” We can't control the security measures our employers and creditors take, but we can take important measures to ensure we're doing the best we can to avoid being an identity theft victim.

Secure Your Personal Computer

It's easy to be lax with the information we keep on our personal computers. Personal information, financial data and passwords all need to be protected to avoid their being stolen and used by an identity thief. Ensure that “passers by” can't access key ID and financial data by securing it with passwords. You probably don't know the background of the pest control person or the cleaning lady and without secure password protection, anyone with access to your computer could take a quick look and find data that they could use or sell to a hungry ID criminal. When creating these passwords, always use a combination of numbers and letters that will seem completely illogical to anyone but you. Don't use a birthdays, children's name, etc. They're too easy to figure out.

To help secure your computer from an Internet security breach, install Internet security software including a firewall. A firewall is a barrier that protects your computer from anyone who tries to access it from outside without authorization.

Become E-Mail Savvy

Email is an outstanding tool for communication, but we need to be aware of the potential for its misuse by identity thieves and act accordingly. There are two common ways criminals can target you via email:

- Phishing is an email fraud method where the ID thieves send you a legitimate looking email in an attempt to get hold of your personal and financial information. In a recent Federal Trade Commission (FTC) case, a 17-year-old male sent out messages purporting to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the “AOL Billing Center” link, however, they were taken to a spoofed AOL Web page that asked for personal information, including credit card numbers, personal identification numbers (PINs), social security numbers, banking numbers, and passwords.

To avoid being a victim of a phishing scam, never go directly from an email link into a web site with a form asking for your information. Always put the actual URL, not the one in the email, into your web browser and sign in directly. Potential phishing activity should always be reported to the company/ organization associated with the questionable email.

Related News

Stealing Home:
Izzard Hones ID Theft
in “Riches”

Conn. State Workers'
Info Ends Up on Web

Latest ID Theft Scam:
Fake Job Listings

SmartGuard Newsletter

- Spyware can be used to gather all types of confidential information and in most cases the user has no idea the information is being taken. Spyware lets the spy access everything you do online including usernames, passwords, online shopping purchases and e-mail or chat correspondence. In the hands of an identity thief this type of information is a deadly treasure trove. The spyware can get to your computer via an email attachment. To avoid inadvertently installing spyware on your computer, never open an email or email attachment from a sender you are not familiar with.

Surfing, Sharing and Passwords

Be careful what you do, where you go and where you buy. Your computer will warn you if you are about to enter a web site or page that is not "secure" meaning your information will not be encrypted to protect your privacy. Never input personal, password, financial or credit card information into insecure pages. Secure web pages will have an https:// web address rather than http://. The "s" means secure. Insecure web pages may also include a broken key symbol or an open padlock symbol at the bottom of your screen.



Are You a Victim?

Because most of us haven't been computer/internet security savvy from day one, it is possible that your personal information has already been jeopardized and a thief is waiting patiently for the right time to take over. If a criminal does get your personal information via the web, without an ID monitoring service to watch for changes and the use of your data, you may not become aware of the misuse of your identity until severe financial damage has already occurred. The thieves will take the information they obtained via the web to either recreate your identity for themselves or sell it to a third party for future use.

Stay on top of the use of your personal information. Don't become a victim.

Identity Theft Insurance

Once victimized by identity theft, restoring one's name and good credit is a time consuming and costly process.

For this reason, we offer an AIG policy in the amount of \$25K with a \$0 deductible. This coverage protects against the financial hardships associated with identity theft such as falsely incurred debt, lost wages, legal fees, and correspondence with creditors.

In addition to financial relief, policyholders have access 24/7 to trained identity theft specialists. These experts will aid victims in the recovery process until their crisis is completely resolved.