

Cyber-crime an epidemic which is anchored in identity theft, but gone far beyond it – is everyone's problem.

Today, cyber criminals are becoming more sophisticated and searching for bigger payoffs. Understanding the changing landscape and risks, while also constantly evaluating and re-evaluating your vulnerability, is critical to avoiding cyber-crime.

Cyber Threats

A first step in protecting yourself is to be aware of the potential for crime. With an increase of online activity, the popularity of social networking, and the increasing comfort level with the internet, criminals see opportunity. Following are the top five emerging cyber security threats for 2009.

- Malware – software designed to infiltrate or damage a computer system
- Botnets – groups of computers infected with malicious code and controlled by an outside master.
- Cyber warfare – the use of computers and the internet in conducting warfare in cyberspace.
- Threats to voice communications over the internet and mobile devices.
- The evolving cyber crime economy.

Understanding your Risks

Knowledge is power. In the information age it is imperative to stay informed about the types of cyber crime that you could fall victim to. There are a number of techniques that criminals employ to gain valuable information about individuals. The following are three categories of risk everyone should be aware of:

- “Whaling” – This technique target high net worth individuals and involves sending e-mails to money managers, financial advisors, and family offers. Often personally addressed, these emails include links that install malicious software.
- “Fake Caller ID” – Scammers use internet-based phone service to fake the caller IDs of banks and financial advisors. Because the phone ID bears the name of their bank or trusted advisor, victims are tricked into providing personal information.
- “Social Networking” – The internet and social media sites have made it far easier for both stalkers and scammers to learn about, and track, their intended victims.

How to Lock Out Hackers

- Many security experts advise against using wireless networks. Hackers can stake out your home and listen to your online activity.
- Don't leave your laptop computer in hotel rooms or places where others can access it. Hackers install a keystroke tracker which then transmits your account names, PINs, and passwords.
- Be aware that free email services, such as Gmail, available from Google, have been criticized by privacy groups because many of these services come with a program that scans the content messages and sends advertising.
- When you log on to your bank account or any other password-protected site that stores your personal information, be sure to log off when you are finished and close your browser completely.
- Run the latest version of a proven anti-virus software program on your computer.
- Do not respond to pop-up ads that alert you to a virus infection. Legitimate anti-virus companies do not use pop-ads to inform you about the status of your computer.
- Use passwords that are not easily guessed and do not share passwords with anyone.

Five Types of Identity Theft

While not new, identity theft is evolving and is typically the foundation for cyber liability.

- Department of Motor Vehicles – Use a victim's identity to obtain a drivers license.
- Social Security – Use of victim's social security number for employment purposes.
- Criminal Identity – Use of victim's information to escape fines or jail.
- Financial Identity – Use of victim's information to obtain vehicles, real estate and other goods or services.
- Medical Identity – Use of victim's name, social security number, or insurance coverage to obtain prescriptions or medical services which reduces the victim's available benefits and makes it harder for victims to obtain an accurate copy of their medical records.

How to Insure Cyber Losses

Insurers and brokers can take an active role in protecting the cyber security of their clients. The first step is educating the client on the risks. Many insurers offer identity theft restoration services, some of which are provided automatically at no charge, and others that can be added to one's homeowner's policy.

- **Buy a shredder that cuts your paper into confetti**
Thieves use discarded information to collect personal data on victims.
 - Credit Applications
 - Expired credit cards
 - Old bank and credit card statements
- **Eliminate unwanted credit solicitations**
Reduce the chance of fraud perpetrated on you by removing unwanted solicitations.
 - Contact 888-567-8688 and opt out of pre-screened credit card applications
 - Register for the national do not call list
- **Reduce access to your personal data**
In addition to “dumpster diving” thieves utilize a number of methods to secure personal data. Guard your information carefully both inside and outside your home.
 - Do not give personal information via email or telephone unless you have initiated the contact.
 - Do not carry your social security card with you.
 - Stop mail delivery when you are way from home to prevent a build up that ID thieves can remove.
- **Monitor your financial records**
Credit card and bank statements should be reviewed each month.
 - Secure cancelled checks and bank statements in a location with limited access.
 - Keep a record of all open accounts in the event you need to rebuild your ID.
- **Review social security benefits**
Review your annual social security benefits report for accuracy.
 - Review of your social security statement can highlight attempts to seek employment using your identity.
 - Contact 800-772-1213 to request earning and benefit statement.
- **Lock out thieves from entering via a cyber portal**
Access to the internet and personal computers should be treated like your front door.
 - Use passwords that are not easily guessed.
 - Do not share passwords with anyone.
 - Purchase virus, adware and firewall protection for your internet access.
 - If you have a wireless network make certain that access is encrypted.
- **Be prepared to protect yourself if ID theft occurs**
Copies of your financial records could prove invaluable in the event of an occurrence.
 - Organize your records and keep copies of all agreements, contact and account information.
 - Have contact information for all three bureaus available for immediate notice.
 - Experian – 888-397-3742
 - Equifax – 888-766-0008
 - TransUnion – 800-680-7289
- **Find out what insurance protection exists**
If you are not sure what coverage you have for this type of loss, contact your agent.
 - Insurance can mitigate some of the expenses related to restore your identity.
 - The cost surrounding this issue, such as time for the victim, is immeasurable and in general not insurable.

This information is provided for general information purposes only.

Sources include:

“Information Week Exposes the Internet Underworld.” Bloggernews.net, February 12, 2007
“Emerging Cyber Threats Report for 2009,” Georgia Tech Information Security Center
“Cyber Scams on the Uptick in Downturn,” *Wall Street Journal*, January 2009
“Beware of Facebook Scams,” Aaron Broverman, Bankrate.com, March 25, 2009
“Identity Theft: The Aftermath 2008,” Identity Theft Resource Center, May, 2009