Identity Theft: Evolving with Technology

The Internet and Our World

In today's world, people must keep up with technology in order to conduct their daily routines. They are required to adapt daily to new knowledge and exciting discoveries that are constantly changing the way they live and do business. Today, everything from saying hello to a friend down the street to videoconferencing with someone around the world can be done electronically, from home. Technological advances now allow people to carry out the most mundane of tasks, such as ordering groceries from the store, to the most complex activities, such as performing complicated surgery, all from a separate, remote location: a computer connected to the Internet.

Since its beginnings in the 1990s, the Internet has grown into a vast electronic network that now spans the entire globe, and it will only continue to grow. Because people use the Internet in their everyday lives, they rely on it for a safe and accurate exchange of information. Constantly, personal data such as Social Security numbers, credit card numbers, and passwords are traveling through wires, and also through the air, from one computer to another. With security measures in place to protect this sort of information online, most people feel safe on the Internet and trust that their personal information will remain confidential. But, unfortunately, criminals have also adapted to advancements in technology and, these days, people are becoming victims of crimes committed over the Internet.

The Evolution of Crime on the Internet

For years, criminals have been using discarded credit card receipts, bank statements, tax notices, and other bills (often found in the trash) to gain the personal information necessary to assume another person's identity. However, on today's electronic playing field, these criminals have used technology to devise cunning new methods of theft in the form of cyber crimes. Now, computer hacking and email scams known as phishing are included among the risks of sharing information online. Computer hackers are able to enter areas of the Internet where they are prohibited and hack in to another computer network. Once they are inside a computer's network, they are able to view documents, files, and confidential data and use it for their own personal gain. Phishing, on the other hand, is a method in which people are duped into providing their own personal data to a thief who is posing as a legitimate business or agency. Both of these cyber crimes have been steadily on the rise in recent years. In fact, according to the Wall Street Journal, there were more than 9.9 million cases of identity theft last year in the United States.

Hacking Into Your Life

One example of the growing computer hacking problem in which personal information was stolen emerged in February when an information broker, ChoicePoint Inc., announced that an identity theft ring had hacked into its database and gained access to hundreds of thousands of personal documents. Some of the information that was stolen included full names, Social Security numbers, home addresses, and credit reports. Many other large corporations such as T-Mobile USA were also recently hacked, and had their clients' information stolen. Even superstar Paris Hilton could not escape the threat of identity theft as her personal photos, text messages, and phone numbers in her personal directory were stolen by a hacker and spread across the Internet. The U.S. Senate will soon hold hearings to determine whether these corporations and information brokers require more extensive regulation.

Phishing - Don't Get Hooked!

Phishing is currently on the rise around the world as well. Phising works because scammers are able to construct bogus emails, pop-up ads, and even websites that appear to be from legitimate businesses or agencies. They inspire a false sense of trust, then send out emails asking for personal and financial data so they can steal identities. Some phishing emails may even install software on your computer that could be used to redirect your computer to bogus websites. Be extremely cautious of whom you trust with personal information on the Internet. You should know that legitimate businesses will never ask you to provide nor confirm any personal information through an email or pop-up message.

Tips to Protect Yourself and the Internet

The Internet can be a powerful tool, and the convenience it offers to manage business and recreation is invaluable. But theft and fraud are damaging the positive reputation of the Internet as a medium for business. Consumers are losing confidence in their own safety on the Internet, and fewer people are making purchases online these days.

However, there are steps that you can take to decrease your chances of becoming a victim, and to help catch cyber-criminals at work:

- Be aware that there are people online who would like to gain access to your personal information. Do not share this information unless you have initiated the exchange or are absolutely sure of who is receiving it.
- Install security and scanning software onto your computer to protect it from online hacking.
- Do not use your name, date of birth, address, or any other personal information for passwords. These passwords are easily cracked by hackers. In fact, it is suggested that for any password, you should not use a word that is found in the dictionary, as there are hacking programs that will attempt every word in the dictionary.
- Never disclose personal information in response to an email. Legitimate businesses would never ask you to do this. If an email or pop-up ad requests you to confirm personal information, even if it looks genuine, it is an example of phishing and should be reported to reportphishing@antiphishing.org, the attorneys at the Securities and Exchange Commission at enforcement@sec.gov, and to the Federal Trade Commission at uce@ftc.gov.
- If you are concerned about an email you receive from a company, contact that company by phone to verify the information. If there is a web link provided in the email, type it directly into your browser instead of using the link or copying and pasting it, as some links can be redirected to other sites.
- When giving personal information over a website, check to make sure that site is secure. Look at the first part of the web address in your browser. It should read https:// and not http://
- Regularly check your credit card and bank statements and keep track of your transactions. Also, log into your online accounts frequently. This way, you will be able to notice any changes to your account soon after it happens.

By taking these steps, you can greatly reduce your chance of having your identity stolen, and help to combat this growing problem. If you are careful not to reveal personal information online, and help to make others aware of the risks, you will be playing a part in making the Internet a safer place for all of us to communicate and conduct business. For more information on phishing and identity theft, visit www.antiphishing.org.