PROTECTING YOUR IDENTITY

No matter what you do online, there is always a risk that someone could glean enough private information about you to usurp your identity. Your financial credit affects nearly every facet of your life, so in order to maintain control over your information, the following tech tips are in order. There are several types of information that are appealing to thieves:

. Credit card numbers
. CW2 security numbers(those 3- or 4- digit codes on the back of your credit cards)
. Credit reports
. Social security numbers
. Driver's license numbers
. ATM cards
. Telephone calling cards
. Mortgage information
. Dates of birth
0. Online passwords
1. PIN numbers
2. Home/business addresses
3. E-mail addresses
4. Phone numbers

Compromised Accounts

When any of account is compromised, close it immediately. E-mails can "phish" for information about you. If an e-mail sounds like it is from Pay-Pal or your bank telling you there is a security concern, and you should click the embedded link to go the site to correct it, DON'T! These links are often tailored to take you to look-alike Web sites designed to trick you into entering your personal information directly into the malicious hacker's computer. What you should do instead is open your Web browser and manually type in the link to the Web site you wish to visit to check on your account (don't ever cut and paste a link). This is the only way you can be reasonably certain you won't be misdirected to someone waiting to prey on your information. Sometimes it isn't even your fault. The security at some companies that have your personal information is lax and vulnerable to a malicious hacker attack.

Low Tech Backups

In any case where you suspect that your information has been stolen, you need to be prepared and to have organized your paper bank records for at least one year. You will need to prove your account balance to the financial institution's fraud department as soon as possible. Detailed steps to take if your ID is stolen can be found at the following links:

The plan to follow if your ID is stolen
(FTC document) "When bad things happen to your good name"
U.S. Department of Justice ID theft kit

Online Passwords

The biggest Achilles' heels are online passwords. To protect yourself, always use combinations of upper and lowercase characters (including symbols and numbers) so that hackers who concentrate on commonly used words in the dictionary won't guess it easily. Use longer words with more characters and combine two words together with a symbol. You may even want to use words from two different languages so that automated password guessing tools won't work.

Computers aren't the only way thieves can get your personal information. Telemarketers are often hardworking people, but there are those who are persistent for the wrong purposes. If someone calls you and hassles you to give them your personal information, don't! Even if they sound legit, you never know to whom you are talking to over the phone.

Voice over IP Privacy

The Bush Administration is asking the Federal Communications Commission (FCC) to order Net telephony providers to comply with a law that would permit police to wiretap conversations carried over the Internet. Unlike regular voice calls, where wiretaps would have to physically connect to the line, VoIP could be tapped anywhere at anytime. The problem that forces us to sacrifice our privacy and rights stems from the FBI's belief that Internet telephone calls are a national security threat that must be countered with new police wiretapping rules. The way this would work is that the FBI would require broadband Internet providers to provide more efficient, standardized surveillance facilities, effectively changing the way Internet providers do business.

The reasons for these changes are because a terrorist could potentially use VoIP to circumvent legitimate wiretaps from calls being placed over the Internet. If terrorists can evade lawful electronic surveillance though technology, it puts everyone at risk. The real trick is to find a new way in which to effectively trace Internet phone conversations. The federal government is funding the development of surveillance tools through scientific projects that would allow police to identify whether suspects have been using VoIP to communicate secretly.

VoIP communications are hard to track. Think about the great expanse of the Internet where traffic can go literally anywhere. Vonage and ATT phone adapter boxes are portable and can be installed virtually anywhere in the world. You can take your box, plug it into the Internet halfway across the world and still receive calls on your local phone number.

Anonymity

If that's not enough, there are a number of services on the net that make your Internet traffic go through a special service that removes all tracing information, making you invisible or anonymous to the world. When such services are used, it becomes almost impossible to wiretap a call. The only way around this problem is to work with the VoIP providers directly by placing tracing information embedded within the VoIP call itself. In this way, if traffic is routed through an anonymous server, there is still a way to find out who the call is coming from/going to and trace the people on each end of the call. Privacy advocates, however, are infuriated by the federal government's initiatives to have the ability to tap our VoIP calls at will. They see this as a direct attack on our privacy. VoIP providers are nonetheless working with the FBI and FCC to facilitate the approval of wiretapping requirements so that the Internet does not become a haven for secret communications between terrorists and spies.

Source : http://www.geeks.com/techtips/2005/techtips-DEC15-05.htm