

Cybercrime is phishy business!

By Bruce A. Love

I recently received some great questions from a business class at our local High School. As a former college professor, it seems fitting that my first Q & A column features a question from a student!

Our student writes, “How can the average computer user protect himself/herself from cybercrime?”

The term cybercrime has different definitions depending upon which qualified expert you ask. In the broadest sense, cybercrime relates to the use of computers and the Internet to conduct any illegal activity. This includes activities such as credit card fraud, unauthorized access of computer systems (hacking), downloading or posting child pornography, software piracy, and cyberstalking, to name just a few.

I mostly associate cybercrime with identity theft. According to information published by the Federal Trade Commission, cybercrime affected nearly 10 million Americans in 2003, costing individuals and businesses approximately \$53 billion. There are several things you can do to reduce your risk of attacks against your identity.

- 1) DO NOT give out passwords, PINs, or any other personal information in response to e-mails you receive. Scam artists, posing as utility companies, banks, or credit card companies, send e-mails attempting to get recipients to give away information thieves can use. Never respond to e-mail requesting confidential information. Use a browser or phone to contact the legitimate company directly.
- 2) Check your credit report on a regular basis (at least once a year). This will not protect you from identity theft, but it will alert you to purchases made (and payments missed) in your name without your authorization. Credit reports are easily obtained from the big three credit bureaus: Equifax, Experian, and TransUnion.
- 3) Use a shredder or your fireplace to destroy old documents containing sensitive information. While trash picking or “dumpster diving” does not seem to fit the definition of cybercrimes, it is one way in which thieves steal identities.
- 4) Protect your social security number with your life. No other number is so closely tied to your identity. It amazes me that some colleges still use Social Security numbers for student IDs. What is wrong with this? When I teach, I have access to names and social security numbers for each of my students. Administrators, and even student interns, often are privy to this same information. When I distribute exam booklets, students provide me with signatures and student IDs to authenticate their Identity. If I sell this information for \$10 per name, I can make about \$20,000. Get my point? Colleges! Wake up and protect your students, or be prepared to show up in court to defend your negligent practices!
- 5) Defend your mother's name. Many credit card companies use mother's maiden name as an authenticating password. This information is not too difficult to obtain. Being married to a genealogy enthusiast, I know that some (other) amateur genealogists are so willing to share information on the Internet regarding family trees, that they post details about living relatives. This is a major breach of confidentiality. Advise your offending, though well-intentioned, relative not to post such information on public websites! Also, arrange with your credit card company to use a different password.
- 6) Use up-to-date antivirus software and spyware blockers.
- 7) Do not use a public computer (such as libraries and cyber cafes) to transmit sensitive information.
- 8) Review your bank statement monthly for suspicious activity.
- 9) Verify that your boss destroys confidential, information about employees, rather than tossing it in the dumpster.
- 10) Never send confidential information via unencrypted e-mail – even to trusted recipients.

These Q & A columns will be featured periodically to address questions from students, residents, and business owners. I look forward to hearing from you!

Love Consulting
600 Oakmont Place
Roaring Spring, PA 16673
814-224-2651

articles@loveconsulting.com

© 2004 Love Consulting