Identity theft – What could possibly be worse?

Identity theft has become one of the most rampant and sinister forms of crime. Although businesses can be affected by this type of crime, individuals have suffered the most.

Identity theft is defined by the US Federal Bureau of Investigation (FBI) as "… the misuse of another individual's personal identifying information for fraudulent purposes." Those fraudulent purposes include taking out a loan, applying for a credit card, using your bank account, and purchasing goods in your name. The end result is that the innocent victim may be on the hook for debts and purchases they have not contracted.

To put the risk of identity theft in perspective, the American Federal Trade Commission (FTC) estimated that 8.3 million American consumers were victims of identity theft in 2005. The FTC also estimated that an impressive 200 million hours were spent by those victims attempting to recover from identity theft, meaning that individuals need to spend an enormous amount of time rectifying the damage.

Have you been phishing lately?

A very common and unfortunately successful identity theft technique is called *phishing*. Phishing, which is pronounced just like the aquatic activity, can be defined as "… masquerading as a trustworthy entity in an electronic communication". This is aimed at attempting to *hook* unsuspecting individuals by getting them to reveal personal and financial information. Many phishing attacks start with an email. The individual receives a bogus notification from a bank or popular online service such as eBay, which asks the person to log onto their online account. The message specifies that unless they logon immediately, their account will be suspended or cancelled. The email provides a link to click on to perform this task. This is where things go wrong: when the individual clicks on the link, they are directed to a web site which is a replica to the legitimate web site. The replica is a pirate site which has nothing to do with the legitimate web site. Once on the web site, the individual is requested to enter information such as their debit card number, PIN, password, date of birth or other such information. If the individual enters this information, serious issues may arise since the *phishers* now hold sensitive personal data. *Phishers* send out millions of these emails and are successful even if only a few individuals give them the information they request. If you think an email you received is a phishing attack, simply delete it. If you think it may be valid, consider this: most financial institutions will not send such requests by email, it is better to contact them in person or by phone to confirm the validity of the email before proceeding with the request.

Secure your computer

Use of the Internet is one of the most common sources of identity theft. In order to protect yourself, it is important to know what risks there are. Programs such as spyware and viruses are capable of quietly infiltrating your computer. They may be monitoring what you're typing and then sending the information to an identity thief. As such, it is important to have up-to-date anti-virus, anti-spyware and firewall software installed on your computer. Also, keep your computers operating system up to date with vendor updates and make sure you are using an alphanumeric password with at least eight characters.

Organizations are not immune to identity theft

Organizations should make sure their employees are familiar with the risks of identity theft by discussing these risks in internal newsletters, presentations and other relevant forums. Why should companies be worrying about identity theft? Consider the following: If a finance department employee gives out the company's banking information because of a phishing attack, the company then becomes a victim. Along with employee education, companies should make sure that an email filtering application is in place to capture spam and phishing e-mails before they reach the employees, since phishing e-mails are often very convincing.

Paper trails

Remember to properly destroy all discarded confidential documents. Any document which contains names, addresses, financial information, dates of birth and any information which can identify someone personally could be used to steal an identity. To avoid this, individuals and organizations alike must make sure they shred all of these documents with a paper shredder. There are also professional organizations which can shred large volumes of documents for a fee.

The key is to protect your information diligently and only give it to organizations or individuals you trust.

I invite readers to contact me with any information security related questions. I will also be happy to meet with organizations that have IT security concerns and who wish to discuss them in a confidential manner. Please e-mail me at michoschumann@kpmg.ky or telephone on 949 4800.

Micho Schumann is a Senior Manager with KPMG's IT Advisory group in the Cayman Islands and can be contacted at michoschumann@kpmg.ky or on 949-4800 for information security questions and Information Security consulting services. He holds a Masters degree in Information systems, is a Certified Information Systems Security Professional (CISSP) and a Certified Information Systems Auditor (CISA). He has over seven years of IT security experience working extensively with financial institutions, government agencies and high-technology firms.

- Ends -