SECTION 12
MY ONLINE PRIVACY & PC SECURITY

12. MY PRIVACY & SECURITY

12.1 IDENTITY FRAUD

Identity fraud involves pretending to be someone else in order to steal money or other benefits. The person whose identity is used may suffer various consequences when held responsible for the perpetrator's actions. Australia has laws in place at both federal and state level to prevent the misuse of personal information and data.

Identity fraudsters will use various methods to gain this information: via the use of phishing (see Section 12.2), the use of Spyware (see Section 13) and the interception of un-encrypted internet communications (see Section 12.3).

Caution should be taken with revealing sensitive information over unsecured networks or on computers without an appropriate level of protection (public computers should be treated with extreme caution).

12.2 E-MAIL SECURITY

Some things to be aware of with your e-mail:

- Phishing: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication – never click on a link in an unsolicited email that takes you to a site that then asks you to enter sensitive information
- E-mails containing suspect attachments which may contain spyware or malware like Trojan horses
- E-mail messages transit through unsecured servers and intermediate computers where it is possible for unencrypted messages to be intercepted and read
- Many Internet Server Providers (ISPs) store copies of messages for back-up purposes

In general terms, e-mail is about as secure as a postcard through the mail.

12.3 SECURITY CERTIFICATES/SSL/TLS

Transport Layer Security (TLS) Protocol and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over networks such as the Internet. Several versions of the protocols are in wide-spread use for web browsing, e-mail, instant messaging and voice-over-IP (VoIP).

Part of this process involves buying a security certificate for the web site (used in identity verification and data protection) from a third party Certification Authority. Certificates are only valid for a finite period of time and then must be renewed. A site with an expired security certificate should be treated with caution by users, but may still be browsed, as long as the user exercises appropriate care with the level of sensitive information revealed (as the communication may no longer be secure).

A secure/encrypted network connection may be detected by the presence of a padlock in the browser taskbar (not on the actual web page). This will be positioned at either the top or the bottom of the browser.

12.4 PASSWORD & PIN SECURITY

Some standard precautions to take with your PINs and passwords:

- Password complexity – use a combination of letters and numbers – don't use the names of family or pets!
- Regularly change your password – even if you just change the number/s in your password
- Never reveal your password/PIN to anyone and don't keep a written record in your wallet or purse
- Do not use the same password/PIN for everything. If you want to limit the number of passwords/PINs you use, then create a small group that you use for specific purposes

12.5 SOCIAL NETWORKING

While sites like Facebook, MySpace and the various blogging sites offer exciting social networking opportunities, some care should be taken to ensure that the user doesn't unnecessarily expose themselves to the risk of security or privacy violations.

Prior to setting up a profile (which usually requires the user to enter a certain degree of personal information), users should familiarise themselves with the privacy settings offered by the site, and ensure that their profiles are set up in such a way that suits their personal privacy needs.

Be aware that many sites retain the personal information you enter even if you deactivate or delete your profile. While this information can generally be withheld from general public access (as with Facebook), the data is online and is potentially vulnerable.

The level of personal information revealed can be used for identity fraud purposes (see Section 12.1). Users should be wary of revealing information that might help identify PINs or passwords, or making information like your date-of-birth and full address visible.

There is also the matter of personal privacy. Unrestricted sites can be searched by users (maybe even prospective employers) looking for background information on an individual. If you value your privacy, then you should be careful about the type of information you make available in these circumstances.

12.6 COOKIES

Cookies are used for authenticating, session tracking and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts. Cookies have been an internet privacy concern because they can be used for tracking browsing behaviour.

Cookies are not computer programs. They are parcels of text sent by a server to a browser and then sent back unchanged by the client each time it accesses that server, and are unable to perform any operation by themselves. In particular, they are neither spyware nor viruses, although cookies from certain sites are described as spyware by many anti-spyware products because they allow users to be tracked when they visit various sites.

Most browsers allow users to decide whether to accept cookies, but rejection makes some websites unusable. For example, shopping carts implemented using cookies do not work if cookies are rejected.

12.7 R.U.N.S.A.F.E. (PC SECURITY)

R.U.N.S.A.F.E documents key information regarding the safe and secure operation of desktop computers. The R.U.N.S.A.F.E concept and documentation has been adapted to suit the Victoria University environment. The R.U.N.S.A.F.E acronym is made up of the following:

- R - Refuse to run unsafe programs
- U - Update software regularly
- N - Nullify unneeded risks
- S - Safeguard our identity and passwords
- A - Assure sufficient resources for proper system care
- F - Face insecurity
- E - Everybody needs to do their part

The goal of R.U.N.S.A.F.E is to help you attain the knowledge and skills necessary to more safely operate a network connected computer.

For more information see: http://intranet.vu.edu.au/its/Awareness