SAFE COMMUNITY

CYBERCRIME – MINIMIZING THE RISK

|| Part 2

David Thomas

IT is a sobering fact that since the publication of part one of this feature last week, some 4.2 million Facebook accounts will have been compromised and some 10.5 million people will have been a victim of cybercrime.

This feature provides advice on simple steps to take to minimise the risk of cybercrime although it is acknowledged by experts that even with the most sophisticated security systems it is impossible to eliminate the risk completely.

Secure your computer

A leading academic once described good online security "is like having a professional bodyguard working discreetly in the background, but there to spot all signs of danger and ready to step in to protect you against the attacks you expect and those you were never aware of."

It is important to have anti-virus software for your computer, but how do you choose? This can be a complex subject but independent expertise is available for example through ICSA Labs (www.icsalabs.com) where virtually every anti-virus product is described and tested and PC Advisor (www.pcadvisor.co.uk/test-centre). PC Advisor has just reviewed the top 5 anti-virus software products in the UK and this is worth checking before committing to buy. Your software should guard against breach of firewalls, malware and spyware attacks. Beware of rogue anti-virus programmes.

Also consider using a product such as C Cleaner for cleaning Windows PC. It protects your privacy online and makes your computer faster and more secure. It is easy and fast to download and is free from www.piriform.com/ccleaner

Passwords

It is important to carefully select and manage your passwords by avoiding using actual words found in a dictionary; names; user name; sequential numbers particularly 1234; telephone number; and in fact anything people could guess as belonging to you. They should not be shared with others or written down. Strong passwords should be a minimum of eight alpha numeric characters and easy to remember. Use different passwords for each account.

Safe use of the internet

Closing your browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button. Avoid using the option of "remember" your username and password information.

Read the fine print on website privacy policies. On many social networking and photo sharing sites, there is wording on the privacy policies that allow the website to keep information and photos posted to the site, sometimes indefinitely, even after the original has been deleted by the user.

Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Public Wi-Fi and "Hot Spots" are particularly vulnerable, so avoid conducting financial or corporate transactions on these networks. Ensure when you use computers in business centres in hotels that you log off completely.

> *"Always terminate your online session by clicking on the 'Log out or Sign Out' button"*

To protect your identity be cautious when giving out personal information such as your name, address, phone number or financial information on the internet. Make sure that websites are secure or that you've enabled privacy settings (e.g. when accessing/using social networking sites). Be careful what information you post online. Once it is on the Internet, it is there forever!

Safe use of online dating sites

With an increasing use of such sites the possibility of becoming a victim of cybercrime has increased. These include stalking and harassment, spams, fraud, blackmail and people masquerading as someone who they are not.

To guard against this, choose a site that will protect your anonymity until you choose to reveal personal information and will enforce its policies against inappropriate use. Run a Google image search on the photos in profiles you receive, to ensure they have not been stolen to create a fake profile.

Make sure that you are always in control of what happens. Do not let anyone pressure you into giving away more information than you feel comfortable with, particularly personal information, such as phone numbers.

Be extremely wary about removing clothes or doing other things in front of your webcam that could be used against you – even if you think you know the other party.

As a second line of defence for your privacy, set up a separate email account that does not use your real name. Make sure your phone number is 'blocked' to people you contact on dating sites. Pick a user name that does not include any personal information.

Protect your data

Use encryption for your most sensitive files such as tax returns and financial records, make regular back-ups of all your important data, and store it in another location.

Review financial statements regularly; reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted.

Avoid being scammed

Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

Safe online shopping

In addition to practicing safe surfing, you also need to be careful where you shop online. Look for a trust mark to tell you if a site is safe. And when you're on a payment page, look for the lock symbol in your browser, indicating that the site uses encryption to keep your information safe. Check the site starts with "https://" instead of "http://" as this indicates the site uses encryption. When paying, use a credit card instead of a debit card as the card issuer may reimburse you if the site turns out to be fraudulent.

Finally

If you need to have any work done on your computer ensure that the technician is fully trusted. If you are a victim of an online crime or encounter illegal internet content (e.g. child exploitation), report this to your local police.

|| features@algarveresident.com

David Thomas is a former Assistant Commissioner of the Hong Kong Police, consultant to INTERPOL and the United Nations Office on Drugs and Crime. In October 2011 he founded Safe Communities Algarve an on-line platform here in the Algarve to help the authorities and the community prevent crime. It is now registered as Associação Safe Communities Algarve, the first association of its type in Portugal. 913 045 093
www.facebook.com/scalgarve
www.safecommunitiesalgarve.com