SAFE COMMUNITY

CYBERCRIME – IDENTIFYING THE THREAT

|| Part 1

David Thomas

TO many people crime prevention is about securing your home by installing alarms, gates and window bars. Although still important, there is now a more sinister type of crime threat where the culprit cannot be seen, there are no boundaries and the results can have devastating consequences on individuals, organisations and even governments.

This is the world of cybercrime.

This increasing threat is mirrored by the fact that many matters currently being brought to Safe Communities Algarve's attention by residents come under the cybercrime umbrella.

In this two-part feature, I will attempt to explain what is cybercrime, how extensive it is and what can be done to help avoid becoming a victim. This article deals with the types and extent of cybercrime and part-two will cover ways to minimise the risk to you.

Cybercrime generally covers: computer viruses or malware; a phishing message; online harassment; hacking into a social networking account; being approached online by sexual predators; online scams; online credit card fraud; identity theft; cyber bullying; smishing (which is phishing through SMS messaging) and ransomware.

Globally, cybercrime is the fastest growing crime. Criminals know that it's easier and more profitable than "physical crime" and the probability of being caught is lower.

In a study undertaken by Norton it was found that the annual cost of cybercrime in 2012 was US$338 billion compared with global drug trafficking at US$411 billion.

Estimates are that the number of cybercrime victims per year is around 430 to 550 million and some 54% of all adults using the internet have experienced a virus or malware on their computer.

Cybercrime can originate from anywhere in the world. In February 2013, some 2.4 million cybercrime attacks originated from Russia, 907,000 from Taiwan, 566,000 from Ukraine, 350,000 from Romania and 165,000 from China.

Some examples of cybercrime attacks

Victims of cybercrime can be anyone. In March 2013 it was reported that as many as 15 celebrities, politicians and top government officials, including US First Lady Michelle Obama and FBI Director Robert Mueller, had been targeted by internet hackers who have posted their social security numbers, credit card account numbers, and banking information on websites originating out of Russia.

Banks are one of the leading targets for cybercrime attacks and spend millions in preventative security. However, cyber criminals are equally determined to circumvent their comprehensive security systems.

In March 2012, fraudsters initiated transfers totalling €35 million from 5,000 Dutch business accounts based in two banks. A study identified 60 servers processing thousands of attempted thefts that initially targeted consumers before moving onto businesses.

Only two weeks ago eight cyber criminals were arrested after hacking into the computers of a Barclays Bank branch in London by pretending to be information technology engineers. They then planted devices and a GSM (transmitting device) which allowed them to remotely control the bank's computers, transferring over £1.3 million to their accounts. In September the Metropolitan Police detained 12 men over an attempt to hack into Banco Santander SA computers, preventing a theft potentially worth millions of pounds.

Phishing

In the Algarve, there seems to be an increasing number of people who have experienced phishing attacks. Phishing is an attempt, normally through an email spoof, to get you to disclose personal information such as passwords to someone masquerading as a legitimate entity.

These emails often contain links to websites infected by malware, a software design to disrupt your computers operations. Examples include phishing attacks under the names Microsoft; HSBC; Halifax Bank; Amazon; Santander Bank; PayPal; Millennium Bank; Lloyds Bank; HM Revenue and Customs, Barclays Bank and bogus emails from friends saying that they had been stranded overseas and need your financial assistance.

Social networking sites

The use of social networking sites provides opportunities that can be exploited by cyber criminals. A survey conducted in early 2013 found that 600,000 Facebook accounts are compromised everyday, and that one in 10 of all social network users said they had fallen to a scam or a fake link on a social network platform.

Norton noted that 40% of social network users had been a victim of e-crime on social networks; 17% of social network users reported that someone had hacked into their profile and impersonated them; 10% had been victims of scams or fake links on social networks.

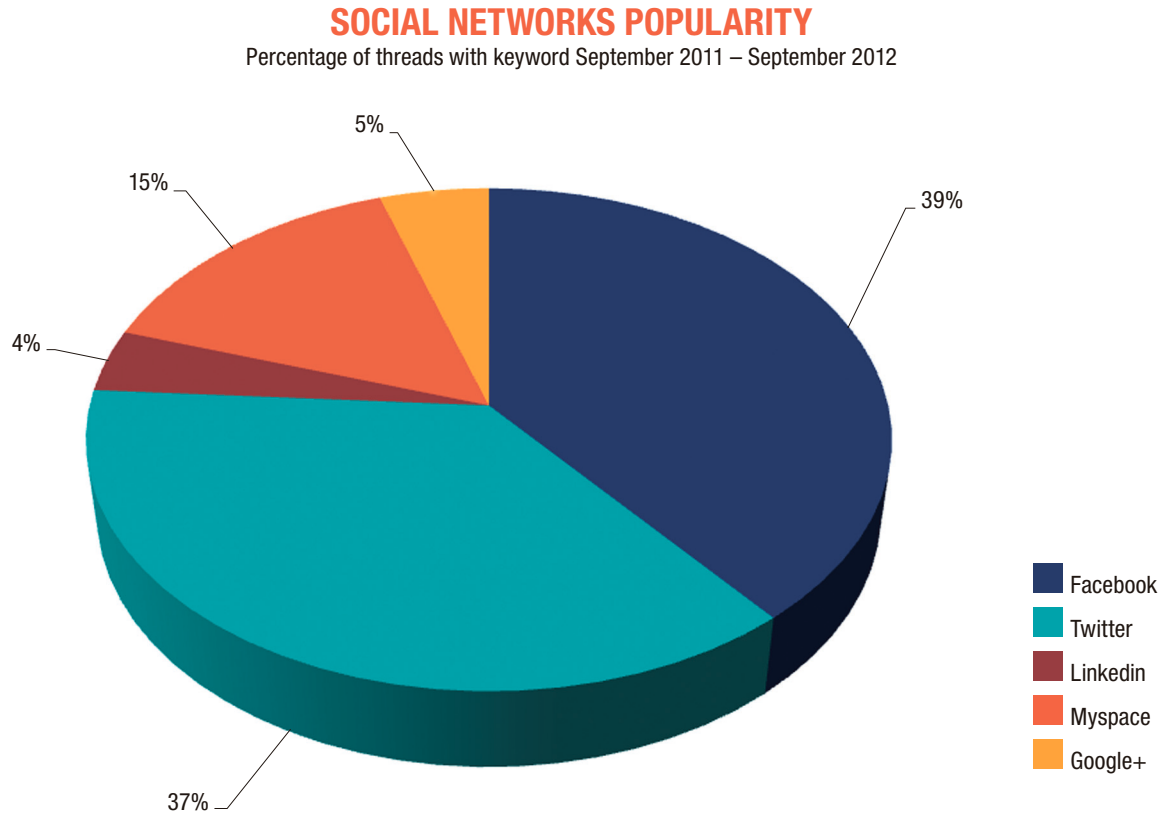
Alarmingly 19% of respondents had been notified that their password had been compromised and needed to be changed. When you realise that there are 33 million Facebook users alone in the UK and a billion worldwide, the extent of malpractice is alarming.

In a recent UK House of Commons debate, the conversation threads on one of the internet's largest hacker forums (it has a membership of 250,000) and a number of smaller forums was presented. It found that social networks were of increasing interest to online hackers.

Facebook was the most popular platform discussed by hackers, featuring in 39% of conversations, followed by Twitter – 37%. Other sites featured can be seen from the chart. A common request in these discussions was for assistance in hacking into an individual's social network profile, either to spy on them or for revenge.

I hope this is not too depressing reading, but unfortunately the effects of cybercrime, whether social, political or economic, cause havoc to individuals. Some typical negative online experiences that people have encountered are listed in the table. Take the test and see how many of these you have experienced yourself? It is important to minimize the risks by taking steps now before it is too late.

Next week: Cybercrime Part 2



|| Negative online experiences

Take the test

How many of these would you answer "yes" to?

For all:

- I inadvertently downloaded a virus to my own or to my family computer
- I've been bullied or harassed online on a computer or smartphone
- I responded to an online or email scam, phishing or smishing message thinking it was a legitimate request
- I experienced a ransomware pop-up demanding money to unlock my computer
- Someone has hacked into my social networking profile and pretended to be me
- I have seen very violent images, videos or games online

For children/teenagers only

- Another child or teenager I don't know online tried to get me to meet them in the real world
- An adult tried to get me to do something online I thought was wrong
- Another child or teenager tried to get me to do something online I thought was wrong
- I received sexually suggestive or nude images of someone I know/do not know on my smartphone
- An adult I don't know tried to add me as a friend on a social networking site
- Another child or teenager I don't know tried to add me as a friend on a social networking site

|| 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