EnglishWaves.fr
The French radio station that speaks English !

TechTalk

Cyber Security, Part 2 ©

by John McCarthy

Hi and welcome once again to Tech Talk. Last time we looked at the dangers posed by hacking and DDoS attacks. Well, phishing has also become one of the most popular kinds of cyber criminality. This is a form of fraud in which the scammer tries to obtain information, such as log in credentials or bank account information, by masquerading as a familiar entity or person. Generally, the potential victim will receive an e-mail purporting to be from a well-known company, which includes logos and other identifying information taken from that company's website. In my own personal case, heinous attempts were made to separate me from my ill-gotten gains by con-merchants passing off as my bank and Internet Provider. The links within the body of the mail make it appear that they go to the official website in order to trick the targeted prey into divulging personal information such as passwords, credit card details and bank account information. Phishing has gained in popularity with cybercriminals because it's become far easier to trick an unsuspecting victim into clicking a malicious link rather than trying to break through a computer's firewall and antivirus defences. The best way to avoid this scam is simply to ignore any e-mail requests for personal information such as pin numbers and banking details.

Another popular cybercrime is identity theft. This is becoming an increasingly common problem in Europe as fraudsters discover an unprecedented number of ways to get hold of the information required to steal someone's identity. Basically, identity theft involves the perpetrator of the crime taking the victim's personal information and then using this illegally for his or her own personal gain. Information often targeted by identity thieves includes date of birth, address, e-mail address, previous addresses, mother's maiden name, pin number, bank account details and of course passwords. The most common types of crime are, unsurprisingly, of a financial nature, such as credit card fraud, bank and telecommunications fraud. However, criminals can also use your identity to commit a wide array of offences such as entering a country illegally, smuggling, committing cybercrimes, laundering money, trafficking drugs and generally committing almost every imaginable crime in your name.

It's almost impossible completely to prevent identity theft, but there are sensible precautions you can take to reduce the likelihood of becoming a victim. Always bear in mind that the advent of social media has facilitated matters considerably for identity thieves, so ensure you protect your data by checking your privacy settings on social media. Without wishing to push you into pointless paranoia, also make sure you completely destroy all documents containing personal data rather than merely consigning them to the rubbish bin.

Rather disturbingly, a surprisingly large number of people believe that smartphones are scam-immune. WhatsApp users in the UK were very recently targeted by scam messages from one of the victim's contacts encouraging them to click on a link in order to receive £100 worth of vouchers. Having clicked on the link, scammers could collect personal information from the device, install tracking cookies and perform a whole host of undesirable manipulations.

As smartphone technology continues to evolve, it also paves the way for an increasing amount of mobile phone scams. These scams can cost their victims anywhere in the range of just a few Euros to their whole life savings, so it's always better to be safe than sorry.
Security experts recommend three common-sense ways of staying safe:

1 - Don't connect to a suspicious Wi-Fi network

- When away from home, set your Wi-Fi to 'ask to join networks' so you're conscious of the network you're connected to.
- Don't pay for temporary Wi-Fi access, especially in airports. It could be a scam to get your credit card information.

2 - Don't respond to text messages or calls from unknown sources

3 - Make sure you only download apps that are well known and trusted

- When using banking or credit card apps, make sure you're connected to a trusted Wi-Fi network.
- Log out of accounts and close apps when you're finished.