Have I been scammed?

It has been some time since I covered the subject of cybercrime, but with some recent cases being referred to us at Safe Communities Portugal, now is a time for a reminder of how this can affect our daily lives and what preventive measures we can take.

Firstly it is important to realise that if you do receive an email that is a scam, it not because your email address has been selected from millions. In most cases such emails are randomly generated.

The extent of scams in circulation is alarming and growing. It is a global issue and is as relevant in Portugal as it is elsewhere. Cybercrime does not respect national boundaries. Alarmingly this comes as fraud offences continue to rise. For instance in the UK residents are now more likely to be victims of fraud and cybercrime than any type of offence, according to the Office of National Statistics. Fraud and cybercrime offences are now ten times more common than burglary.

In the UK Action Fraud recorded 48,981 frauds in 2017-18 affecting people aged over 60 - equivalent to nearly six crimes every hour, this was up from 25,659 reports in 2015-16. Which UK however reported September 2018 that more than 96% of cases reported to Action Fraud go unsolved.

The growing scale of online fraud suggests that many people are still not aware of how to keep safe online and that there is more to do to change citizens' behaviour.

Two of the most common forms of cybercrime are phishing and ransomware, usually delivered to you by email or, on social media through messages for example.

Phishing

This is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information and money. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or banks. The e-mails state, often with a degree of urgency, that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail.

Scammers can also use a technique called spoofing to make it appear as if you've received an email from yourself. Never reply to an email that asks you to send personal or account information, or click links that supposedly take you to a company website, or open any file attached to a suspicious-looking email.

Ransomware

This is a type of malicious software that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. There are several different ways that ransomware can infect your computer. One of the most common methods today is through a malicious spam, which is unsolicited email that is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.

The number one rule if you find yourself infected with ransomware is to never pay the ransom. If you are infected restore any impacted files from a known good backup. Restoration of your files from a backup is the fastest way to regain access to your data.

Something a little more sinister

One fine (or not so fine) day, you check your inbox and discover a message that starts like this:

“I’m aware, ********** is your password. You don’t know me and you are probably thinking why you are getting this email, right? Well, I actually placed a malware on the adult video clips (porn) web site…”

In reality, there is no omnipotent “virus” or shameful video. How does someone know your password? Simple: The blackmailer has got hold of one of the many databases of user accounts and passwords available on the dark net, leaked from a variety of online services. Alas, such leaks are not uncommon — in the United States alone, no fewer than 163 million user records were compromised in just the first three quarters of 2017.

As for “knowing” that you’ve been viewing adult content, it’s a shot in the dark. The e-mail you received was sent to thousands, perhaps millions of people, with the addressee’s password automatically merged into the message from the database. Even if only a few dozen recipients pay up, that will be more than enough for the scammer.

In this case NEVER reply, simply delete and block and NEVER ever pay.

Difficulties faced in combatting on-line fraud

The international and ‘hidden’ nature of online fraud makes it difficult to pursue and prosecute criminals because of the need for international cooperation and an ability to take action across borders. Although investigators may have cutting-edge technologies to track down online or telephone fraudsters, it’s an uphill struggle.

Prevention

Check your email addresses through https://haveibeenpwned.com/ This excellent facility will show if your email address and passwords have been compromised. If so consider changing your password.

Use strong passwords and do not use the same password with your other accounts.

Never provide personal information when answering an email, unsolicited phone call, text message or instant message.

Use reputable antivirus software and a firewall. Maintaining a strong firewall and keeping your security software up to date are critical. It’s important to use antivirus software from a reputable company because of all the fake software out there.

Do make sure that all systems and software are up-to-date with relevant patches. Exploit kits hosted on compromised websites are commonly used to spread malware. Regular patching of vulnerable software is necessary to help prevent infection.

David Thomas

President Safe Communities portugal