RANSOMWARE EXPLAINED

The terms “virus”, “hijacker”, “malware”, and “spyware” have been bandied about for years where most PC users have been aware of them but another lesser known term recently assaulted about 300,000 users worldwide: “ransomware”. This global ransom nicknamed “WannaCry” gained importance because it affected major companies and institutions such as Telefonica of Spain and the UK’s health care system. The perpetrators of this act are still unknown (although there are suspects) and like other hackers they are technologically advanced, globally connected and very smart. In less than 3 hours they had already infected users in 11 countries so they are very quick to spread.

What is ransomware? As it implies it is malicious software that locks a computer, tablet or smartphone and demands a ransom to unlock it. The first known case appeared in 2005 so it is not that new. How it affects your device? The software is usually contained within an attachment to an email that masquerades as something innocent…therein lies the danger as the hackers are counting on your innocence and trust to open your personal mail and click on that particular link. For example mail from a major bank, utility company, your email provider or even your own organization may not really be from them….it just ***looks*** that way…but seriously how often do you **really** get mail from your bank, electric company or mail provider that is not advertising,? Being suspicious of the source could save you a lot of grief and money. Downloading a bad program or app and visiting illegal websites or those displaying malicious ads can also open the door to this software.

Once opened the software encrypts the hard drive and it is becomes impossible to navigate, access or retrieve anything stored such as your personal documents, photographs, or music. In order to unlock your device, the victim must pay a ransom which amount varies anywhere from €200 - €500 although there is never a guarantee that you will get access back or if you do that your data is still intact. The hackers allow a few of days for payment and if none is made the victim's personal files are deleted. In this latest incident payment had to be made in ***Bitcoins*** (virtual but real currency: 1 Bitcoin = €1907.14 / $2133.25 / GBP1641.11)…yet another world of unknowns to many but all too real.

How can you protect yourself? Being aware and wary of where you navigate and what you click on is the first habit to develop. Installing a paid (forget free),reputable and all-inclusive anti-virus software can protect you in the majority of threats. It was found that in this latest episode no users of these programs were affected because the malicious links were deemed inoperable. And finally, get in the habit of backing up your personal data on a regular basis (preferably once a month if you are a daily navigator).

Life with the internet is a given fact today but being a victim of crime is not.