CYBER-CRIME

Over the past few years we hear more and more about Cyber-crime and the threats it poses mankind in the 21st Century. However, to the majority of people and certainly those of us working outside of IT departments, little is known about this 'global threat'.

According to the dictionary Cyber is defined as relating to information technology, the internet and virtual reality. Meanwhile 'Cyberspace' refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks in communication and data exchange activities.

This threat was recognised in the UK when, in 2010, the National Security Council announced that hostile attacks upon UK cyberspace would be considered a Tier 1 threat to national security, along with International Terrorism, natural disasters and International Military crisis. Further information regarding the UK Security Cyber Strategy can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Therefore every time you or I use our smart phone, home computer, lap-top, email or social networking sites we are entering cyberspace and as such opening ourselves to threats from crime. Some of the techniques utilised in cyber attacks are:

• 'Social Engineering' - whereby hackers trick you and I into offering them access to information and data. Terms such as 'Phishing', 'Whaling' and 'Smishing' cover these and examples are fraudulent emails asking for passwords, or credit card information, or instructions to download a certain program (normally to answer a false invoice you were sent previously), which then gives the criminals access to your phone/computer.

• 'Malware' - whereby hackers disrupt communication systems through attacks using malicious software such as 'viruses' and 'worms', etc.

• 'Local/Physical Access' – whereby hackers breach our security by stealing passwords written down/stored in wallets or diaries etc. Mobile Phones & Lap Tops stolen with important data and insufficient security credentials such as a strong password.

• 'Network Attack' – whereby hackers will try and gather passwords and other sensitive information by setting up malicious websites, breaking into Wi-Fi networks or disguising malicious software which we then download in good faith.

HOW CAN WE INCREASE OUR PROTECTION AGAINST THESE THREATS?

• Ensure credentials such as username, passwords etc. are not stored with a device, such a lap top or mobile phone, as they are open to theft or tampering

• When using a device in open spaces beware of being overlooked i.e. tailgating

• Minimise the amount of information stored on a device

• Change passwords on a regular basis and do not use the same password for all programs

• Take care before opening an email where you do not recognise the sender or the email starts with Dear Sir/Madam rather than your name

• Beware of emails/calls asking you to give information such as account numbers, passwords, etc.

• Follow the router manufacturer instructions for securing your home based Wi-Fi networks

• Turn off your router when you are away to deter possible hacking attempts

There are various websites to guide us on protection including:

https://www.getsafeonline.org/ways-you-work/mobile-and-home-access/

https://www.getsafeonline.org/protecting-your-computer/physical-security/

Alresford and District Neighbourhood Watch Association website-
www.neighbourhood.watch.alresford.org
e-mail – contact.adnwa@gmail.com

CRIME IN PROGRESS — 999
NON URGENT – 101
CRIMESTOPPERS – 0800 555 111