Crime prevention advice for

Common Threats

Although it is important to educate yourself on how to protect your businesses, it is also important to help you understand what you are protecting yourself against. Showing you these is not designed to increase the fear of crime but to increase your knowledge base so you are better prepared to understand the world of cyber security. Some of the most common threats are seen below.

Phishing
Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party (cyber criminal). It is often carried out via email, masquerading as a legitimate source but in fact is looking to steal personal details such as login information. It is often difficult to distinguish between legitimate and phishing emails but often clues give them away such as spelling mistakes, unusual attachments or emails that are simply from a business or source that you have never had dealings with.

Spam
Spam, unlike phishing which has the intention of causing significant harm, is sent to try and get the recipient to visit a certain website for sales or to drive up website visitor numbers. Spam can sometimes be linked to fraudulent means so it is important to be cautious when opening a spam email.

Malware
Malware is a general term for malicious software. Malware includes viruses, worms, Trojans and spyware. The software is used to gain unauthorised access to computers and can gather sensitive and private information.

Virus
A virus is a file that runs on a computer, sometimes it is visible but sometimes it runs in the background without being noticed. There are a variety of viruses, including worms and Trojans. Worms are designed to spread from computer, infecting every computer it passes through. Trojans are malicious programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

Adware
Adware should always be treated with caution. Adware delivers advertisements by tracking your usage and can redirect you to unwanted website. It can often come with free software that you install and unless it notifies you that it is collecting data from your computer then it should be considered malicious.

Ransomware
Ransomware is a form of malware where criminals can lock your computer and display a message demanding a certain amount of money to be aid otherwise they will wipe your computer of its data. Ransomware is often activated through human error, opening a corrupt email attachment or visiting an infected website so it is important to ensure all staff are aware of online security to at least a basic level.

Distributed Denial of Service (DDoS)
A denial of service attack often targets websites. A denial of service attack uses one computer to flood a network meaning no one else can access that network. A Distributed Denial of Service attack involves multiple computers, often botnets (a network of infected robot computers) being used to flood the network. This is often used as a temporary attack to prevent the use of a website or other online systems run by a business but these are often large corporations who are victims of a targeted attack.

Things to consider:
Cyber Essentials
Cyber Liability Insurance (This comes with the completion of Cyber Essentials)
Firewalls and Internet Security Protection (Anti-virus)
Backing up of data

For more detailed information on the above you may like to visit the following or look at some of the other advice sheets on the Warwickshire Business Watch website:

Get Safe Online – https://www.getsafeonline.org/
Cyberstreetwise - https://www.cyberstreetwise.com/

Reporting Business Cyber Crime
If you have been or believe you have been a victim of Cyber Crime please report it directly to Action Fraud. This can be done by visiting www.actionfraud.police.uk or calling **0300 123 2040**.
Action Fraud is not an emergency service, in case of an emergency please dial **999**.