

Basic Digital Safety

Introduction: Protecting all your devices is very important. Especially from viruses, malware, online scams and hackers. According to The Metropolitan Police, with the internet at the centre of daily life, it's inevitable that there are many types of fraud to go along with it. (Metropolitan Police, 2024) This can be anything from identity theft, online transactions, dating scams and more.

Photo from Bing.com/images, 2024



It is vital that you take precautions when online. People online can be vulnerable and be manipulated by scammers, who lie about themselves, pretending to be somebody they are not. These individuals gain the trust of vulnerable people who can easily fall in love or lose finances. This can lead to heartbreak or debt.



Photo from Bing.com/images, 2024

The term hacker can have different meanings depending on the context in which it is used. Hacker refers to someone using their computer skills to gain unauthorised access to computer systems or networks. There are many different types of hackers. These include, criminal, financial gain. Meaning the theft of credit card numbers or defrauding banking systems. According to Malwarebytes hackers take over 1.1 million accounts by trying reused passwords. (Malwarebytes.com, 2024) Hackers can steal sensitive information such as customer data or financial records which can lead to financial losses, legal liabilities and damage to the company's reputation.

Digital safety is a very important part of the internet. The public need to be safe where possible. Digital safety must be always used, for example; be careful of public Wi-Fi which is an easy source for hackers to gain your personal information. We must also be cautious when it comes to email attachments as they can contain fake websites. The internet is used for many reasons that most individuals in society rely on i.e. banking, employment, shopping and general information. These things make results in the use of important, personal information such as, full name, Date of birth, address and bank details. These few factors are enough for hackers, scammers and viruses to take the information and impersonate an individual.

What is a virus?

An ill-natured software application that can attach itself to other programmes, self-replicate and spread itself onto other devices. Common computer viruses include;

- Web scripting virus – older, unsupported browsers have vulnerabilities allowing attackers to run code on the local device.
- Resident virus – a virus that can access computer memory and sit dormant until a payload is delivered. This malware may stay dormant until a specific time or when a user performs a new action.

Things to remember during digital safety;

- Back up all your data. If your data is archived, you can always wipe an infected system and restore from backup.
- Creating strong passwords and implement some form of multifactor authentication.
- Keep your antivirus software up to date
- Think before you click
- Be careful with email attachments
- Avoid dodgy websites
- Never give banking or personal details to anyone you don't know or trust
- Always log on to a website directly, rather than clicking on links through email.
- Don't be embarrassed about reporting a scam because the scammers are cunning and clever, there's no shame in being deceived. By reporting it you'll make it more difficult for them to deceive others.



Photo from Bing.com/images, 2024

References:

Hacker: Who are hackers? what is hacking? (2024)

Malwarebytes. Available at:

<https://www.malwarebytes.com/hacker>
(Accessed: 31 March 2024).

(No date) Advice about personal fraud |

metropolitan police. Available at:

<https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/> (Accessed: 31 March 2024).