Online Safety

Telford and Wrekin Safeguarding PARTNERSHIP

1. What is online safety?
Simply put, online safety refers to the act of staying safe online. Commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets.

2. Who can it affect?
Online safety is paramount in the world we live in, it can affect absolutely everyone from you personally to multinational companies. Ikea, Post Office and the NHS have all been affected . Lack of knowledge can make you especially vulnerable. There are ways which you can protect yourself by becoming aware of how you may be affected. 'STOP-THINK-FRAUD'

3. Why is online safety important?
There are different ways that you could be affected. Financial scams, fraudulent websites, online scams via Social media platforms such as Instagram, Text messages, phone calls, Courier fraud and even QR codes. Fraudsters use a range of ways to try and get your personal details for identify theft or financial gain. Companies can be targeted using Ransomware, enabling them to access data held by these companies. Phishing/smishing emails and texts target consumers pretending to be from a well-known source. Opening these confirm the number or email is live and make you vulnerable to further attacks. Quishing is when QR codes are stuck over legitimate ones for example parking charges.

4. What you can do.
•**DO**: Choose Strong Passwords. Password managers can help. Do not use identifiable information such as dates of birth, children's names etc. Don't use the same password. Three random words, make them complex add characters for letters for numbers.
•**DON'T** share your password.
•**DO**: Enable Two-Factor Authentication. Makes it more secure if using different devices.
•**DO**: Keep your devices and apps up-to-date, for up-to-date software and security
•**DON'T** stick with a Single Email Account. Create a separate email account for important things such as banking.
•**DON'T** store Personal Card Details on Websites.

5. Consequences.
Fraudsters can obtain personal details, bank account details, potential passwords for other sites, safeguarding information and most of all money. The amount of money lost to fraud in a single month during 2024 in our local area is £1.5 million, nationally this figure rises to £105 million. Scammers are very good at finding vulnerabilities particularly around love and belonging. Repeat victims often are aware they are being scammed they will continue contact and sending money, as they feel it's their only form of human contact.

6. What to do if concerned.
Happening now call 999.
Further information is available online to support you. The Little Guide to... preventing fraud and cyber crime | Metropolitan Police
You can request a check to see if your data has been part of a breach. Here. This will prompt you to change passwords on relevant sites.
Check if a financial firm is authorised Here.
The key message is **'If it looks too good to be true it probably is'**

7. Help available.
Action Fraud – report fraud and cybercrime. www.actionfraud.police.uk or call - 0300 123 2040
Phishing emails report to – report@phishing.gov.uk
Text (Smishing) fraud – text to 7726
Report a Fraudulent website – ncsc.gov.uk/report-scam-website
Financial conduct Authority - https://www.fca.org.uk/