BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

PROTECT YOURSELF ONLINE: OUR TOP TEN TIPS

If you're new to the internet, or already use it to take advantage of the huge variety of things it can do to make life easier, we'd like to help you to stay safe online.

Here are our top tips to help you to protect yourself, your money, your identity and your devices:

1. Choose, use and protect your **passwords** carefully, and use a different one for every online account in case one is hacked. Don't use a name or dictionary word. Use at least 8 digits, with a mix of upper & lower case letters and numbers, possibly an acronym of a meaningful phrase. Remember, your email, if compromised, could be used to reset all your other passwords – so ensure your email password is strong and unique.

2. Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode/fingerprint.

3. Ensure you always have **internet security software** loaded on computers and a similar app on your mobile devices, kept updated and switched on. Remember that smartphones and tablets can get compromised too. Download software and app updates as soon as possible, they may contain vital security upgrades to keep your device and data safe.

4. Don't assume **Wi-Fi hotspots** in places like cafes or hotels are secure - never use them to do anything confidential, like using your email or making a payment. Instead, use 3G, 4G or a VPN (virtual private network). Ensure your home Wi-Fi has a strong password security code.

5. Never reveal **too much personal or financial information** in emails, on social networking and dating sites, or in person. You never know who might see it, or use it. Identity theft is increasing. Always dispose of sensitive documents, bills, or addressed letters by shredding or confidential waste. Avoid posting that you are away from home on social media.

6. Take your time and **think twice**. Beware that online or on the phone, **people aren't always who they claim to be**. Fake emails and calls are common ways for fraudsters to approach their victims, so if you're unsure, research them online or call the company using the published number. Remember - if something seems too good to be true, it probably is.

7. **Don't click on links in emails**, posts, tweets or texts – and **don't open attachments** if the source isn't 100% known and trustworthy, or if it seems strange you'd be receiving them. Clicking on a bad link could upload malicious software, which could result in data loss, financial loss or even lock you out of your device. Never log onto your online banking or any other site via an email link – fake sites look like the real thing. Always go to your bank or other company's login page by typing their web address into your browser.

8. Never pay for anything by **direct bank transfer** – and never pay for anything via a money transfer service, such as Western Union – unless it's to someone you know personally who is reputable. Remember that credit cards offer greater protection than most other payment methods. Alternatively, use a secure payment site such as PayPal.

9. **Regularly back-up your data**, securely, to a portable hard drive or online. If your device is lost or compromised, you can then retrieve your essential or irreplaceable information.

10. For free expert advice about all aspects of staying safe online, **visit www.getsafeonline.org**.