

Welfare Awareness Topic: Staying Safe Online.

Overview – *The internet has made it easier than ever to communicate, create and share content and information. Though technologies offer us convenience and increased productivity, it is important to remember the security risks they carry.*

It is important to keeping your data and privacy secure, engaging in practices to prevent hacking and loss of cyber security, and preventing harmful interactions with other people or content to protect you or your organization. If you are currently working, your office will have its own rules on cyber security, but here are some best practice tips for everyone:

- **Be careful what you click on:** do not open emails or click on links from unknown individuals- banks and financial institutions will never ask you to verify your bank details by clicking on a link. Before you click, look for 'https://' and the padlock image to show that the site is secure, check for other indicators- links that say '.com.co' are likely to be unsafe. Beware of sponsored links at the top or side of a search page, as these are not always secure.
- **Privacy is everything-** keep your data safe, encrypt files, set up passcodes on your devices, and keep personal information hidden, with security set so that only friends can view your profiles on social media. Don't make comments or postings regarding your work, colleagues or other people that breach their rights, including their right to data privacy, and don't use work contact details when using external online social networking sites, unless approved by your work!
- **Do not connect to unsecured Wi-Fi-** public places that offer free Wi-Fi are useful, but if they are unsecured, they are open to being hacked, so secure your Wi-Fi by using the encryption option.
- **Install anti-virus/anti-spyware software and a firewall-** critical parts of your device's protection.
- **Remote Wipe-** these applications can be very important if a device is lost, stolen, or goes missing. On apple devices, you can erase your data through using Find My iPhone, and on windows and android, it is also possible to do this.
- **Keep software updated:** when software is not updated and bugs are left in the software, it becomes vulnerable, and the bug can be exploited by hackers.
- **Backup your data:** to avoid losing important information and data, securely back it up.
- **Use a secure payment option** (e.g., PayPal) for online purchases.
- **Be wary of fake news:** remember not all you see online is always fact.
- **Know where to find help:** understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone

Article/Source / Find out more

- Check out the [UK Safer Internet Centre](#) website, they have lots of [tips on internet safety](#), and have a [dedicated advice centre](#) for help and support.
- Childline have information about [online safety](#), setting up good [privacy settings](#), and lots of other resources and support pages. [The Proud Trust](#) also has tips and advice on staying safe online.
- The Government's National Cyber Security Centre has tips on [using social media safely](#), as well as [advice and guidance](#) on various topics like passwords, phishing, and more!

Support

If you would like to talk to the safeguarding team about anything you have just read, we will listen without judgement and signpost you to support. If you would like to talk to a member of the Safeguarding Team then please get in touch: safeguarding@bpp.com

