BIRMINGHAM LDG'S PREVENTING CYBER CRIME PLAN

Seasonal calendar of activity

Across all months there are always simple tips to promote:

- Have strong usernames and passwords, including different passwords for different accounts, passwords which are personal to you, passwords which are refreshed at least two or three times per year.
- Make sure you're computer and mobile phone are protected and secure – pay for and download antivirus/antimalware/antispyware from a trust source (signposting on CyberStreetwise, for instance); one administrator for your personal or business WiFi network; always have your firewall enabled.
- Always download the latest software updates, don't put it off. These are updates to prevent hackers using programmes on your computer to access your personal information. Always, always update your antivirus/antimalware software when prompted to.
- Use secure networks wherever you are inputting usernames, passwords, completing financial transactions. Be wary of public WiFi networks and who might be able to access your activity online.
- Be wary of "free" – free WiFi, free antivirus or antimalware software, free IT products (like Microsoft Office), free mobile phone apps (even from Google Store and particular for Android phones). These can often be set up cybercriminals to capture your personal information and data – do you know and trust the source?
- Simple stats – How many people affected? How many people with risky online behaviour? Etc.
- Latest scams – from National Trading Standards ECrime Team.

January	February	March	April	May	June	July	August	September	October	November	December
Check your privacy settings and how much information about you is openly accessible on the web. Check for financial records or references, old CV's, current address etc.	Safer Internet Day (10th). Get behind Safer Internet Day and "create a safer internet together" via http://www.saferinternet.org.uk	Review, refresh and strengthen your online passwords	Check your computer and mobile phone security, as well as banking and bill paying are secure – have you downloaded the latest software? What security software are you using? Do's and don'ts for public WiFi networks.	Phishing e-mails – do you know what to look like? Know what to do when you see one? Definitely don't forward to all!	Preparing to go on holiday? A few tips – don't broadcast on the web that you're going on holiday, especially when and where! Don't use public WiFi networks, at the airport etc. for any sensitive or secure activity. Consider refreshing your passwords.	Summertime scams – be aware of fake festival tickets, fake rugby world cup tickets, paying up front for products or services from people you don't know	Consider checking your credit report (one free report per year permitted from all credit rating agencies) to try and identify any unsanctioned activity	Review your social networks – who do you still know? Who don't you know? Who has access to potentially sensitive information about you?	National Cyber Security Month and Get Safe Online Week. Make sure you've got antivirus and anti-spyware on your computer and keep it up to date. Check the health of your computer.	Christmas shopping begins – if buying items online be aware of who you are giving your card and bank details to – do you know and trust the company. Be aware of the usernames and passwords set up for new accounts – avoid using the same ones you might already have.	Christmas scams – check your scam spotting skills and what to look for on e-mail, social media, advertising, free mobile phone apps etc.