Staying Safe In Cyberspace

Device Safety

- **New Device Set Up** - all new devices are shipped with factory set login and passwords. We have become good at securing our mobile phones and tablets, but many of us are relaxed with other connected devices, such as home network routers and wifi-enabled TVs or set top boxes. Take care to make these devices your own and to protect the information stored on them. Factory setting login and passwords are readily available online for anyone to access.

- **Software Updates** - it is essential to keep software on all devices, whether portable or desktop, up to date. If possible and appropriate, set updates to run automatically. By updating software for both operating systems and applications, you will not only have the latest features to enjoy but the latest security issues will have been addressed. If you find that you are having problems updating any software, you may need to perform a fresh install.

- **Unusual Behaviour** - if you find that your device is running slowly or your laptop/desktop fan is constantly on, get it checked out. This may be a sign of malware having been purposely installed.

- **Value The Contents** - it is always important to remember exactly what your devices are doing for you and the information that they hold. Personal information is the most valuable commodity of the modern age.

- **Backups** - the most overlooked responsibility that anyone who owns a device has is to keep regular backups of the information that it holds. These should be performed weekly at the very least.

Fraud & Identity Theft

- **Report** - as soon as you notice or have been made aware that ID theft or fraudulent activity has occurred on one of your accounts, report the activity to all the necessary organisations. Get cards and/or accounts frozen and order replacements, and notify the police on 101 in order to obtain a crime reference number should it be necessary.

- **Secure Compromised Online Access** - immediately after reporting fraud, change the passwords on any accounts linked with the incident.

- **Potential Ongoing Threat** - if information has been stolen from an online account of any kind, it may be necessary to inform other organisations that are responsible for issuing you with certain details. For example, if personal details such as passport number, driving licence details, National Insurance number, mobile phone number etc. have been compromised, then contact those authorities so that they are aware.

- **Online Banking** - use card readers for online banking as part of your multi-factor authentication. That way, you will need to have the reader, your card and knowledge of your password(s) and memorable data in order to access your accounts.

- **Use Credit Reporting Agencies** - there are a number of credit reporting agencies in the UK that offer identity fraud monitoring. Consider using one to highlight suspicious activity. Two of the leading agencies are:
  - Experian: experian.com
  - Equifax: equifax.co.uk

This leaflet has been designed and written by Veritas Justice CIC, a local stalking advocacy service, to provide basic digital safety information for all home users. Due to the nature of technology and the speed at which it changes, please seek further specific guidance from the following websites:

- **Sussex Police**: sussex.police.uk
  - Non-emergency calls: 101
  - Action Fraud: actionfraud.police.uk
    - Call: 0300 123 2040
  - Get Safe Online: getsafeonline.org
  - NCA Child Protection: ceop.police.uk
  - UK Safer Internet Centre: saferinternet.org.uk
  - Internet Watch Foundation: iwf.org.uk
  - NSPCC: nsppc.org.uk
  - ParentPort: parentport.org.uk
  - Vodafone Digital Parenting: vodafone.com/content/digital-parenting.html

- **Veritas justice sussex**
  - T: 01273 234773/07736 149940
  - E: info@veritas-justice.co.uk
  - W: veritas-justice.co.uk

- **Get Safe Online**
- **NCA Child Protection**
- **UK Safer Internet Centre**
- **Internet Watch Foundation**
- **NSPCC**
- **ParentPort**
- **Vodafone Digital Parenting**
Account Protection

- **Passwords** - the main defence between any would-be criminal and your personal data. Make sure that you use strong passwords of 8 or more characters, made up of a mix of upper & lower case letters, numbers and even symbols. Never use words that are found in dictionaries, unless you can disguise them. Use different passwords for different accounts and store them safely where only you can get to them, either in a suitable password vault app or on paper and in a locked safe at home.

- **Multi-factor Authentication** - wherever possible, try to enable multi-factor authentication, so that at least one extra level of security is required in order to access your personal or financial details. Ask the service provider if they offer this security option - many do now.

- **Account Activity Notifications** - many websites will now offer the service of notifying you whenever there is suspicious activity on your account, for instance if someone logs in from an unknown device or from a foreign country. You may have to seek out these settings on the website by actively managing your account.

- **Don’t Leave Screens Logged In** - always lock your computer or mobile device’s screen if you are in the middle of using a logged in session. It doesn’t matter what the account is, get into the habit. All information is valuable information.

- **Be Aware of Your Surroundings** - who is watching you? You take care at the cash point, so make sure that no one is watching over your shoulder while you log in to your accounts on your devices.

Safeguarding Children

- **Parental Controls** - anyone responsible for children that use connected devices are able to control the use of those devices by either the operating system or the relevant application settings. From restricting unsuitable content, blocking websites and setting time usage, to providing you with reports on your child’s activity, parental control software is both versatile and incredibly important. Children are vulnerable to online threats from individuals or groups of people, and cyberbullying can have lasting consequences.

- **Education** - it is very important to regularly discuss the importance of digital safety with any children in your care. They need to understand that any restrictions, while possibly upsetting for them, are in place for their own protection, and education will help them to understand.

- **Social Media & Sharing** - the majority of social media sites have an age restriction of 13, but this is impossible to police. Social media has exploded as a way of life for most of the developed world and is worth billions in revenue, so accounts need to be set up so that only the necessary details and images are shared with people that are trusted and known to the account holder. All sites have these security settings, but they do not educate users effectively.

- **Gaming** - online gaming has become a global phenomenon worth billions, with gamers connecting to each other via their consoles all over the world. It is important to ensure that children know who they are communicating with and that security settings are fully scrutinised.

Malware Attacks

- **Phishing & Vishing** - phishing (malicious emails) and vishing (malicious phone calls) are viral, and their instigators can make small fortunes for very little outlay in time or money. The key is to never click on a link or an attachment in an email unless you recognise the sender. If you are in the slightest bit suspicious, don’t risk it. Check with the purported sender to see if they really did send the email. Most larger businesses now have a dedicated email address to forward suspicious emails to for checking. This also helps them to trace and identify criminals. If you receive a suspicious phone call - and many are very convincing - then do your own checks. Get the name, politely end the call, and call the company back on a known genuine number to verify the call.

- **Anti-Malware Applications** - always use the latest antivirus software on your computers and devices, and ensure that they are set to automatically update the definitions daily.

- **Web Browser Settings** - many websites can contain malicious code with the specific intent to harvest personal and financial details. Some are even copies of genuine login pages, which intentionally crash once you have entered your login details. The attacker can go to the genuine site and login as you, leaving you to believe that the genuine site may be down. Make sure you go through the settings tabs on your web browser, and set the security and access settings according to you and your family’s needs. There are many different browsers to choose from - don’t just settle with what’s installed when you buy a device.

© 2019 Veritas Justice