Prepare Your Business

Cyber Safety Advice

Bedfordshire PREPARED

v1.0

Action to take?

These suggested actions are designed to help prevent you becoming a victim of Cyber enabled crime and create a better sense of Information security around your home/business.

No.	Action	Rationale/comment
1	Change the current password (PW) for all your email accounts. This will lock out anyone that has previously had access to your emails	If your PW is known to another, they may be able to access your account at work/home internally or externally; or emails from the web without you noticing. They can then monitor all you email traffic and be aware of contracts, payments, invoices, or other personal information. Set up rules to divert your emails so you do not get to see them and then communicate to others using your details and arrange mandate frauds/ID theft etc. NOTE: PW should be between 12-16 digits long, the longer the better. Using upper & lower case, numbers and special features (i.e. !".,:@). AND NEVER REPEATED.
2	Complete the same process for ALL other accounts. Bank account, websites, groups, memberships etc. Also complete this for social media, i.e. fb, twitter, instagram etc.	Again NEVER REPEAT A PW You may consider storing your PW in an encrypted password program tor such as keychain. You may also consider writing the PW down. If so, place in a book without highlighting it has PW it. Cover in a plan envelope and place in a very safe place (such as a Safe). This will cause you administrative delays but you will be able to show that your PW security is well protected.
3	Ensure you have active, up to date Antivirus (AV) that includes firewall, spyware and malware protection.	Check the licence is in date, check the account is active and be aware when the last scan was performed. Use AV on all end devices, such as Computers, laptop, smart phones, IPad (including apple devices) etc.
4	Ensure all security patches have been uploaded. I.e. from your operating system. Microsoft release new security updates most Tuesday evenings. Update all of your APP's on your phones and other devices	The software company has identified a security risk and provided a free upgrade to protect you. The hacker will be aware of these security gaps, and will be looking for devices that have not upgraded. Only use official APP stores such as Apple store or Google store.

No.	Action	Rationale/comment
5	Back up any data you would hate to lose, or that is personal data. Pay particular attention to the personal data of your customers, staff etc as due to GDPR you must be able to manage all personal data, secure it, and delete it if requested. [May 2018]	Several backups are advised. • 1x external at least 6 months old. • 1x recent. External to your server (i.e. not permanently connected) Depending on your company 1 day, 1 week 2 weeks or monthly – ask yourself what is required by your industry, what is desirable and practical. • Cloud storage may be relevant, but you are still responsible for the security of data and any loss. Consider security services and location of data centre. • Consider how much work would it take if you lost your system data and needed the backups. Check backups actually work.
	Turn off device/server when not in use, particularly overnight.	Keeping devices on overnight has an increased risk of attack. There are many computers around the world seeking idyll devices to attack.
	Change default settings of your routers.	The PW is not secure and is available on the dart web. • Go to hub manager; change the router name so it does not tell anyone your company/household name or name of the router • Change both PW and admin PW (remembering PW advice above) • Re-pair all devices to your router, i.e. printers, phones, TV. Check for unknown devices • Turn off the SSID
6	Remove date of birth and other personal details from your social media accounts.	To reduce hostile social engineering possibilities. Consider removing GPS metadata from photos or when you tell everyone you are not in or going away. Details about your work email account, job description, activities. Also consider close family and work colleagues (what are they saying about you and your company).

No.	Action	Rationale/comment
7	Physical security	Is your office locked when unattended? Can people gain entry to your office, server, etc. without your knowledge? Do for have sufficient doors, locks, alarms, or monitoring. Are cabinets for paper documents locked. How is your post handled, is it left in external post boxes, trays etc. for people to remove.
8	Report ALL thefts, frauds, cyber issues to Action Fraud.	This will allow the Police to be aware, warn others, take steps to identify the offenders and take action. If it is not reported it cannot be actioned. When GDPR becomes law in May 2018, you will only have 72 hours to report any breach or loss of data. You will need to show you took all reasonable steps to protect the personal data, otherwise you will face a very high fine and possibly criminal action as Directors, leads of a company.
9	You may consider it prudent for you and your staff to read a quick FREE e-book that may help	http://www.omic.pub/cybercrime
10	Contact cyberprotect@bedfordshire.pnn.police.uk	A point of contact (POC) If you have any incident or wish for additional help or advice.

More advice

See the Cyber essentials (CE) & ISO27001 and General Data Protection Regulation (GDPR) presentations on our website.