25 cyber security tips for your organisation

The cyber security landscape is constantly changing. Nevertheless, adopting some simple processes, procedures and technical precautions can help protect your organisation from most common threats. It is also important your staff are educated about cyber security awareness. Although not exhaustive, the following 25 tips will help ensure you are cyber secure.

1. **Introduce multi-factor authentication** – it's easy to do, strengthens security and is a step towards meeting compliance obligations.
2. **Out of date software is a weak link** in your cyber security – ensure updates and security patches are done regularly.
3. **Be confident in your back-up systems** – there's nothing worse than being hit by ransomware or a natural disaster only to discover much of your data cannot be recovered.
4. **Be sure you have a good Firewall** – it should monitor both incoming and outgoing data, requires proper setup for your business needs and ongoing management.
5. **Implement an Incident Response Strategy** – this will make it easy for your business to respond as fast as possible in the event of a cyber-attack and minimise damage caused.
6. **Ensure you have a password policy in place** – introduce security awareness training and test users' behaviours to check the message is getting home.
7. **Be sure your staff know the rules of safe surfing** – introduce web content filtering software that blocks access to unsafe websites.
8. **How secure are your communications?** – be sure to send confidential information using encrypted email, impose access controls and user privileges, make the most of advanced security features of multi-function printers.
9. **Conduct phishing drills** - check your teams' understanding following cyber security training.
10. **Be sure your IT network is cyber secure** – get a Cyber Security Assessment to establish the current state of your security readiness and recommend areas of improvement. Good cyber security provides a range of business benefits.
11. **Remember, there is no such thing as 100% security** – good backup provision and disaster recovery plans mean your business will pull through if the worst happens.
12. **Use a spam filter** - an advanced spam filter will allow you to improve productivity by blocking non-malicious spam emails and prevent phishing emails from being delivered to inboxes.
13. **Stop using Windows 7** – Microsoft no longer supports Windows 7. This means no upgrades, no bug fixes and no security patches, making you increasingly vulnerable to cyber-attack and out of GDPR compliance. You should move to Windows 10 now.
14. **Lock up physically and virtually** – don't leave your devices open when unattended, always lock them or have them setup to auto-lock when idle. Similarly, don't leave areas such as server rooms unlocked.

25 cyber security tips for your organisation

15. **Use a password manager** – creating and remembering many unique, complex passwords can prove a challenge. Instead, use a password manager.
16. **Be wary of external drives** – don't plug USB flash drives into your computer, they can easily spread malware from one computer to another.
17. **How secure are your printers?** – today's printers and copiers are hooked into your IT network and must be secured against cyber-attack.
18. **Avoid low-tech data breaches** – don't let business critical documents and confidential files sit unclaimed in printer trays across your business. Introduce user authentication to restrict what people can do with company printers.
19. **Never click links in emails from unknown senders** – always use caution and common sense when opening emails from unknown senders. Never open attachments or click on links. Instead, when in doubt, delete the email.
20. **Only work on trusted, secure networks** – it might be tempting to check your email using the local coffee shop's free, public WiFi but resist the temptation. Unsecured public WiFi is an open door for hackers.
21. **Cancel old user accounts –** when people leave your company, make sure their user accounts are disabled and all user privileges rescinded. Dormant accounts are perfect for hiding the malicious activity of hackers.
22. **Zero trust** - zero trust restricts access to the entire network by isolating applications and segmenting network access based on user permissions, authentication and user verification.
23. **Tools for the job** – introduce role-based access to your IT systems. This ensures people only have access to the systems and data required to do their job. Role-based access can help prevent accidental data breaches and malicious activity.
24. **Avoid using freeware** – everyone likes a freebie but relying on free anti-virus software can be a big mistake. It's often very limited in terms of functionality and usually unsupported.
25. **Get more than you bargained for –** using freeware and trialware is tempting but often comes with increased security risks from malware and bloatware that downloads in the background.

If you would like a Cyber Security Assessment or learn more about improving your current security arrangements then contact Modern Networks now.