31 Cybersecurity Tips
to Protect Your Business

NE**X**TWORKS™

Cybersecurity Tips to Protect Your Business

Tip 1: Train all staff members on cybersecurity routinely

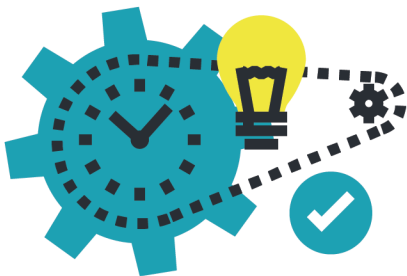**Tip 2:** Use strong passwords that are easy to remember and hard to guess

Tip 3: Properly dispose of electronic media

Tip 4: Use encryption to protect data and minimize breaches

Tip 5: Back up your data regularly

Tip 6: Test your data backups to ensure they're working as expected

Tip 7: Ensure you patch your operating systems and all applications

Tip 8: Use multi-factor authentication (MFA)

Tip 9: Ensure you have cyber insurance to respond to & recover from a data breach

Cybersecurity Tips to Protect Your Business

Tip 10: Remove unused apps to eliminate vulnerabilities

Tip 11: Use trusted anti-virus and anti-malware software

Tip 12: Be aware - don't overshare on social media

Tip 13: Have a mobile device action plan

Tip 14: Regularly audit systems to identify anomalies

Tip 15: Stay updated on current threats

Tip 16: Beware of malvertising

Tip 17: Document policies & procedures

Cybersecurity Tips
to Protect Your Business

Tip 18: Work with a trusted IT vendor

Tip 19: Keep your web browsers updated

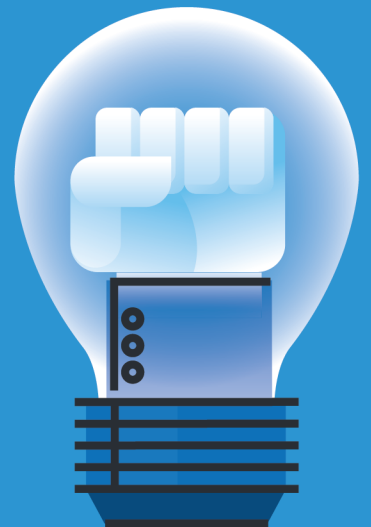**Tip 20: Avoid connecting to unsecured wi-fi networks**

Tip 21: Don't plug unknown devices into your computer

Tip 22: Confirm requests via multiple lines of communication

Tip 23: Be proactive in your compliance & cybersecurity

Tip 24: Monitor your credit & financial statements

Tip 25: Perform vulnerability scans & penetration tests

Cybersecurity Tips to Protect Your Business

Tip 26: Have a disaster recovery plan in place

Tip 27: Review access controls regularly

Tip 28: Perform a data audit

Tip 29: Always lock your devices

Tip 30: Think before you click

Tip 31: Delete old accounts that you no longer use

NEXTWORKS™

Have questions or looking for more cybersecurity tips?

Contact us!

360-558-7665
support@next-works.com
www.next-works.com