30 Ways to Increase Your Cybersecurity in 30 Days

stratti
IT BUSINESS SOLUTIONS

Do one each day for a month, and you'll be well on your way toward safer data security.

Day 1 Set up bank fraud alerts for withdrawals and transfers.	**Day 2** Enable Multi-Factor Authentication (MFA) on everything you can.	**Day 3** Install LastPass.	**Day 4** Change your passwords.	**Day 5** Enable and apply software updates on your computer, tablet, and smartphone.	**Day 6** Delete old apps off your computer and phone.	**Day 7** Schedule a recurring cybersecurity training session for your team.
Day 8 Change your browser settings to increase security.	**Day 9** Read a blog about cyber insurance.	**Day 10** Back up your computer and your server.	**Day 11** Back up your website.	**Day 12** Invest in (or use an existing) webcam cover for all computers and phones.	**Day 13** Install a privacy-first web browser.	**Day 14** Ensure physical backups of your server.
Day 15 Purge all "open source intelligence" you have online.	**Day 16** Enable recovery and backup features on your phone.	**Day 17** Encrypt your phone with a secure passcode.	**Day 18** Hide lock screen notifications.	**Day 19** Update the passwords on your copiers and printers.	**Day 20** Destroy the hard drives of any hardware you plan to recycle.	**Day 21** Create a separate guest wifi network.
Day 22 Review your network security.	**Day 23** Purchase similar website URLs.	**Day 24** Set up a VPN for all remote workers.	**Day 25** Turn your Bluetooth off when not in use.	**Day 26** Delete old accounts.	**Day 27** Introduce physical security protocols.	**Day 28** Set up a training session on social engineering.
Day 29 Turn on automated screenlock.	**Day 30** Develop a Backup and Recovery Response plan.					

With 30 years in the industry, Stratti is your expert IT wingman, your focused partner who's always on duty and has your back. If you're ready to stop worrying about your business security and leave it to the experts, contact Stratti today!

www.stratti.com | Toll Free Tel: (888) 455-3939 | Local Tel: (530) 342-8999 | wingman@stratti.com

30 Ways to Increase Your Cybersecurity in 30 Days

Below, we've made it easy to get started on protecting your data with easy-to-do tasks.

1. **Set up bank fraud alerts for withdrawals and transfers.** Doing so will ensure you're notified of hackers in real time.
2. **Enable Multi-Factor Authentication (MFA) on everything you can.** Extra login steps on your email, Amazon account, etc., mean hackers can't access your data, even when your password is compromised.
3. **Install LastPass.** A password manager removes the need (and danger) of reusing identical credentials across multiple accounts.
4. **Change your passwords.** Once you have LastPass set up, go through your accounts and change your password using LastPass-suggested, high-security passwords to increase your chances of locking out undetected threats.
5. **Enable and apply software updates on your computer, tablet, and smartphone.** When vendors publish new updates, hackers can reverse engineer them to discover vulnerabilities, which puts any un-updated systems at risk.
6. **Delete old apps off your computer and phone.** Unused applications typically have unpatched security vulnerabilities and should be deleted if not in use.
7. **Schedule a recurring cybersecurity training session for your team.** Educate yourself and your team about the latest phishing email techniques and implement spam filters to prevent them.
8. **Change your browser settings to increase security.** That little "remember password" prompt from Chrome or Safari? Say no thanks. Configure your browser to never save cookies or login credentials for business-critical systems. Use a service like LastPass instead.
9. **Read this blog about cyber insurance.** Does your business have cyber insurance? Unlike general liability insurance, cyber insurance is designed to protect a company from financial loss associated with cyber exposures, data breaches, and ransomware attacks.
10. **Back up your computer and your server.** Immunize yourself from hardware failure and ransomware attacks with regular (i.e. every day) computer backups.
11. **Back up your website.** Yep, websites need backup, too. Check in with your web host provider to ensure your website is fully backed up.
12. **Invest in (or use an existing) webcam cover for all computers and phones.** Hackers can access your camera even when the indicator lights are off or the cameras are not in use.
13. **Install a privacy-first web browser.** Swap Chrome, Safari, and Bing for a more secure browser like DuckDuckGo to keep information leaks to a minimum.
14. **Ensure physical backups of your server.** Ensure you have daily backups of your server. We recommend both physical and cloud backups. They should be encrypted and immutable, with the ability to go back 30 days or more for restoration.
15. **Purge all "open source intelligence" you have online.** Delete sensitive personal information from social media like your birthday, hometown, personal email, photos, etc. On social media accounts, set the security high to only allow friends to access your information. In the hands of the wrong person, these details can be used to impersonate you and access your accounts.
16. **Enable recovery and backup features on your phone.** That includes "find my iPhone" for iPhone users and "find my device" for Android. Use these services to locate your lost device or delete its data if it's been stolen. Enable backup on your phone and/or consider backing up to your computer.
17. **Encrypt your phone with a secure passcode.** Enable passcode protection on your iPhone or Android to encrypt your data by default. Take it one step further by setting up facial, iris, or thumbprint recognition. Always ensure your phone is set to auto-lock as well.
18. **Hide lock screen notification.** For an extra level of security, block all notifications from appearing on your phone lock screen. These notifications could help tip off a hacker and compromise your MFA.
19. **Updates the passwords on your copiers and printers.** Change the password from the manufactured default on your multifunction printers as well as any other device on your network. Use LastPass to generate a complicated password, then document it in LastPass for future use.
20. **Destroy the hard drives of any hardware you plan to recycle.** Old devices headed for decommissioning? At a minimum: all hard drives should be wiped and operating systems reset.
21. **Create a separate guest wifi network.** Keep your internal network, with access to sensitive company data, separate from the public network to help insulate your core business infrastructure.
22. **Review your network security.** Ask your IT team to do a review of your network security to ensure everything is properly configured. (Even better: a Managed IT Service provider like Stratti runs regular audits!)
23. **Purchase similar website URLs.** Spend a few minutes to purchase look-alike variations and misspellings of your main website domain to get ahead of scammers. Then host these domains and redirect them to your website.
24. **Set up a VPN for all remote workers.** Consider VPN use with an MFA login a requirement for your at-home employees; virtual private networks mask your IP address and make your networks much more difficult to attack.
25. **Turn your Bluetooth off when not in use.** Bluetooth devices can communicate with one another and let malicious actors send unsolicited spam and phishing messages to your device.
26. **Delete old accounts.** Make a list of unused email, shopping, apps, and other online accounts and delete them. It's possible you reused the same login credentials with multiple companies and services. This means a data breach at one company could compromise several other unrelated accounts.
27. **Introduce physical security protocols.** Evaluate where physical versions of sensitive data might be located (such as customer files, etc.) and limit access (such as a physical lock or passcode) to business-critical areas like your server room.
28. **Set up a training session on social engineering.** Educate your team about the latest manipulative social engineering techniques and how to spot them.
29. **Turn on automated screenlock.** To prevent unauthorized remote access, be sure your workstation has automated screenlock set up, typically after five minutes.
30. **Develop a Backup and Recovery Response plan.** Plan ahead for security worst-case scenarios like a ransomed, breached, or stolen device. Explore your options for legal aid, understand the full scope of your insurance, and rehearse how to restore your systems from backups so you can minimize downtime.