

Cybersecurity Awareness Month: A Tip a Day Helps Keep Threat Actors Away

October 2024

Tips brought to you by Optiv, the cyber advisory and solutions leader. Check out more resources, including our [Cybersecurity Dictionary](#) and [Security Awareness Training Deck](#), at [Optiv.com](#).

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1 Use multi-factor authentication when it's available	2 Secure web meetings with a password	3 Never use the same password twice	4 Secure your workspace and devices before stepping away for any length of time	5 Turn off file-sharing features before connecting to public Wi-Fi
6 Don't interact with text messages, calls or emails from unfamiliar sources	7 Turn off auto-connect for Wi-Fi and Bluetooth to avoid threat actors' networks	8 Don't leave mobile devices unattended	9 Delete unused software and apps to reduce your attack surface	10 If you suspect one of your accounts is compromised, change all your passwords	11 Keep track of your online accounts. Delete those that are no longer in use	12 Longer passwords are stronger passwords. 12 or more characters is best
13 Consider using a phrase to create a complex password. #PassPhrases > #Passwords	14 Do not use easily researched answers to security questions, such as a pet's name	15 Verify that the person calling you is who they say they are	16 Steer clear of websites that begin with "http" and stick with ones that start with "https"	17 Back up your data to prevent losing it	18 Review app permissions before installing them. Check how your data will be used	19 Limit the personal details you share online
20 Regularly scan your devices with anti-virus software	21 Do not connect unknown devices to your mobile device or computer	22 Research before downloading software or apps to determine its legacy	23 Think twice before clicking on advertisements	24 Keep your devices and software up to date. Turn on auto-update when available	25 Stay aware of new risks around smart tech like wearable and Wi-Fi-connected devices	26 Report any suspicious emails, texts or calls to protect colleagues from falling victim
27 Spoofed emails are phishing emails that appear to come from a known sender	28 Read emails carefully. Phishing emails may be alarming or sound too good to be true	29 Don't use public Wi-Fi to access sensitive information, pay bills or make purchases	30 If you need to use public Wi-Fi for work, use your employer's VPN to create a private network	31 Done browsing on public Wi-Fi? Log out of any services and "forget the network" in settings		

