

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

