AiSP | CYBER WELLNESS

HYGIENE TIPS

1. A strong password consists of 12 letters, upper and lower case, as well as special characters.
2. Always enable multi-factor authentication (MFA) to keep your accounts more secure.
3. Unless your device is offline and physically inaccessible by the rest of the world, there is no such thing as “secure enough”.
4. It is good practice to regularly backup your data on the cloud or a local storage device, at least once a month.
5. Always scan external devices for malware before accessing them.
6. You can reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.
7. Adopt a secure file sharing solution to encrypt your files while they’re in transit and at rest to prevent unauthorised access and keep your files safe.
8. Adware collects information about you to serve you more targeted ads. Use antiadware to clean adware and other unwanted programs from your computer.
9. Avoid visiting unknown websites or downloading software from untrusted sources.
10. Physical security is as important as Cyber security. Never leave your devices unattended.
11. Do not click on links given in an email. Manually type in the hyperlink yourself to prevent being redirected. A Click can contain hidden parameters you would not have typed in.
12. Lock your device every time you leave your desk.
13. It is important to keep track of your digital footprint, including social media.
14. Scan for viruses regularly, for example, once per week.
15. Did you know? The information you post on social media could be used to steal your identity or hack into your online accounts.
16. Check the privacy settings of your social media accounts and set them so that only people you know can view.

17. If you're unsure as to why you are being asked for your personal information, call the company to check.
18. If you are posting someone else's information online, seek their approval first.
19. Do not participate in facilitating harassment or violence towards someone through your social media posts.
20. Did you know? One of the top cybercrimes committed in Singapore are online scams.
21. Cybersecurity awareness starts from a young age. It is advisable to impart this knowledge to our youths.
22. Visit haveibeenpwned.com to find out if any of your accounts have been compromised.
23. Check out Cyber Security Agency of Singapore's "Go Safe Online" campaign to learn more about protecting yourself on the internet.
24. Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.
25. When you connect to a public network, you are vulnerable to risks such as manin-the middle attacks, data theft etc.
26. Avoid using public networks or use a VPN when you're connected to one.
27. Everyone is a potential target for hackers, including you. Do not have a "it will not happen to me" mindset.
28. Destroy/shred hard copy confidential documents that contain personal information.
29. Always consider the consequences when sharing things online.
30. Even the best software will fail if there is human error, do not put 100% trust in your software and expect to be immune.
31. Before posting anything, think if you would like it if someone did the same to you.
32. Top malicious email attachment types are .doc and .dot (37%) and .exe (19.5%)
33. ~300billion passphrases are used by humans and machines worldwide.
34. 45% of breaches featured hacking, 17% involved malware and 22% involved phishing.
35. The best defence to cybersecurity is to be aware.

36. Be continuously aware and do the right thing.
37. Always use encryption when storing or transmitting sensitive data.
38. Implement application control integrated with antivirus, to allow only authorised software to work.
39. Restrict administrator privileges so as not to give attackers privileged rights to compromise systems.
40. Ensure authorised access only, by implementing multifactor authentication.
41. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
42. Leverage full set of protection feature of your security solutions/technology.
43. No connection that is connected to the internet is unhackable.
44. IoT without security is equivalent to Internet of Threats.
45. Passwords are like undergarments, change it frequently and don't share it with others.
46. Did you know? 95% of cybersecurity breaches are caused by human error.
47. Enable security features on your devices to prevent unauthorised access.
48. If you suspect your account has been breached, change password immediately and inform the platform.
49. Sensitive browsing, such as banking or shopping, should be only done on your own device.
50. Create a unique password for each website and app and store them in a password manager.