10 ACTIONABLE METHODS TO IMPROVE YOUR SECURITY POSTURE

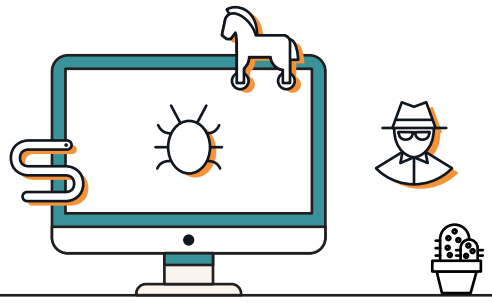
1

Don’t use counterfeit software. Reports estimate Thailand specifically has around 8/10 computers running some form of counterfeit software. This is problematic for 2 reasons, frequently the counterfeit disks and downloads used to install the software actually have malware on them; secondly the software will not update or perform appropriately leaving your computer vulnerable to cyberattacks particularly if it's a counterfeit anti-virus software solution.

2

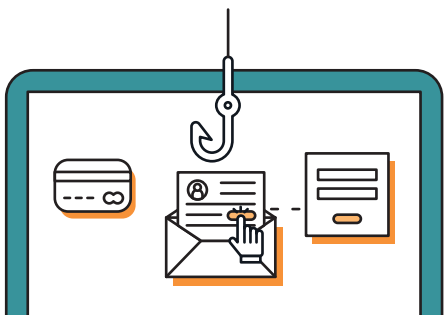
Be wary of the small print and terms and conditions on all downloaded applications. Many times “free” applications can sell on sensitive information about your usage or your personal data. They also can be liberal with your information, and it is not uncommon for it to fall into the wrong hands.

3



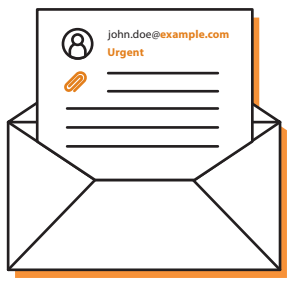
Stay up to date with the latest threats. Every virus is different and their impacts and infections methods are never the same. By following the latest in technology news you will be in a better position to defend yourself.

4



Be cautious with emails. Email is the most common method for infection and fraud. 2017 saw a significant rise in and BEC scams fueled by poor email security protocol– we expect the future to continue this trend.

5



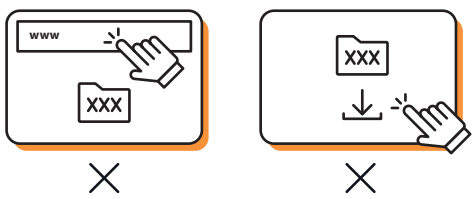
Vigilance with emails includes checking to see if an email is ‘spoofed’ – IE there is a spelling difference in the email or domain name. Be wary of branding rules and signatures from your common contact companies, red flags will be if these are wrong or inconsistent.

Don't open emails that don’t relate to you or your business nor open any files which you think are suspicious. When sending money, always follow up a two tiered process i.e. email and call confirms.

6

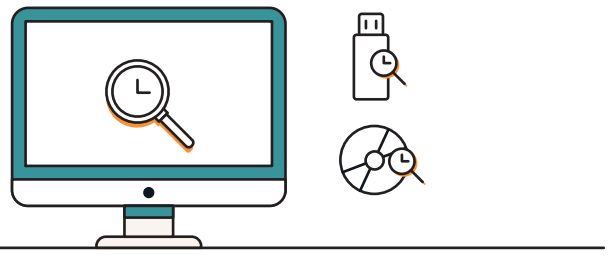
Poor password hygiene is another opportunity that is seized by hackers to access accounts. Passwords should be changed frequently, Aware suggest every 90 days at most. Also, never use the same password twice – if one account is compromised you don’t want all accounts to be vulnerable. In your passwords, use special characters, upper and lower cases whenever possible.

7



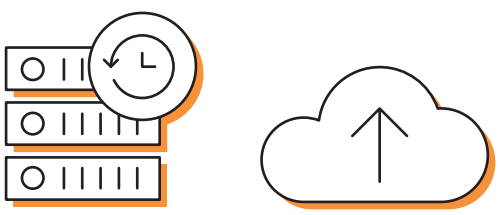
Drive by downloads from malicious or unprotected websites is another method of infection. Don’t browse or click links on suspicious websites, similarly don’t download from them.

8



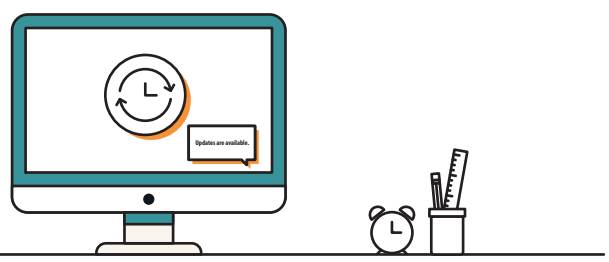
Be proactive with your device hygiene: this means not only having up-to-date software but also using it effectively. Scan your computer once a week, scan all other attached devices before you use them to reduce the risk.

9



Back-up all your data, this is your core security. Should the worst happen you will be able to restore most, if not all your data. This is the only sure way to protect against ransomware.

10



If you have official, licensed software – make sure you make the most of them with regular updates and patches. If this is a nuisance for you or your business, use a managed service provider to take care of it for you.

Aware

+66 5326 3350 info@aware.co.th www.aware.co.th