INAHSAK
MANAGEMENT CONSULTING / LEAN SIX SIGMA

Guide Sheet

Security Advisement: General Office Recommendations

	**Be smart when browsing, surfing or clicking links** Hackers are skilled at creating fake but professional looking websites, so be on the lookout for these signs that could signal it is a malicious site: • Check for presence of a complete address, phone number, and/or email contact • Check the web address for misspellings, extra words, characters or numbers that seem off or suspicious • Roll your mouse pointer over a link to reveal its true destination in the bottom corner of your browser • If there is NO padlock in the browser window, or no https:// at the beginning of the web address to signify that it is using a secure link, do not enter personal information on the site • Be wary of websites that request lots of personal information • Avoid 'pharming' by checking the address in your browser's address bar after you arrive to make sure it matches the address you typed • Be wary of websites and links in unsolicited emails from strangers
	**Do not click links or open attachments on emails from unknown senders** • Do not forward suspicious or spam emails • Delete the email, and delete from the Deleted box as well • Report the email style as suspicious to your IT manager, to identify patterns or decide to block addresses if needed
	**Phishing and Vishing attempts can occur via email, phone, sms, and social media** • Attempts to get you to give up information using psychological tactics are common, such as "password verification" emails, urgent requests, respond to verify user, or callers asking for who is in charge of finances, etc. • Notice subject line, often RE: or FW: as if already an email chain • Note generic salutations "Dear Friend"
	**Lock your phone and computer/desk when you are not using it** • To prevent unauthorized users from gaining access to your computer, phone, and the critical business data it holds • Place reminder notes on your desk, or set up an automatic lock after inactivity
	**Protect your passwords** • Use care when you enter your password in front of other people – in the office, and in public places such as airports or cafes • Do not write down your passwords where they can be easily found • Do not share your login or password
	**Create and Maintain Strong Passwords** • Simple passwords such as 12345 or abcde, and even your dog's name can be easily guessed or discovered • Combinations of numbers, letters, and symbols are effective passwords, but can be difficult to remember • Passphrases using multi-words are increasingly more difficult to crack and easier to remember because of the spaces or use a symbol such as @ for your space. For example, Fluffy@Clouds@Are@Soft could be more effective than a random string of characters, because most attacks (brute force attacks) are guessing strings randomly, not forming words • Require password changes every 60 or 90 days • Do not allow work passwords to be the same as personal ones

	**Change Passwords if Compromised** • If you suspect your accounts have been compromised, good practice is to change all passwords as soon as possible • Adversaries can remain in compromised systems for months to observe behaviours and often assume passwords are the same in other devices, so be sure to change all account passwords even in systems that you believe were not affected
	**Protect personal computers and devices with anti-virus/anti-malware software** • When working remotely, be sure to use installed anti-virus software, and be sure to keep it up to date • In the office, these updates should be regularly enforced and installed • Out of the office, require that adequate protective software is put on personal devices, as adversaries can learn about business behaviours through vulnerabilities on personal accounts as well, and could even create data or money ransomware situations personally that may impact business operations
	**Report suspicious behavior to your IT or CSIRT (Cyber Security Incident Response Team)** If your office does not have a dedicated IT or CSIRT team, design a process of notification to the individual who is responsible for technology systems and networks.
	**Get rid of junk** • Old files, photos, archived information take up space and slows down performance of devices. Slow performance could impair or slow down the anti-virus protections, and you may not notice irregular performance if you have too much clutter already slowing down the networks • Adversaries can target older files and software more easily without detection
	**Get rid of unused software** Check up on your software usage and activity. If it is not being used, uninstall and reduce the chance of an adversary taking advantage of vulnerabilities in older software packages that are not getting updated.
	**Do not install unauthorized software** • Create policies of acceptable software on business laptops and devices • Check for unauthorized software installations and uninstall promptly
	**Back up regularly and frequently** Store copies of your files on an external hard drive that is separate from your network systems, in case of a virus, loss, or hardware breakdown.
	**Review your social settings** Make sure your business and personal privacy settings are at your desired settings. Purge your contact list, as these are accessed by social media accounts, and be mindful of profiles that are inactive or contacts that are no longer relevant.