SILVIA IHENSEKHIEN *CISO, ShipServ*
https://www.linkedin.com/in/silvia-ihensekhien-099a4a27/
Website www.shipserv.com

Silvia is an accomplished Information Security and Project Management Professional with extensive international exposure. She has over 20 years of diverse leadership experience in technology, programme management and cyber security. She considers information security as one of the key business enablers for corporate success. Her expertise in cyber security includes governance, risk and compliance, platform and cloud security

TIP 1. PASSWORD HEALTH CHECK

Create long and unique passwords that contain a mix of uppercase and lowercase case letters, numbers and special characters. Avoid using personal information (e.g., pet's name, birthdates). Don't use the same password across multiple accounts. Change passwords regularly and don't reuse old passwords. Never reveal your password to anyone or write it down on paper. Consider using a password manager to keep track of your passwords.

TIP 2. MOBILE DEVICE SECURITY

Password-protect devices or enable biometric access (i.e., fingerprint or facial recognition). Install mobile security software. Keep systems and applications updated. Regularly backup data. Enable remote lock and data wipe capability on devices. Delete unused and outdated applications. Never leave devices unattended. Safely dispose of devices by doing a full factory reset. Turn off Bluetooth when it is not needed.

TIP 3. HOW TO SPOT A PHISHING EMAIL

Sender's name and email don't match. Contains suspicious attachments (e.g., zip files). Uses generic greetings instead of your name (e.g., 'Dear valued customer). Poorly written email (e.g., bad formatting, spelling and grammar mistakes).
Demands urgent action oftentimes with a strict deadline. Asks for personal details (e.g., password). Links look unusual or don't match intended URL destination. Uses scare tactics (e.g., account deactivation).

TIP 4. PROTECTION AGAINST RANSOM WARE

Use email filtering or scanning tools. Implement strict user access controls. Build staff awareness around cyber security best practices. Backup computing devices regularly. Patch systems and software. Perform regular security testing (i.e., penetration tests on systems and employee phishing tests). Enforce strong password and multi-factor authentication.

TIP 5. EMAIL SECURITY

Use hard-to-guess passwords or passphrases. Log out of system or activate password enabled screensaver whenever leaving your workstation. Keep business and personal emails separate. Scan all emails for viruses and malware. Enable spam filter. Install antivirus and antimalware solutions - and keep them up to date. Don't click on links or open attachments from unsolicited emails. Don't access emails from public networks.

TIP 6. VIDEO CONFERENCE SECURITY

Avoid reusing meeting IDs. Consider video conferencing software that offers end-to-end encryption. Password-protect meetings. Enable waiting room to verify attendees. Use virtual background or blurring features to block out anything confidential in your background. Limit screen sharing to only apps needed. Turn off cameras and microphones when not required during meetings. Verify that video conferencing link is from a known and trusted source.

TIP 7. BACKUP YOUR DATA

Ensure important and crucial files and data are backed up. Increase backup frequency and automate whenever possible. Consider cloud-based backups in case of a breach or stolen device. Encrypt backups while both in transit and at rest. Safeguard physical backup devices using a fire-proof safe. Regularly test backups to ensure they can be restored when needed.

TIP 8. REMOTE WORKING

Enable multi-factor authentication. Use power management or password-protected screensaver when temporarily moving away from your device. Don't use public Wi-Fi when checking emails or performing sensitive activities(i.e., banking). Use a secure connection using Virtual Private Network (VPN) when on public networks. Use your Smartphone and mobile internet or turn on mobile hotspot for laptop connection if unable to connect to a secure Wi-Fi.

TIP 9. CLOUD SECURITY

Choose reliable cloud vendors with security certifications. Enforce a strong password policy to prevent users from creating easily guessed passwords. Enable multi-factor authentication.

Implement stringent user access controls. Execute endpoint security solutions (i.e., antivirus, firewall, internet security tools). Encrypt data assets to prevent malicious actors from detecting vulnerabilities across the cloud infrastructure

TIP 10. BEWARE OF SOCIAL ENGINEERING

Never let anyone through an access-controlled door without showing proper ID. Avoid clicking on pop-up ads when surfing the web. Never plug USB flash drives found in public areas (i.e., parking lot, coffee shops) into your computer. Always keep antivirus and anti-malware software updated. Don't download attachments or click on any links from unknown sources.