www.ibs.com.cy

OCTOBER: THE CYBERSECURITY AWARENESS MONTH

By Olga Papadimitriou – Sales Administrator

The rush to enable a remote and hybrid workforce in 2022 may have provided some reprieve, but the rise in the usage of personal devices has also given security professionals more endpoints to monitor and secure. Despite all that technology is capable of, people remain the greatest asset. Security experts must train their staff members to safeguard their identities, keep their equipment and software up to date, and avoid falling victim to phishing scams.

Malware (22%) and phishing (20%) will continue to be the two main causes of cyberattacks in 2022. Humans continue to be the most dependable and low-cost attack vector for hackers globally, despite the rise of ransomware as a service (RaaS) and other advanced tools. We must all remain aware on how to defend ourselves against breaches at both work and at home.

4 TIPS TO BECOME CYBERSMART.

Phishing: Phishing attacks, including false emails, websites, and texts, accounted for 30% of attacks in 2021. In the previous year's Terranova Gone Phishing Tournament, 19.8% of players clicked on the phishing email link and 14.4% downloaded the fraudulent file. Following are some tips to avoid phishing attacks:

- Check the email address of the sender for reliable contact details. The sender address may be misspelled or irrelevant, which are common phishing red flags. Don't respond if you're unsure. Create a new email to reply to this one instead.
- Unless you have confirmed the sender, never open email attachments or click on links.

Software and Devices: Cybercriminals frequently exploit outdated, unpatched devices and software. Because of this, maintaining good online habits is crucial to avoiding malicious software that can steal users' personal information. To help keep your devices secure:

- Turn on the lock function for all your mobile devices.
- Turn on multifactor authentication (MFA) for all your private accounts and apps.
- Install system updates and run antivirus software right away.

Scams: Criminals may frequently contact you to "correct" a non-existed issue. A sense of urgency will be present in the email or text, such as *"Act now to prevent having your account closed!"* Do not click the link if you encounter this kind of warning. And always keep in mind to report any suspected fraud so the company may take the appropriate action. Following are some reminders:

- Be wary of false texts or calls from tech support requiring immediate action.
- Never respond to any instructions to download software from a third-party website.
- If in doubt, use another browser tab and go directly to the business's website.

Passwords: To prevent unwanted access to accounts, devices, and information, passwords are our first line of defence. Password fatigue is a constant risk since the average individual today has more than 150 online accounts. Here are some pointers on password security:

- To generate stronger passwords, use the password generator built into your browser.
- Be careful while accessing financial and personal information via a public Wi-Fi network.
- Consider becoming password-free or using a password manager.
- Cybercriminals are determined and relentless, working nonstop 24 hours a day. Therefore, we must always be cybersmart.

MICROSOFT SECURITY SOLUTIONS FOR SMALL OR MEDIUM-SIZED BUSINESS.

For a corporation, security is essential. Cyberattacks against businesses are becoming more frequent and sophisticated. Small firms are frequently at risk from ransomware, and they account for 50% to 75% of the victims. Ransomware attacks have increased by 300% over the past year. More than 60% of small enterprises that suffered a cyberattack were unable to operate. The danger is high for small and medium-sized clients that must deal with budgetary restraints and shortages in expert security skills due to the rapid adoption of technology and greater hybrid work.

Microsoft provides thorough, cost-effective, and simple to use security solutions that enable you to work safely from any location and are particularly created for companies with up to 300 employees:

Microsoft Defender for Business

- Up to 300 users
- Enterprise-grade protection across your devices and operating systems
- Threat and vulnerability management
- Next-generation antivirus protection

- Endpoint detection and response
- Automated investigation and response

Single app included: Microsoft Defender

Microsoft 365 Business Premium

Everything listed in Microsoft Defender for Business, plus:

- Defender for Office 365 to help protect email from phishing attacks
- Secure work data on personal devices, with Microsoft Intune
- Enable secure access to work apps with Azure AD Premium Plan 1
- Protect against lost or stolen passwords advanced multi-factor authentication
- Protect data with Azure Information Protection and data loss prevention
- Archiving, ediscovery and legal hold
- Best-in-class Office apps and powerful cloud services
- Collaborate via chat and online meetings using Microsoft Teams
- 1 TB of cloud storage per user on OneDrive

Apps and services included: Microsoft Outlook, Microsoft OneDrive, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft SharePoint, Microsoft Teams, Microsoft Exchange, Microsoft Publisher (PC only), Microsoft Access (PC only), Microsoft Intune, Microsoft Defender, Microsoft Azure Information Protection, Microsoft Azure AD Premium P1, Microsoft Azure Virtual Desktop.