RALPH CHAMMAH – *Chief Executive Officer, OwlGaze*
https://www.linkedin.com/in/ralphchammah/
https://www.owlgaze.com

Ralph's experience focuses on cyber innovation, analytics, and service development. After completing a prominent and successful career with Deloitte, both in Canada and Hong Kong, Ralph noticed an opportunity segment that was not being met in the current cyber security market and decided to fill that need: innovation in cyber security. Ralph helps organisations to strategically build the foundation of their business and lead them to the next stage of their growth with the latest best practices and software.

TIP 1. CYBER ATTACKS CAN HAPPEN TO ANYONE

Accept the fact that a cyber-attack can happen to anyone. Every individual and organisation can be a target of cyber criminals, regardless of scale, country, or financial capabilities. Cyber criminals are no longer limited to individual actors, but also highly sophisticated organisations that leverage advanced tools. Hence, it is important to stay vigilant and continuously improve cyber security. All of us are accountable and should take measures to protect ourselves.

TIP 2. KEEP DEVICES AND SOFTWARE UP-TO-DATE

Always keep your devices and software up-to-date. One of the easiest ways to minimise the risk of security breaches is continuous updating to the latest versions and patches. Updates often include the remediation on certain known vulnerabilities and bug fixes. It is always recommended to keep your personal and employee devices up-to-date, this includes Bring Your Own Devices, to prevent the vulnerabilities from being exploited.

TIP 3. SET UP MULTI-FACTOR AUTHENTICATION

Multi-factor authentication can prevent unauthorised access. It improves security by requiring the user to provide two or more authentication factors to prove their identity. Authentication factors are classified into three types: something you know (e.g. password), something you have (e.g. mobile phone, token) and something you are (e.g. fingerprint, voice). A combination of two or more factors heightens security.

TIP 4. RECONSIDER PASSWORD ROTATION CYCLE

Password expiration policies may do more harm than good. A common IT practice is to mandate password changes for users every 30 days or so; but new studies show that this might not be as effective for cyber security as it seems. The National Institute of Standards and Technology (NIST) recommends against this practice for personal accounts, as it prompts users to write down new passwords or use predictable and easy to remember passwords with sequential characters. Reduce segregated logins and enable single-sign-on to avoid your employees need to save numerous passwords for different applications.

TIP 5. LOCATE YOUR DATA AND SECURE IT

Know what data and systems you have and what business need they support. Classifying and centralising this information will allow implementing data security controls to protect your data where it is vulnerable. A comprehensive data mapping with details around backup frequency, criticality of the data and the impact to business operations, can lead to better compliance and privacy management as well as better incident response.

TIP 6. LIMIT DOWNLOAD AND INSTALLATION

Limit your download and installation. Downloads can include malware through which hackers gain access to your system. Any unnecessary software or browser extensions should be avoided. For organisation: download and installation rights of employees should be restricted until additional review and approval. If a download is necessary, do it from the legitimate source.

TIP 7. RANSOMWARE – TO PAY OR NOT TO PAY

Dealing with ransomware is not a security issue, it's a business continuity issue. With the global pandemic impacting all type of business to shift to remote work, security has an ever-widening scope of influence on your ability to do business. Dilemmas organisations must deal with are: to pay a ransom or not? Will cyber insurance provide adequate shelter? What's the role of government? Having an Incident Response (IR) plan will prepare you to address these questions.

TIP 8. USE SECURE WI-FI NETWORK

Be careful with public Wi-Fi networks. When you connect to a public network, you are sharing the network with everyone else who is connected. Any information you send or receive on the network may be exposed. Avoid managing personal information when using public Wi-Fi, always connect to a Virtual Private Network (VPN) for encrypted connections.

TIP 9. DO NOT FORGET PHYSICAL SECURITY

Do not leave your devices unattended and unlocked. Physical security is as important as logical security. If you need to leave your laptop, desktop or phone behind for any duration, lock the screen first so no one else can use it. Similarly, secure flash drives or external hard drives should be encrypted to avoid unauthorised access and data leakage, especially those with sensitive information.

TIP 10. MIND WHAT YOU SHARE ON THE INTERNET – SOCIAL ENGINEERING

Be aware of what you share online. Hackers can gather much information about you by observing your public profile on the internet (i.e.: LinkedIn, Facebook). Your Personally Identifiable Information (PII) or sensitive information exposed may lead to identity theft and financial loss. Hence, be careful when posting your boarding pass picture for your next business trip or sharing thoughts and interacting online, just like you would not share any personal information with a stranger.