YURI MILOSLAVSKY *CEO, SharePass*
LinkedIn: https://www.linkedin.com/in/yurimiloslavsky/
Website: https://sharepass.com/

Yuri Miloslavsky, an experienced IT professional based in Australia, brings over a decade of expertise in operational cybersecurity. As the CEO of SharePass, he oversees developing and implementing secure communication solutions. With a background in IT consulting and a passion for innovation, Yuri is dedicated to advancing cybersecurity measures to safeguard sensitive information in today's digital landscape.

TIP 1. BE CAUTIOUS WITH AGREEMENTS

When navigating websites and signing up for accounts, take the time to review the privacy policy. Understand how your data will be utilised and shared. Remember, once you provide information, it's no longer solely yours. Inquire about the necessity of certain data collection and consider opting out when appropriate. Avoid hastily agreeing to terms without fully assessing the implications. Ultimately, safeguarding your privacy is your responsibility.

TIP 2. VERIFY ALL FILES, EVEN FROM TRUSTED SOURCES

While antivirus software may be installed on your devices, it's essential to independently scan received files to ensure they're free of threats. Ideally, scans should be conducted on a non-production device or with a standard user account lacking elevated privileges. This extra precaution helps mitigate the risk of malware or malicious content slipping through undetected.

TIP 3. PRIORITISE MULTI-FACTOR AUTHENTICATION (MFA)

Utilise Multi-Factor Authentication (MFA) consistently. It provides an additional layer of security for your accounts, effectively thwarting hacking attempts. Even if a hacker gains access to your username and password, MFA acts as a safeguard, preventing unauthorised entry. Remember, it's preferable to pair MFA with a weaker password than to rely solely on a strong password without this added protection. Of course, strong passwords and MFA are the best way to go.

TIP 4: EMBRACE PHYSICAL SECURITY KEYS

Physical security keys bolster your MFA approach, fortifying account security with additional protection. Unlike conventional authentication methods like passwords or PINs, these keys resist phishing attacks and digital compromises. Integrating them enhances overall security and reduces the risk of unauthorised access to your accounts. As physical devices, security keys are the epitome of multi-factor authentication, providing unparalleled security.

TIP 5. QUESTION THE NEED FOR PERSONAL DETAILS

Whenever personal information is requested, inquire about the purpose behind it. After receiving a satisfactory explanation, provide only the necessary details. Refrain from offering additional information voluntarily, ensuring you disclose only what is explicitly required.

TIP 6. RESPOND PROMPTLY TO SUSPICIOUS ACTIVITY

Vigilance is key to safeguarding your online presence. If you encounter any unusual notifications, such as unauthorised

access attempts or warning messages from your accounts, investigate them promptly. Verify the authenticity of these messages and take appropriate action if needed. Promptly addressing suspicious activity helps prevent potential security breaches and ensures the integrity of your accounts and personal information.

TIP 7. VERIFY EMAIL SOURCES TO COMBAT PHISHING ATTACKS

One of the most effective strategies in the battle against phishing and email attacks is to verify the source of incoming emails. Always scrutinise the domain from which the email originated. Legitimate emails typically come from recognised domains associated with the sender's organisation. Be wary of emails originating from suspicious or unfamiliar domains, especially those associated with consumer email services. By verifying the source of emails, you can thwart phishing attempts and protect yourself from malicious cyber threats.

TIP 8. MINIMISE USE OF LOCAL ADMIN OR ELEVATED PRIVILEGE ACCOUNTS

Steer clear of employing local admin or elevated privilege accounts, even on personal devices, irrespective of your role as a system admin or authorised personnel. Refrain from dispensing privileged account access unless necessary. Diversify access levels among users to avert centralisation and mitigate the risk of a single point of failure. By adopting this approach, you bolster security and minimise potential vulnerabilities.

TIP 9. EXERCISE CAUTION ON SOCIAL MEDIA AND PUBLIC FORUMS

Be prudent when using social media and public forums; refrain from divulging excessive personal information. Your online presence resembles a puzzle, and sharing too many pieces enables interested parties to infer or deduce the rest. Once your online identity is compromised, it's challenging to regain control. Given our reliance on digital platforms, an identity breach can have far-reaching repercussions, impacting finances, career prospects, personal life, and more.

TIP 10. MANAGING YOUR DIGITAL FOOTPRINT

Please exercise caution when sharing confidential information like Personally Identifiable Information (PII), as it leaves a digital footprint. Remember that data you share may be stored on others' devices, posing potential risks. Fortunately, there are secure solutions available, such as password managers and encrypted communication software, offering precise control over data flow and management of digital footprints. Utilise these tools to safeguard your sensitive information effectively.