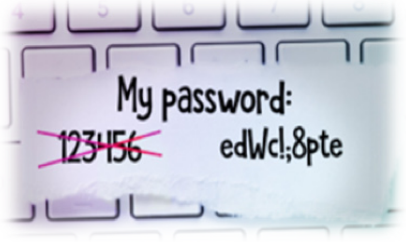
GEOFFREY RUTTO, *System Engineer, Kinetic IT - Technical consultant-Talkcoms Calling App*
LinkedIn/ https://www.linkedin.com/in/geoffrey-rutto/

Geoffrey Rutto is a dedicated, self-driven IT professional with over 10 years experience in safeguarding security and infrastructure across customer's environment in End User Computing services and systems support. He has demonstrated expertise in implementing cybersecurity projects, analytics and problem-solving techniques. He is an active member in the community creating awareness of cybersecurity risks and assisting small businesses take advantage of ICT tools to protect people and mitigate cyber threats.

TIP 1. USE STRONG PASSWORDS

Create simple unique and complex passwords, for every account created online and offline. If you have multiple accounts with different passwords, a password manager can help control them for you. Avoid-reusing passwords across different platforms e.g. Work email, Personal email, and loyalty cards account etc. With password manager, you only need to remember one master password.



TIP 2. USE SECURE PASSPHRASES

Choose passphrases consisting of random words for added security. Passphrases are the more secure version of passwords. Make them lengthy of at least 14 characters in total, unpredictable, and unique to every account created

TIP 3. KEEP YOUR DEVICES UPDATED

Ensure you enable automatic updates on your devices to have latest security patches and features. Use latest version where applicable such as windows, iOS and Android.

TIP 4. ACTIVATE MULTI-FACTOR AUTHENTICATION (MFA)

Strengthen your accounts by enabling MFA. It adds another layer of protection and requires more than one method of authentication to verify a user's identity for login. It is highly recommended that crucial services like user and email accounts, online banking, Online shopping, gaming and social media account to have two or more different types of actions to verify your identity.

TIP 5. BACKUP YOUR DATA REGULARLY

The most trusted way to have control of your data is to backup and you can recover at time of loss or damage. As the owner of the systems and data, protect your valuable files by regularly backing them up to an external device or cloud storage.

TIP 6. AVOID CLICKING SUSPICIOUS LINKS

Train employees to refrain from clicking links or attachments in unsolicited messages. Just visiting a site is enough to pass on malicious code. It is best to stick to sites you already know and official websites or contact trusted sources through verified channels.

TIP 7. STAY ALERT FOR SCAMS

Exercise extreme caution of suspicious emails, SMS, calls, or social media messages. Look out for signs of urgency, emotion, or requests for sensitive information and relevance to current events. Verify their legitimacy by contacting trusted sources directly.

TIP 8. MANAGE OWNERS, USERS, AND PERMISSION LEVELS INCLUDING PRIVACY SETTINGS

Review user access rights and privileges by managing the privacy and security settings on your devices, online services and applications. That way, you only ensure you are sharing required information for right purpose.

TIP 9. REPORT CYBERCRIME AND SCAMS

Share your knowledge to help others become more cyber aware by reporting incidents of scams to Scamwatch and cybercrime to ReportCyber or relevant authorities. That way you help protect yourself and others from online threats. Seek assistance when needed and don't hesitate to ask for help if you encounter suspicious activity or have concerns about your online security. Stay informed and vigilant in navigating the digital landscape safely.

TIP 10. DEPLOY AN ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION

Enhance your cybersecurity protection with EDR solutions. With the help of cyber professionals, you can advance beyond antivirus solutions. An EDR provides proactive threat detection, rapid response and comprehensive endpoint protection against wide range of cyber threats - giving you peace of mind to monitor and respond to potential threats on endpoints such as computers, servers, mobile devices within a network