DR NICKSON M. KARIE - *Cybersecurity Research Fellow, Cyber Security Cooperative Research Centre, Edith Cowan University, Perth, Australia.*
LinkedIn: https://au.linkedin.com/in/dr-nickson-m-karie-a247a620

Nickson M. Karie received his PhD degree in computer science from the University of Pre¬to-ria, South Africa, in 2016. Currently, Nickson is a Cybersecurity CRC Research Fellow at Edith Cowan University, Security Research Insti¬tute, Perth, Western Australia. He has more than 10 years experience in academic research, teaching, and consultancy in different countries including India, Kenya, South Africa, Swazi¬land, and Australia. His research interests include intrusion detection and prevention, information and computer security architecture, network security and foren-sics, mobile forensics, and IoT security. He is also actively engaged as a high impact interna¬tional conference and journal author and reviewer.

TIP 1. ALWAYS PROTECT SMARTPHONES AND OTHER MOBILE DEVICES

With the emergence of 'Internet of Things' (IoT) technologies, any device can connect to another. This has made individual and business smartphones and devices a potential target by hackers using over a million known types of mobile malware. Businesses and individuals can protect their devices by patching them, using difficult passcodes, and by only installing applications from trusted sources.

TIP 2. ALWAYS REMEMBER YOU ARE A TARGET TO HACKERS

Small businesses, as well as individuals, should not make a fool of themselves thinking "It will never happen to me". As long as you own a digital device, either at home or at work, that can connect to another digital device, you are at risk - and the chances that you can be hacked are always high. Businesses and individuals can keep safe by never exposing personal and financial information to anyone.

TIP 3. NEVER USE PUBLIC WI-FI FOR OFFICIAL WORK

Unless you are using a strong and trusted Virtual Private Network (VPN), never use public Wi-Fi services if security is a priority to you, especially Wi-Fi offered free of charge. Using a VPN will ensure that the traffic between your device and the VPN server is always encrypted; thus making it hard for criminals to access any individual or business data on your device.

TIP 4. ALWAYS THINK BEFORE YOU ACT OR CLICK ONLINE

Even though businesses and individuals have the freedom to do whatever they want online, it does not mean one should ever be reckless. With malware and sophisticated phishing techniques becoming the norm, businesses and individuals must safeguard their online accounts and all information on them. Always use unique and strong passwords. Never reuse passwords at any time. Never click or respond to requests you are not fully aware of; especially through emails, text messages, phone calls, and web pages.

TIP 5. ENSURE GOOD PATCH MANAGEMENT

Patches are not optional when it comes to correcting errors, vulnerabilities or bugs in an existing business or individual software. Businesses can stay safe by ensuring that all operating systems, applications, and embedded systems in use are up to date. A good patch management process ensures that all business and individual IT assets are not susceptible to exploitation. Patching is also good for supporting business system uptime and compliance.

TIP 6. GOOD PASSWORD MANAGEMENT IS NOT OPTIONAL

Always store and manage passwords efficiently as it's a good way to prevent unauthorised access to existing IT assets. With the many passwords that a business or individual can have, it can be tempting to take shortcuts or reuse the same passwords for different accounts. Consider a password manager to help in maintaining strong and unique passwords for all existing accounts.

TIP 7. CONSIDER USING TWO OR MULTI-FACTOR AUTHENTICATION

Businesses, and individuals, can enhance their security by using two or multi-factor authentication as this adds a security layer on top of the existing traditional username and password before being granted access to a website or application. With multi-factor authentication, it is very hard for hackers to be granted access to data by just stealing one of the authentication factors and also very hard for hackers to steal a complete set of credentials necessary to facilitate successful logins.

TIP 8. NO SOFTWARE IS IMMUNE

It is a known fact that "No connected machine is totally immune". This principle applies to software as well. Businesses and individuals should know that "No software is totally immune". With the advancements in technology, even trusted software in the market, is becoming a target for viruses. Always have an extra layer of security to protect business and individual data against cyber attacks.

TIP 9. USE A VIRTUAL PRIVATE NETWORK (VPN) WHEN WORKING FROM HOME

A growing number of employees are currently working from home as a result of the COVID-19 pandemic. Cybercriminals have, in recent times, targeted employees working from home to steal business or individual data. It is therefore important that employees working from home use VPN to connect to workplace networks, as well as secure their web browsing and remote network access.

TIP 10. ALWAYS AND FOREVER BACK UP YOUR DATA

Storage technology is becoming cheaper, making it easy for anyone to back up their data every day. Both physical onsite, as well as cloud or remote storage facilities, are now available to anyone. In the case of ransomware or malware attacks, data backups can help business organisations recover very quickly by restoring their systems with a recently performed backup; thus ensuring zero impact on performance.

"The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme."

FEROZE SODHI - *CEO at Z Plus Cyber Security*
www.zplus.net.au
Email: info@zplus.net.au
Cyber Security Trainer and Consultant

TIP 1. MUST CHANGE DEFAULT CREDENTIALS

Must change ALL the Default Credentials of your IoT devices. Especially of your Router Login Credentials. I'm not only talking about Wi-Fi username and password. But, the one you generally use to logon to the modem's home page at https://192.168.0.1 (this IP may vary from provider to provider, refer to your router booklet).

TIP 2. TURN OFF YOUR IOT DEVICES INCLUDING ROUTER ONCE IN EVERY 24 HOURS

TURN OFF your IoT devices, including router, for at least 1 minute in every 24 hours (if possible). It will disconnect all temporary connections, if any. This is because some malwares reside in your device's RAM only.

TIP 3. CHANGE YOUR PASSWORDS ONCE IN 3 MONTHS (EVEN MONTHLY, IF POSSIBLE)

Must change your all passwords once in every 3 months (even monthly, if possible). In this way, hackers will not be able to login to your accounts using stolen passwords.

TIP 4. CONVERT YOUR PASSWORDS WITH MEANINGLESS PASSPHRASES

Change your passwords with a meaningless passphrase; plus combinations of upper, lower, numeric and special symbols. In this way attacker/hackers will not be able to guess it from your publicly available information.
e.g.: UncleRailwayHorse12!@

TIP 5. REGULAR OFFLINE AND OFFSITE DATA BACKUP

Make sure you are taking regular data backups; and you also have backup copies offline and off site. This practice will help you to recover from incidents like a cyber attack or natural disaster.

TIP 6. MULTIFACTOR AUTHENTICATION (MFA)

Must enable Multi Factor Authentication (MFA) on your all accounts (wherever possible). You can use OTP on your mobile device or Google Authenticator or Microsoft Authenticator etc. It will protect your account from hackers as you need a combination of more than one key to access your accounts.

TIP 7. UPDATE SOFTWARE / OPERATING SYSTEMS

Make sure your all software and Operating Systems are up to date and all patches are installed.
BE AWARE OF FAKE UPDATES. VISIT VENDOR'S WEBSITE AND COMPARE YOUR SOFTWARE VERSIONS. HACKERS ARE SENDING PUSH NOTIFICATION IN YOUR SOFTWARE TO INSTALL MALWARE THROUGH FAKE SOFTWARE UPDATES.

TIP 8. STAFF TRAINING

Humans are the weakest factor in your Cyber Security Chain. You, and your all staff members, must be fully trained and aware to deal with cyber incidents.

TIP 9. DO NOT INSTALL FREE APPLICATIONS / SOFTWARE / PIRATED SOFTWARE

Do NOT install free applications/software unless they are from reliable and authentic sources. For example:- application from your bank or government are fine. But think twice before installing any third-party free applications, because you

don't know who the developers are and what sort of code they have embedded behind the scenes.
Pirated software are another cyber security threat. You will not get security updates/patches for pirated software. Therefore, vulnerabilities (if any) will remain there for hackers.

TIP 10. REMOVE UNWANTED SOFTWARE AND USER ACCOUNTS

Remove all unwanted software and user accounts from your systems immediately.
Security patches are not available for obsolete software (most of the time).
Unwanted/ex-staff user accounts are risks to organisations. Someone may login and can cause damage using these types of accounts.

DR JENINE BEEKHUYZEN OAM - *Founder & CEO Tech Girls Movement Foundation & Adroit Research Pty Ltd*
LinkedIn/Website https://www.linkedin.com/in/jeninebeek
www.techgirlsmovement.org www.adroitresearch.com.au

Dr Jenine Beekhuyzen OAM is a futurist who believes existing structures in the technology industry must change in order to serve tomorrow's digital landscape, and that our children's future job prospects depend on it. Her focus is on leadership, innovation, education to champion Australian tech entrepreneurship, and address the necessary rebalancing of gender roles within the traditionally male-dominated STEM (Science, Technology, Engineering and Mathematics) space.

TIP 1. USE CREATIVE PASSPHRASES

Passwords are to protect you and so it should be something that is not easy for someone to access. When creating passwords online, create passphrases that are meaningful to you - using a combination of: capital letters, lowercase, numbers and symbols.

TIP 2. BE PASSIONATE

Love what you do; it gives you a sense of purpose. Learn everything you can about your passion. Your passion will always shine through to your customers, so they know that they are your number one concern.

TIP 3. PLAN AHEAD

Consider what you and your company's digital footprint might be 10 years from now. Consider what impact your footprint will play in your business and career. Consider your brand and reputation for years to come.

TIP 4. LEARN CODING

Take some time to learn coding, and that will put you in great stead to understand the cyber world. It is useful in finding bugs and how to hack a code.

TIP 5. DIGITAL FOOTPRINT

Make sure you always consider the consequences for what you, and your company, does online. Absolutely everything you do online is tracked, from sending a message, watching a video, to posting a picture, it makes up who you are as a person online. You will always leave a digital footprint, so: always think: "Is this what I want to be known about me/us?"

TIP 6. INSIST ON PROCEDURES

Policies and procedures are an essential part of any organisation. Have detailed policies and procedures in place; and ensure that your staff are compliant with all of your cyber security requirements.

TIP 7. THINK LIKE A HACKER

Cyber Attacks are a sad reality therefore sometimes it is worth thinking like a hacker. It is absolutely possible to learn how to think like a hacker. Try to break your own systems to identify weaknesses and protect your interests.

TIP 8. DON'T BE AFRAID

As a woman in the industry, don't be afraid to stand up and be counted. Diversity within the field ensures that we all have a voice - and a position at the table. Have courage and be kind; it will pay off.

TIP 9. CONSIDER THE FUTURE

Consider what future professional roles you may have in your career. Is it to be a CEO or President? Think about your social media footprint now, and consider what it will look like in the future.

TIP 10. UPDATE PASSWORDS

Be proactive. Update your passwords regularly, check for malware and viruses, check the settings on your social media and regularly review what you have agreed to. It is difficult to know if someone else is using your login details, which is why it is important to change your passwords often.

NAGESWAREE KODAI RAMSOONDER, *Cyber Security Presenter, Help Desk*

MY Business Incubator™ Western Australia.

LinkedIn: https://www.linkedin.com/in/nageswaree-kodai-ramsoonder-09b44b1b1/

Nageswaree has a master's degree in Cyber Security. She has been an author and presenter for international Conference on Computational Science and Computational Intelligence (CSCI'2020). She has been involved in the CyberCheckMe project at ECU as Content Developer. She is currently MY Business Incubator™ Cyber Security Presenter and Cyber Help Desk / Mentor and is passionate about boosting cyber security awareness.

TIP 1. CREATE UNIQUE PASSWORDS AND PASSPHRASES

A culture of poor password hygiene has been one of the major causes for data breaches as cybercriminals can easily crack weak passwords and gain unauthorised access. Unique, longer passwords and passphrases are recommended to lessen the various risks. Avoid using the same login credentials for different accounts.

TIP 2. USE ANTI-VIRUS SOFTWARE

An anti-virus software is crucial for detection and removal of malware, viruses and adware from your devices. Free online anti-virus software is not reliable, so ensure you buy only from a reputed and trusted software vendor. An IT services provider can install the anti-virus software on your computer devices at work to protect you and your employees. Make sure that your anti-virus software is always updated as new malware are emerging every day.

TIP 3. KEEP YOUR DEVICES UPDATED

Regular software updating is highly recommended as it not only upgrades the existing features but adds new features to the devices. Software updates also patches vulnerabilities in a computer system; thus, automatic updates should be enabled to prevent hackers from gaining access to your devices.

TIP 4. USE TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION

Two-factor or multi-factor authentication should be turned on for both personal and work emails. Along with your password, you can opt to have a code generated and sent to you on your mobile device to verify your identity before allowing you to log in. It provides an extra layer of protection to all your accounts as it requires two or more different forms of identifications to grant you permission to log in.

TIP 5. BACKUP YOUR DATA ONLINE, OFFLINE AND OFF-SITE

Always conduct regular online, offline, and off-site backups, so that data can be restored in case of a ransomware attack, computer crash, natural calamities like fires and floods, or due to accidental property damage. It becomes vital to have an off-site physical backup which is more secure and helps to ensure minimum disruption of business continuity.

TIP 6. ALWAYS HOVER OVER LINKS AND ATTACHMENTS PRIOR TO CLICKING

Email scam/phishing has become the most common threat to businesses causing financial loss and damage to reputations. Ensure to always hover over the links and attachments before clicking to check where the URL are redirecting to, and to ensure that they are genuine links.

TIP 7. DO NOT USE UNKNOWN USB/FLASH DRIVES OR EXTERNAL HARD DRIVES ON YOUR DEVICES

Unknown or random removable media, USB/flash drives or external hard drives should not be used as they can infect your devices and even servers with malicious content and viruses. Cybercriminals can then steal, modify, and/or delete any information from your computer network, causing loss and leakage of data.

TIP 8. DO NOT LEAVE DEVICES UNATTENDED

Do not leave your devices unattended in plain sight and always log off or lock your computer with a password-protected screen saver before moving away from your computer. It can cause loss of privacy as intruders might read, change and/or erase sensitive and confidential information - putting the employer and the business at stake.

TIP 9. BE WARY OF WHAT INFORMATION YOU SHARE ON SOCIAL MEDIA

Be cautious about how much information you share about yourself on social media accounts and check your privacy control setting to verify which information can be made public or kept private. Avoid sharing critical personal information like your home address, date of birth or/and your daily routine schedule on Facebook, Instagram and/or Twitter as a cybercriminal can use your personal details and steal your identity.

TIP 10. AVOID MAKING FINANCIAL TRANSACTIONS USING PUBLIC WI-FI

Public Wi-Fi connection is not secure and using it for any transaction enables cybercriminals to intercept the data sent and received from your device. Cybercriminals can position themselves between you and the end point and install malware in your laptop/mobile device and can easily retrieve and access your banking details, accounts passwords and other sensitive information. Use your mobile phone's network instead and do not connect to any public Wi-Fi connection.

NIKOLAY SHMAKOV *Managing Director, Res-Q IT*
Website res-q.com.au

Res-Q IT is a consultancy company located in Perth, Australia. Through our expert IT services delivered by a team of certified engineers, we help businesses by providing solutions for their every-day IT operations and Computer Support. Our services include set up and support of business phone systems, IT consultancy and support, web hosting and cloud-based solutions, and all things internet. When it comes to setting up systems for a business, whether it's an existing one or a startup, you can count on Res-Q IT Services. We take care of everything you need so that you never see

TIP 1. KEEP YOUR COMPUTERS UP TO DATE

If your computers are not up to date, then hackers can use that vulnerability to take control of your computers. Regularly updating your computers is a vital part in staying safe online.

TIP 2. INSTALL ANTIVIRUS

Your antivirus protection is only as good as its ability to detect any infected files in real-time scanning. It is important to understand that not every Antivirus software is good at detecting viruses. You must constantly stay alert and educate yourself and your staff about online safety.

TIP 3. MAKE SURE YOU LOCK YOUR COMPUTER WHEN IT IS NOT IN USE

If your computer is compromised, then hackers can access your files. If the computer is locked it creates an extra layer of difficulty for someone to access your favorite websites and potentially gain access to sensitive login information.

TIP 4. DO NOT ENGAGE IN ANSWERING PERSONAL QUESTIONS ON FACEBOOK

Social engineering is the psychological manipulation of people into performing actions, or divulging confidential information, as that can enable hackers to deduce the answers to your secret questions.

TIP 5. ENABLE MULTIFACTOR AUTHENTICATION FOR YOUR EMAIL ACCOUNTS

It is very important to add extra layers of protection to block access to your email accounts, particularly if the accounts are to be accessed by somebody else.

TIP 6. NEVER SHARE YOUR PASSWORDS WITH ANYONE

Nothing more to add to this tip really. You can have a secret place, such as a glass container buried in your garden with the master password to your password manager. All jokes aside: the only persons allowed to know about the place where you buried it is your very close family member, or your accountant.

TIP 7. GENERATE A NEW PASSWORD FOR EVERY SITE

It is tempting to use your favorite password for every site you use. However, if the resource gets hacked it then exposes the password combination (email + password) for access to other websites.

TIP 8. USE A PASSWORD MANAGER WHERE POSSIBLE

There are plenty of password managers out there. My favorite is LastPass. The master password can be securely locked in the container and buried in your garden

TIP 9. DOCUMENT HOW YOU RESTORE YOUR BUSINESS IF YOUR WEBSITE, COMPUTERS, OR OTHER IMPORTANT RESOURCE GOES DOWN

It is called the Disaster Recovery Plan. Detail what you need to do to get your computer, website, online shop or business documents back online - and how much time it will take. Write down the contacts and responsible people, as well as access details, for all these resources

TIP 10. BACKUP, BACKUP, BACKUP

You must have backups for all your documents. Regardless of how good you are, there is always a human factor in every cyber-attack. It is essential that your company's highly valuable classified data and assets are protected from its greatest threat: the enemy within the gates and outside.

PAUL HASKELL-DOWLAND *Associate Dean, Edith Cowan University*
LinkedIn: www.linkedin.com/in/pdowland/
Website: paul.haskell-dowland.com

Paul has appeared on local, national and international media commenting on current cyber issues with a global audience reach of more than one billion people. Paul has more than 20 years of experience in cyber security research and education in both the UK and Australia.

TIP 1. UPDATES, UPDATES, EVERYWHERE

We all know we should apply updates, so why do we not do it? Updates should be applied when available and checked regularly. Don't rely on automated patches - make sure they are being applied correctly and consistently.

TIP 2. PASSWORDS DON'T HAVE TO BE COMPLEX

Put simply: qwerty123 is bad; [4r4QnML9Hr>aHKM^WBj is better. But, while complex; lengthy, random passwords are more difficult to guess, they are impossible to remember (for the average human). Try combining a sequence of words as an alternative.

TIP 3. PASSWORDS SHOULD BE UNIQUE

Once you have a strong password, don't reuse it. Use a password manager to ensure that every password (particularly on websites) is unique. That way, if a password is compromised, it will only impact on that one site.

TIP 4. EDUCATION IS WORTH MORE THAN POLICY

You can establish policies and procedures for every conceivable eventuality… but encouraging cyber-safe behaviours in the workplace through training and education will pay dividends.

TIP 5. UTILISE MULTI-FACTOR AUTHENTICATION

Strong password selection is a good start, but you are still only a compromise away from being owned. Rather than depend exclusively on a single password, use multi-factor authentication where credentials are backed up by SMS, authenticator apps or tokens.

TIP 6. WHAT'S THE BACKUP FOR YOUR BACKUP?

Your organisation may have established backup procedures. But, have you tested them recently? Do you know how to restore your systems and data? Do you have backup copies stored off-site for resilience?

TIP 7. PUBLIC WI-FI CAN BE A BACKDOOR INTO YOUR SYSTEMS

While it may be very convenient to use free Wi-Fi outside of the office, is it secure? Most public Wi-Fi services are not inherently risky, but they are a public, shared facility. If you must use one, avoid accessing business systems or use a VPN to protect traffic from interception.

TIP 8. CHECK FOR SIGNS OF COMPROMISE

Monitor your accounts for misuse - especially bank accounts and credit cards. If you see anything suspicious, contact the provider. Regularly check email addresses and phone numbers on haveibeenpwned.com.

TIP 9. EVERY DEVICE IS A POTENTIAL THREAT

The plethora of devices in our daily lives opens complex avenues for compromise. Have clear rules on the use of network connected devices in the workplace. Don't forget automation technologies including air conditioning and lighting control systems.

TIP 10. DON'T FORGET FRIENDS AND FAMILY

Cyber security starts at home - if your employees demonstrate safe behaviours at home, they will bring them into the workplace. Encourage staff to explore cyber security concepts and to become champions for friends and family.

SAMUEL NG, *Director, Cybersecurity & Analytics, Hong Kong Applied Science and Technology Research Institute (ASTRI)*
LinkedIn/Website: www.linkedin.com/in/samuel-n-986751116

Passion fuelled cybersecurity professional with leadership trained by armed forces, Samuel has extensive experience in all cybersecurity domains from both technical and management perspectives. He brought value to organisations by balancing governance, controls, and business strategies ultimately upholding the CIA Triad (Confidentiality, Integrity, Availability) at highest standards. As a 14-years Malaysian army veteran with a Master's Degree and multiple infosec-recognised certifications, he progressed his career to Hong Kong, contributed to various sectors including: banking, telecommunication, cloud, IT infrastructures, start-ups etc. Currently exercising his expertise in Hong Kong Applied Science and Technology Research Institute, responsible for strategic planning and leading research directions of cybersecurity and data analytics.

TIP 1. BE IT BIG OR SMALL, YOU ARE ALWAYS A TARGET

The mindset of "I am too small to be attacked" is the fundamental reason why some businesses fell victim to cyber-attacks; leading to bigger losses which heavily impact the operations and revenue of a business. Threat actors continuously expand their "territory of compromise", either to obtain valuable information, piggybacking on victim's infrastructure or both. Risk-based approach would be helpful for understanding the exposure and mitigate accordingly balancing cost, effort and risks.

TIP 2. TOO GOOD TO BE TRUE? LOOK AGAIN

Having this sense will keep you away from trouble and save your organisation a hefty sum of cyber-attack incident, which cost millions of dollars annually. When you are not paying for a product, you are the product! Threat actors lure victims with a sense of urgency, greed and fear of losing in order to further their exploitation through phishing and other tactics.

TIP 3. GUILTY UNTIL PROVEN INNOCENT

Always check and validate the source when you encounter something. Be it an email, message, or a person's request. Only proceed when validation is obtained and report to the proper channel or authorities when something, or someone, sounds or acts suspiciously.

TIP 4. STRIKE A BALANCE FOR YOUR PASSWORDS AND CONVENIENCE

It's painful to have different passwords for all your online accounts. While it can keep you safe, having a balance for security and convenience is a long-term strategy for cyber resiliencies, both personal and organisational. To create a password: be creative, long and complicated, but make it personal and easy for yourself to remember so - when one of your accounts are compromised, you will be rest-assured that others are still safe.

TIP 5. MULTI-FACTOR AUTHENTICATION

Many platforms now offer the convenience of this additional protection layer. MFA requires minimal amounts of effort, but largely improves security by verifying it's you who are accessing the accounts, not someone unauthorised.

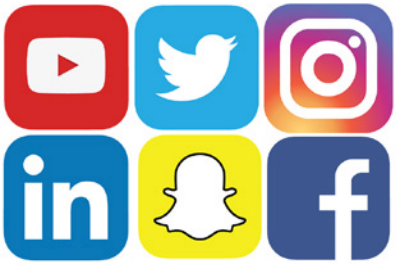
TIP 6. RADIO SILENT AFTER YOU ARE DONE

Mobile devices (with both your personal and company data) can be hacked wirelessly without the owner's interaction, practically even when your phone is in your pocket. Turn off all wireless features such as Wi-Fi, Bluetooth, AirDrop, etc when not in use

TIP 7. AVOID HAVING 'ALL EGGS IN ONE BASKET'

A proper risk assessment will identify the location, criticality and sensitivity of all your company data. A clear view of risks associated with multiple location of data is stored, combined with appropriate security controls based on the level of data criticality, will not only improve security, but keep you out from regulation and compliances issues as well

TIP 8. DON'T LIVE IN SOCIAL MEDIA



Without due care, sharing too much information on social media (such as: name, phone numbers, corporate email addresses and personal locations) can be used by threat actors not only in identifying theft, but information to fuel their bigger attacks such as: phishing, external and internal exploitations, password guessing with partially known information, etc…….

TIP 9. FOLLOW THE RULES – COMPLIANCE TO REGULATIONS

Adhering to local regulations and incorporating globally recognised cybersecurity standards not only helps your organisation to avoid fines and penalties; but also protects and improves your business reputation by building trust between your customers, partners, stakeholders and regulators

TIP 10. FUTURE PROOF YOUR CYBER DEFENCE, BECAUSE THREAT ACTORS DO TOO

Cyber-Defence with Artificial Intelligence and Machine Learning will be a powerful tool in the looming future. Threat alert fatigue and human errors are obvious pain points in cyber defences. Attackers are rapidly moving into Artificial Intelligence and emerging technologies (such as cloud computing) to enhance their offensive tactics, why shouldn't the defenders?

SIMON COHEN *Founder / Owner & CIO Cohesis Pty Ltd*
www.linkedin.com/in/simoncohen1/
www.cohesis.com.au

"Helping businesses implement IT strategies to drive growth, reduce Cyber risk and increase operational effectiveness."

TIP 1: CYBER AWARENESS TRAINING

Business leaders often 'forget' that employees are the first line of any organisation's Cyber defence. Cohesis recommends that ongoing Cyber Awareness training and testing is conducted.

TIP 2: FIX POOR USER BEHAVIOUR

Weak passwords, poor browsing habits and a "do it later" attitude to installing updates, all weaken an organisation's Cyber posture. Strong governance and effective communication are vital to fixing poor user behaviour which can otherwise lead to vulnerabilities in corporate networks.

TIP 3: BE PREPARED - ASSUME YOU WILL BE A VICTIM OF A CYBER ATTACK

The likelihood is that your organisation will suffer a Cyber Attack. Being prepared and having a plan helps you take control of the situation which will build trust with your staff, customers and stakeholders. Cohesis recommends organisations to develop a Cyber Incident Response Procedure.

TIP 4: SENIOR MANAGEMENT NEED TO COLLECTIVELY 'OWN' THE CYBER SECURITY AGENDA

It's important for leadership teams to collectively 'own' the Cyber Security agenda. Organisations that struggle to implement effective cyber security measures, do so because of a belief that 'Cyber' is purely an IT problem and fail to obtain 'buy-in' and support from other senior managers and functional areas.

TIP 5: CYBER SECURITY IS A PROCESS, NOT AN EVENT

Effective Cyber Security should be viewed as an ongoing process. A single penetration test, policy or training video is insufficient to meet the evolving threat landscape. Organisations need to implement a process of continuous improvement focused on identifying and managing risks before they can become issues.

TIP 6: IMPROVE LEVELS OF IT GOVERNANCE AND COMMUNICATIONS

IT governance is frequently perceived as dull and bureaucratic, but it can mean the difference between business success and failure. Cohesis recommends to engage an expert who can help you create effective cyber security policies and procedures.

TIP 7: TEST YOUR ABILITY TO RECOVER

If your software is hosted 'on premise,' make sure that your IT support provider tests your backups and can prove that, in the event of a Cyber Incident, they can effectively recover your systems and data.

TIP 8: DON'T ASSUME THE 'CLOUD' WILL PROTECT YOU FROM A CYBER ATTACK

There is a common misconception amongst many business leaders that moving to the cloud provides a shield against all cyber attacks. While cloud vendors take security (and the marketing of their Cyber credentials) very seriously, no system or service is ever 100% secure.

TIP 9: ENSURE YOUR SYSTEMS AND DATA ARE RESTRICTED TO A 'NEED TO KNOW' BASIS

Ensuring access to networks, systems and data is provided on a 'Need to know' basis reduces the probability of 'insider' data leakage and data breaches.

TIP 10: MOBILE DEVICE MANAGEMENT

Organisations that allow corporate data to be accessed from mobile devices should employ effective Mobile Device Management - aligning technical capability and company policy to ensure staff accept that compromised devices may be locked or wiped.

VIKRAM SAREEN *Founder, Blue Bricks*
LinkedIn: www.linkedin.com/in/vikramsareen/

(Cybersecurity Expert, Multiple Patent Holder, Serial Entrepreneur, Board Advisory Member)
Vikram has over 22 years of experience in the cyber security domain. He holds multiple patents and has successfully commercialised multiple B2B Enterprise products. He has worked with over 120 BFSI enterprises, including banks and government bodies. In fact, his first work was used by then US President Bill Clinton to approve the Digital Act. He has a passion for problem solving, using technology, and is a regular speaker for discussion panels and events. Along with running his company Blue Bricks, he is also pursuing Ethical Hacking, Cyber Law and Cyber Forensics.

TIP 1. MOVE AWAY FROM EMAILS

The biggest emphasis by hackers is through emails where they encourage you to click in the message. Moving away from regular email to other team tools like Slack, Facebook, @Work or Microsoft Team will help your team to communicate much more safely. Also: create simple web forms for your customers to fill in for their enquires. Emails accessed on mobile phone are particularly dangerous as none of us install much needed protection.

TIP 2. JOB ROTATION IS MUST

Job Rotation means having employees switch their roles and work for two to three weeks in different positions. Security perspective is improved as any wrong doing, or escape routes, can be found - along with ensuring that each employee does not have complete control and become potentially dangerous. Please plan job rotations every six months at least. Also, do not give the same access to all your team members. Give MFA security tokens where you can, so it is harder for them to share their passwords with others.

TIP 3. USE GAMES TO SHARE SECURITY TIPS

No one likes boring training sessions, especially. for cyber-security. Games are the best way to engage to make it fun and better understood. Games can mean splitting teams as red, purple, blue with different roles to act out different physical and cyber scenarios. You can use Lego or Post-it notes as props. Trust me it is fun. Occasionally do cyber-security drill in the same way as regular fire drills as it will help a lot.

TIP 4. HACKERS LOVE BIG SECURITY COMPANIES, WHY?

No software or system is 100% secure. Even a 0.01% chance is enough to allow access. Microsoft, CISCO, VMWare, Remote Desktop (Citrix/VPN/VDI), Apple, Google, and hundreds of other large companies, are trusted by you and millions of others. Hackers love big companies as they will find vulnerabilities in this high volume popular software and exploit them; eventually they are causing you damage by stealing data and locking your systems. Go for less well-known, niche products that hackers do not know about. Governments do that, so why don't you?

TIP 5. HARD TALK ON FOMO VS JOMO.

If you have a limited budget amid ever-changing threats and a Cyber Security Officer is asked to protect your business, they will fail, for sure. Please don't go for FOMO (Fear Of Missing Out) or JOMO (Joy Of Missing Out) as neither will help you. Every company's security need is different to suit their particular culture and operation. You need to have an independent BOARD Advisor that is a cyber-security expert (who can guarantee you neutral and frank hard advice). Many companies select an Outsourcing Threat Monitoring Service - but they will never be fully integrated with your business's specific needs.

TIP 6. FIND A 'PARTNER' NOT A 'PRODUCT' FOR A LONG TERM FIX

The Bad, The Ugly and The Good are always catching each other in this hyper-fast cyber world; you might be ahead now, but not for long. We always think we have installed a suitable product and will be protected; this is a false promise to yourself. You need to have a partner that helps you with security needs over time. "It will not happen to me" is not a good mindset, you need to change to "It will happen to me and we need to review/fix it". A Partner that solves your problems over time, and again and again, is what is needed (products and services will become secondary).

TIP 7. PROTECT DATA AT ALL TIMES

Hackers want access to your data and ransom-ware is potentially extra cash for them; plus the fun in harassing you. Once they steal your data, then they lock you out. Data protection at rest and in transit (moving from user computer or mobile to server applications) is needed - so go for an application to protect that data. There is too much importance given to network security and antivirus but, sadly, none of them actually protect your data. If your data is protected, hackers will shy away as you are worthless to them. Ask your application provider to show you how encrypted data is stored. Don't settle for less.

TIP 8. JOINT ACCOUNTABILITY FOR "X AS SERVICE"

Online services can help us reduce cost; but it also comes with big potential headache. If Amazon AWS OR Microsoft Azure, Propertyme or Salesforce loses your data because of their system bug, they do not take accountability for their wrong doing. Most Software as Service systems that you use do not give you join accountability and data ownership. You need to demand them to be accountable for not sharing your data with other parties and to take responsibility in case any data breach happens.

TIP 9. WHERE IS MY DATA AND IS IT SECURE?

If you are going with cloud services, then data mirroring should be your key concern. We should, and can, use cloud based services but the data encryption is what you can control, so implement your own data security / encryption. There are good data protection tools that protect applications, files and data inside databases; most banks and payment companies use that already. This way, even your cloud provider mirrors (or backups up) your data, it is useless to hackers. No one wants to steal data as it then becomes useless and that is the best thing for you. Think of taking protection in your own hands, as no one else really cares for your data but you.

TIP 10. CYBER INSURANCE AND SECURITY ARE TWO SIDES OF THE SAME COIN

Your cyber security plan and rollout will give you direct benefits where you are not only protecting your users, applications, data and reputation; but you are also reducing your risk and, potentially, reducing your cyber insurance premium. In fact, most insurance companies demand you to have essential security in place in case you wish to claim. They will not force you, but they will surely reject your claim if you do not. So: best is to take security in your own hands for control, similarly to what you do for your car and home.

ALLADEAN CHIDUKWANI *Director / Principal Consultant, Cyber Experts Australia*
LinkedIn https://www.linkedin.com/in/alladean/

TIP 1. ONLY A FOOL SAYS "WE HAVE NOTHING WORTH HACKING"

Next time you think "our business is too small to hack" or "we have nothing of worth to be a cybercrime target", remember that one stolen identity can sell for about $60 to $80 on the digital black market (dark web). So your customer, employee and personal details ARE definitely worth something.

TIP 2. ATTACKS AREN'T PERSONAL

With the exception of 'hacktivists', most cyber criminals have nothing personal against you or your business. To them its just business and your data is the product. They simply hijack it and sell it back to you (ransomware) or steal it and sell it to the highest bidder on the dark web.

TIP 3. PRINTERS NEED SECURING TOO

"The printer is just a machine that spits our paper"! Well, think again. Your printer has firmware, RAM, a hard drive and network connections. Printers have all the elements that make up a computer; however most people don't see it that way. Unfortunately, hackers do and they will attack your vulnerable printer and pivot to access the rest of your network or systems. Printer security is just as important as computer security.

TIP 4. PASSPHRASE INSTEAD OF PASSWORD

Yes, your password can have spaces in it. Nowadays its best to make sure you put a space to make it a Pass-phrase (multiple words) instead of a password (one word). If you struggle to remember them, like me, then use a simple pass-phrase formulation techniques like…

"<name of grandparent starting with uppercase> <space> <town of birth> <space> <child/spouse/parent's date of birth>".

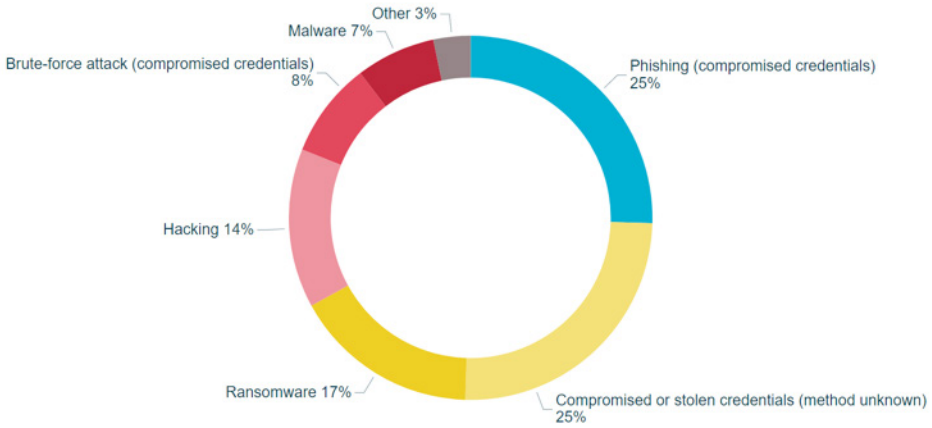
TIP 5. PHISHING EMAILS

Phishing emails are, by far, the biggest threat to individuals and businesses in Australia. The majority of ransomware attacks originate from phishing emails. The safest attitude is to treat every email as suspect until proven otherwise. Be comfortable to ignore/delete emails you are not too sure about. Remember, if it's important, they have other means to find or contact you. They can phone or SMS you (and even post a letter) if you mistakenly identify a legitimate email as a phishing email. You will not miss out on anything.

TIP 6. BEWARE OF SOCIAL ENGINEERING

Cyber criminals are now targeting and exploiting human psychology and behaviours to get unauthorised access to data and systems. They prey on human being's deeply rooted impulses, e.g.: trust, fear, compassion, ignorance, desire to help, appeal to authority etc. and trick you into doing something you shouldn't, or divulging information that you shouldn't. Treat any request via email, phone or sms as sceptical and reduce your chances of falling victim to social engineering.

CYBER INCIDENT BREAKDOWN - ALL SECTORS



Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/

TIP 7. BACKUP IS A MUST

Backups are your only sure way of recovering from a ransomware attack. Ensure backups are run daily. Paying the ransom is a strict no-no and, even if you do pay, there is no guarantee that the criminals will unlock your data, or leave a backdoor to lock it again when they are broke and need some more money.

TIP 8. CYBER ATTACK - NOT IF BUT WHEN

When it comes to cyber-attacks, it's not a matter of IF, but a matter of WHEN. Everyone is a target, whether individual, small business, large enterprise or government. The question is, when it comes your way, how do your defences stack up? Never let your guard down!

TIP 9. DUMPSTER DIVING IS A THING

Cyber criminals use all sorts of techniques to get to your systems and important information including searching through your trash for sticky notes with written passwords, access codes, product designs, business plans, phone lists, calendars and even discarded computer equipment that may still have data on them. Be careful what you dispose, all computers should be data wiped before disposal, and paper documents shredded to ensure they cannot be used by the dumpster divers.

TIP 10. HUMANS ARE THE WEAK LINK

Being the primary target for social engineering attacks e.g. phishing, employees should be educated about cyber threats, their impact on not only business but also on them as an individual. Most importantly, they should be educated on their important role in keeping the business and their livelihoods safe.

CHIOMA CHIGOZIE-OKWUM, *Director of ICT, Spiritan University Nneochi, Abia State, Nigeria.*
https://www.linkedin.com/in/chioma-chigozie-okwum-376793122/

Chioma Chigozie-Okwum, indigenous to Nigeria, is a cyber security researcher, educator, content creator and advocate. Chioma is a serial tech enthusiast and is passionate about cyber safety awareness propagation, which has earned her many national and international recognitions. She is pursuing cyber-psychology and human factor security frontiers.

TIP 1: CYBER SECURITY IS EVERYONE'S BUSINESS

It is good practice for enterprises to ensure that all staff members understand how much cyber security is everybody's business. This will ensure that everyone from top management, through finance, human resources to the doorman, understands what risk their actions (and inactions) can pose to your enterprise. Everyone should be prepared to take responsibility.

TIP 2: QUALITY ASSURE VENDORS AND 3RD PARTY PARTNERS

It is good practice to quality assure and secure proof that the cyber security policies, plans, compliance and regimes of all vendors and 3rd party service providers are in place. This is very vital to ensure that the security vulnerabilities of vendors and partners are not exploited by potential cyber threats.

TIP 3: UPDATE INFRASTRUCTURE

Outdated software and hardware have been identified as vulnerability points, as such outdated infrastructure lack the security patches implemented during updates. It is cyber security best practice to ensure that all software and hardware are updated and running the most current version to eliminate loose ends being potentially exploited by cyber threats.

TIP 4: HAVE A ROBUST CYBER SECURITY TRAINING PLAN

The importance of training, and retraining, of all personnel on cyber security plans, policies and procedures in every enterprise cannot be over emphasised. Training of staff on the latest cyber safety best practices should be periodic, and the training should be scaled to address the needs of every individual employee.

TIP 5: ENSURE ALL PAYMENT TERMINALS ARE FOOL PROOF

Point of sales terminals are usually a target point in small- and medium-scale enterprises. It is therefore very important that all payment terminals are monitored and secured to ensure that they are not hacked into and customers' details are not harvested through them, and to avoid any resulting loss of enterprise reputation.

TIP: 6 MINIMISE CHANCES OF BREEDING MALICIOUS INSIDERS

One of the weakest security links in any enterprise are malicious insiders; these can range from disgruntled, unsatisfied, poorly appreciated and even uninformed insiders. It is best practice to ensure that all employees are treated fairly to eliminate breeding a workforce that can turn malicious and potentially aid cyber threats.

TIP 7: MITIGATE AGAINST COMPLACENCY

Adhering to cyber security procedures religiously is a way of mitigating against creating loopholes that could potentially lead to cyber attacks. Employees are usually enthusiastic in the beginning, but can grow complacent over time, it is therefore important to monitor and eliminate complacency while using technology and AI. Rewards can be given to encourage compliance.

TIP 8: INSTIL AND SUSTAIN A STRONG CYBER SECURITY CULTURE

It is very vital to grow and sustain a very strong cyber security culture within the enterprise. This is achieved by quality assuring all cyber security processes. It is vital to keep reminding staff of their commitment to security using multimedia channels and deployment of simulated hacks to test compliance.

TIP 9: MONITOR AND ASSESS RISKS

It is vital to monitor and assess all possible cyber risks. The risk assessment should be done using both qualitative and quantitative methods to provide insights on the dangers posed by the risks, as well as the level of loss they could cost the enterprise. Investment in SIEM (Security Information Event Management) tools is advocated.

TIP 10: HAVE A STRONG PASSWORD POLICY

Password policies in enterprises stipulate the regimes surrounding creating and using passwords. This also ensures that all platforms accept strong passwords. Employees often feel negligent towards password policies. It is vital to monitor and enforce strict compliance to password policies leveraging on technology.