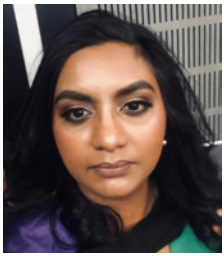

DEEVIANA DUVAL *Cyber GRC Analyst, HBF Health*
LinkedIn/Website www.linkedin.com/in/deeviana-duval
Accountant who transitioned to Cyber Security. Presently working as Cyber Governance, Risk and Compliance Analyst. I believe good cyber hygiene and continuous cyber education and awareness can reduce cyberattacks, their impacts and make us more resilient. Collaborator in City of Joondalup's Business Ready Program 2020 with Stay Cyber Safe and worked closely with small and medium businesses. Participated in various cyber awareness programs and phishing simulations exercises.

TIP 1. GET A CORPORATE EMAIL

If your business uses email, it's at risk. Most attacks occur through emails, the main communication tool is phishing, which always tops the list. Use a corporate email with your company's name as domain (avoid personal ones (e.g., Hotmail, Yahoo, etc.). There is lesser risk of corporate emails being used in scams. Corporate emails also develop your brand and image.

TIP 2. TLS/SSL CERTIFICATE FOR YOUR WEBSITE

Websites without TLS/SSL certificates are marked as unsecure by browsers, i.e., no "s" attached to http, which stands for "secure". Visitors are alerted that information exchanged is unprotected and risks being stolen, read, or modified by attackers. Google lowers rankings of unsecure websites; hence your website position will be affected on search engine results without a valid certificate. Website certificates keep internet connections secure, invest in one to give comfort to your customers that their online transactions and information are secure. Also, another plus for your image.

TIP 3. PASSPHRASES

Passphrases are the new passwords - using a sentence instead of one word makes it more difficult for attackers to crack since it's longer, for e.g., You'v3b33nstruckbyasmoothcriminal
Long passwords, with lower and upper cases, numbers and special characters make them stronger and easy for you to remember but hard for others to guess.
P.S. Treat your passwords as your toothbrush..NEVER SHARE, even with your partner!
P.P.S. Don't use that passphrase!

TIP 4. MULTI-FACTOR AUTHENTICATION (MFA) OR 2FA

MFA is an additional layer of security to credentials when authenticating yourself. You must enable MFA wherever possible. If your username and password have been cracked, your MFA will still be required to access your account.
2FA is when a 2nd factor is required, which is your password, "Something you KNOW".
With MFA, more than two factors are required before you can access an online account. The 3rd factor is "Something you HAVE", such as your phone to get a pin. 4th factor is "Something you ARE", for e.g., fingerprint, face, etc.

TIP 5. BACKUPS

Creating a copy of information on a device is a backup. Backups must be stored in secure and separate locations; (e.g. cloud - OneDrive, iCloud, etc.), and test they are accessible. Set your backups to automatic.
Backups will help you restore information in case of data loss and resume business. Data loss examples are loss of an iPad or a ransomware attack where all your files are encrypted until you pay a ransom to get a password to unlock the files.

TIP 6. PUBLIC WI-FI

If you are working while having a coffee at your favourite café and enjoying free Wi-Fi - bear in mind – When something is free, you are the product...

Malicious attackers mirror networks and you may think you are connecting to the café's network, but it's a bogus one. Information shared between devices or on a website, is intercepted by attackers (Man-in-the-Middle (MitM) attacks) and can be stolen, read, or modified. Such networks are often used to place malware (malicious software) on your device (e.g., keylogger), which captures whatever you are typing and sends the information to attackers.

TIP 7. SOFTWARE UPDATES AND AUTOMATIC UPDATES

Always use updated Operating System, Anti-virus, and Software. Updated versions are changes or corrections done to address bug fixes and, most importantly, security issues. Setting updates to automatic allows users to keep their software and devices updated without having to check for and install available updates manually. Available updates will be checked automatically and installed without user intervention.

TIP 8. BUSINESS EMAIL COMPROMISE (BEC) AND PHISHING

An example of BEC is when you receive an email from a supplier requesting to change their banking details. This should be confirmed via a phone call (to a trusted number) to ensure the request is real and not from a hacked email. Also, if an offer sounds too good to be true, you are probably being scammed. Attackers are social engineers who play with your mind and emotions. Think before you click if any of the following is being triggered: Greed, Fear, Curiosity, Urgency, Helpfulness.

TIP 9. EDUCATE YOUR TEAM

Don't assume your team knows how to be secure online. Simple negligence or unawareness can cost you your business. Communicate clearly about business cyber practices and policies with your employees. Keep them updated with the latest threats and test their knowledge through regular exercises, start with passwords best practices!

TIP 10. YOUR SUPPLIER/VENDOR SECURITY PRACTICE

The nature of your business requires you to deal with other suppliers who might not have sufficient protections, which can cause data breaches. Follow good cyber hygiene and stay updated with current trends. Follow Cyber.gov.au or Scamwatch to know the techniques attackers are using so that you can recognise when you are being targeted and can adjust your controls or respond accordingly.

Report scams and get help from ReportCyber if you think you have been scammed.