**JACQUELINE JAYNE** - *Security Awareness Advocate for the APAC region for KnowBe4*
email: jacquelinej@knowbe4.com
LinkedIn: https://www.linkedin.com/in/jacquelinejayne/
Clubhouse: @jacquelinejayne
Twitter: @JakkiJayne
KnowBe4: https://www.knowbe4.com/
Substack: https://jacquelinejayne.substack.com/

Jacqueline Jayne (JJ) currently serves as Security Awareness Advocate for the APAC region for KnowBe4, the provider of the world's largest security awareness and simulated phishing platform.
With 25+ years' experience as a conduit between people and technology, she has mastered the art of communication and influence. Previously, JJ led a successful cyber security education and awareness program that changed behaviour and created a security culture.
Her insights on the human condition and how to engage at all levels in this space are invaluable.

## TIP 1. PRACTICE GOOD PASSWORD HYGIENE

Passwords are part of daily life, and there are many rules around how long and complex they should be. Perhaps the most important rules are to have unique passwords for each application, never ever reuse the same password, keep your passwords private and never share a password with anyone else. Also, consider investing in a password manager tool to keep track of all of your passwords in a more secure manner.

## TIP 2. USE MULTIFACTOR AUTHENTICATION (MFA, 2FA)

MFA is an authentication method whereby the user is required to provide two or more forms of verification, such as a username and password, followed by a one-time code. These one-time codes can be sent via email, SMS or via a third-party authentication app. MFA prevents unauthorised access to your accounts and systems, making it more difficult for the cybercriminal to hack into your accounts and systems. If possible, always opt for the third-party authentication app.

## TIP 3. USE A VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. What this means is that your online actions are virtually untraceable. Using a VPN is especially important if you want to use free or public unsecured Wi-Fi. VPNs make it more difficult for cybercriminals to breach your privacy and access your personal information while you are online.

## TIP 4. UPDATE YOUR PRIVACY SETTINGS

Your privacy is important and most of us are unaware of what information is being shared or sold. Whether it is social media, your search history or general internet use, your data is valuable. With that in mind, make sure you check the privacy settings a few times a year on ALL the apps you use, your search engines as well as your devices.

## TIP 5. BE AWARE OF PHISHING (MALICIOUS EMAILS)

Phishing emails are designed to elicit a response, click on a link, open an attachment, provide login details or, in the case of Business Email Compromise (BEC), request a financial transaction to a third party posing as a colleague or vendor. Engaging with these emails could result in personally identifiable information, banking and credit card details or passwords being stolen. Be aware of the red flags of a phishing email https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf

### TIP 6. BE AWARE OF SMISHING (MALICIOUS SMSS)

Smishing is the SMS version of phishing. Here, we see text messages such as 'your delivery could not be made, click here' or 'click to hear a missed voice message'. If you click on the link, you will be taken to a fake website and then instructed to download software that is malicious, will steal your data and everything else from your phone. Never click on links in SMSs.


### TIP 7. BE AWARE OF VISHING (MALICIOUS PHONE CALLS)

Vishing is the voice version of phishing, with real people of the other end of the phone or a recorded message. Vishing is designed to extract details from you that can be used to steal your information. If you receive a call requesting personal information, payments or informing you of a fine, be on high alert. Do not share anything. Ask for their number to call them back (then do your research).

### TIP 8. CHECK YOUR SOCIAL MEDIA

Sometimes we forget that our online identities can easily take on a life of their own and cybercriminals are always on the lookout for our personal information. A birthday celebrated on Facebook, a promotion we post on LinkedIn, our contact details across all our social media, a seemingly innocent phone call or text message 'from our bank' or even revealing our mother's maiden name and the street we grew up on in a game shared through Instagram can have lasting negative effects. Think before your post, click or share.

### TIP 9. INCREASE YOUR AWARENESS AND EDUCATION

Empower every single one in your organisation with new school security awareness training. Human error accounts for the majority of cyber attacks (including ransomware), so awareness is the number one way to reduce the risk to your organisation. Make sure the training is relevant, engaging and ongoing, and couple it with simulations to make sure people have an opportunity to test their knowledge.

### TIP 10. BUILD A SECURITY CULTURE

It is not just what you know, it is also how your put that knowledge to use; and the resulting observable secure behaviours. Security culture is defined as the ideas, customs and social behaviours of a group that influences its security. Knowing your employees are doing the right things when you are not looking is the goal. You already have a security culture, however, is it the one you actually want?