**KARINA MANSFIELD** *Managing Director, Phriendly Phishing*
LinkedIn: https://www.linkedin.com/company/phriendlyphishing/
Profile: https://www.linkedin.com/in/karinamansfield/
Website: https://www.phriendlyphishing.com/

Karina Mansfield is Managing Director of Phriendly Phishing, CyberCX's award-winning cyber security and phishing awareness training SaaS platform. Karina has over 20 years of experience in cyber security and telecommunications. She was previously the Senior Director of Telecommunications, Media and Utilities at Microsoft, Managing Director A/NZ at KnowBe4 and has held senior management roles at Optus and Telstra

### TIP 1. OUTLINE AND IMPLEMENT A BYOD (BRING YOUR OWN DEVICE) POLICY

If you encourage employees to use personal devices for work-related tasks, make sure there are clear separation of apps using a device management system. This creates a clear separation between personal and professional data, minimising the risk of accidental data breaches and unauthorised access.

### TIP 2. USE UNCONVENTIONAL WI-FI NAMES (SSID)

A unique SSID makes it difficult for attackers to identify your network. Combine random words or phrases and avoid using any identifiable information about your business. Better yet, keep the SSID hidden.

### TIP 3. GAMIFY CYBERSECURITY TRAINING

Turn cybersecurity education into a fun and engaging experience by incorporating games, quizzes, and competitions. This approach helps reinforce best practices and keeps employees vigilant against potential threats.

### TIP 4. REGULARLY CREATE FULL BACKUPS OF YOUR NETWORK, SERVERS AND DATA

Implement the 321-backup strategy which involves 3 weekly backups, one in cloud, one in storage and one offsite. This will be valuable if you need to restore services quickly following a breach or damage to your network.

### TIP 5. USE A SEPARATE NETWORK FOR IOT DEVICES

Keep Internet of Things (IoT) devices on a separate network from your main business operations. This limits the potential damage if an IoT device is compromised.

### TIP 6. UTILISE A PASSWORD "EXPIRATION" STRATEGY

Encourage employees to update passwords periodically by assigning them an "expiration date". This helps to maintain strong password hygiene and decreases the likelihood of unauthorised access.

### TIP 7. LIMIT ADMIN PRIVILEGES

Otherwise known as the rule of least privilege. Not every employee needs admin access. Limit the number of users with administrative privileges to reduce the risk of accidental or intentional data breaches.

### TIP 8. USE A PHISHING SIMULATION STRATEGY

Get an idea of the human factor risk in your business by sending monthly phishing simulations to see how many employees are clicking on links or replying to spam. Then, apply security awareness training where needed.

### TIP 9. ENCOURAGE THE USE OF AUTHENTICATION APPS FOR DEVICES

Implement multi-factor authentication (MFA) using hashed security keys to protect sensitive accounts from unauthorised access. These offer a more robust security layer than SMS-based 2FA.

### TIP 10. CREATE A "SECURITY CHAMPION" PROGRAM

Nominate an employee from each department to act as a security advocate. These individuals will promote cyber security best practices, receive additional training, and serve as a point of contact for cyber security concerns within their department.