Phriendly Phishing

5 Ways to Help Your Organisation Stay Safe

1 Don't let the hackers egg you on!

Social engineering phishing attempts use tactics such as urgency and fear to trick your employees into divulging sensitive information or taking action that can compromise your network.

Train employees to recognise these tactics and avoid falling for them. Encourage a culture of cyber security and healthy scepticism.

2 Don’t let cyber criminals crack your passwords:

Weak passwords are an easy target for cyber criminals. Encourage employees to use strong, unique passwords that are difficult to guess.

Consider using passphrases or password managers to create and store complex passwords securely. The use of multi-factor authentication on any device that connects to the network to add an extra layer of protection should be mandatory.

3 Hop to it and update your software regularly

Outdated software can be an easy target for cyber criminals. Keep all software, including operating systems and applications, up to date with the latest security patches and updates.

Add it to the calendar so that all employees get used to running scans, updates and checking software.

4 Hunt for risky emails like you hunt for eggs

Phishing emails are a common tactic used by social engineers. Train employees to identify these risky emails and report them. Run phishing simulations to assess employees' readiness and identify areas for improvement.

Our platform can run these simulations for you, leaving you to the important stuff.

5 Don't put all your eggs in one basket:

Limit employee access to sensitive information on a need-to-know basis. Restrict access to data based on employees' roles and responsibilities.

Encrypt sensitive data and implement strict access controls to limit the impact of a potential breach.