Phriendly Phishing

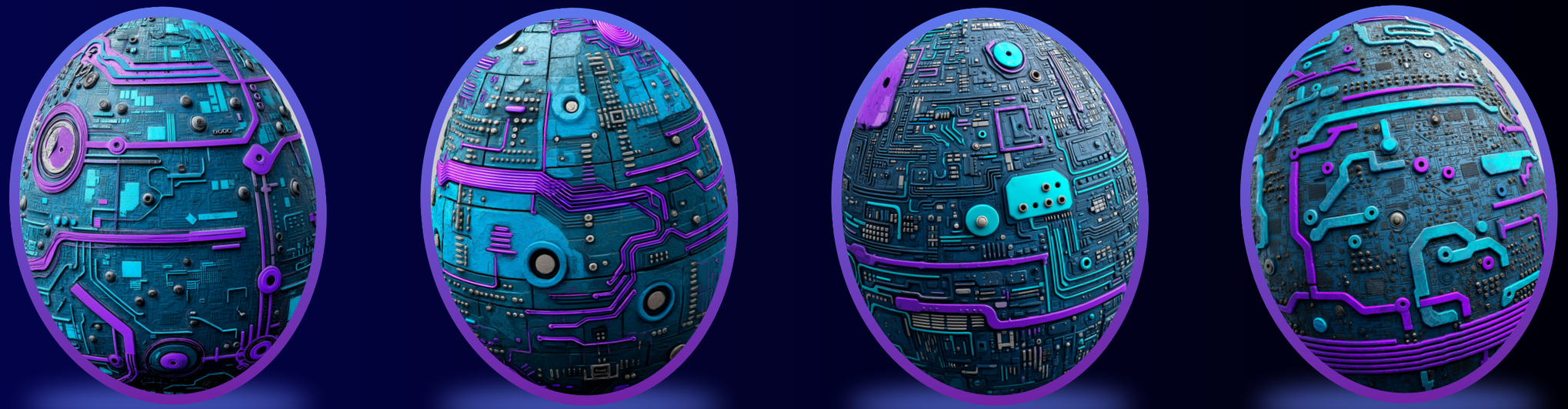
Scammers on the hunt

YOUR GUIDE TO STAYING SAFE THIS HOLIDAY

Phriendly Phishing

Scammers are on the hunt these holidays, here are helpful tips on how to keep you and your community safe.

Our cyber bunnies have uncovered tips to stay safe and they've hopped down the rabbit hole, so you don't have to. CLICK EACH EGG for an essential cyber tip!



Phriendly Phishing

SCAN WITH CAUTION: QR CODES CAN HIDE SCAMS

QR codes can hide malicious links. Scammers often use fake giveaways, deals and competitions to get people to scan.

If something looks too good to be true, it probably is. Before opening the link, check the previewed domain for spelling errors, unusual domains, or shortened URLs.

When in doubt, visit the organisation's official website directly instead of scanning.

Phriendly Phishing

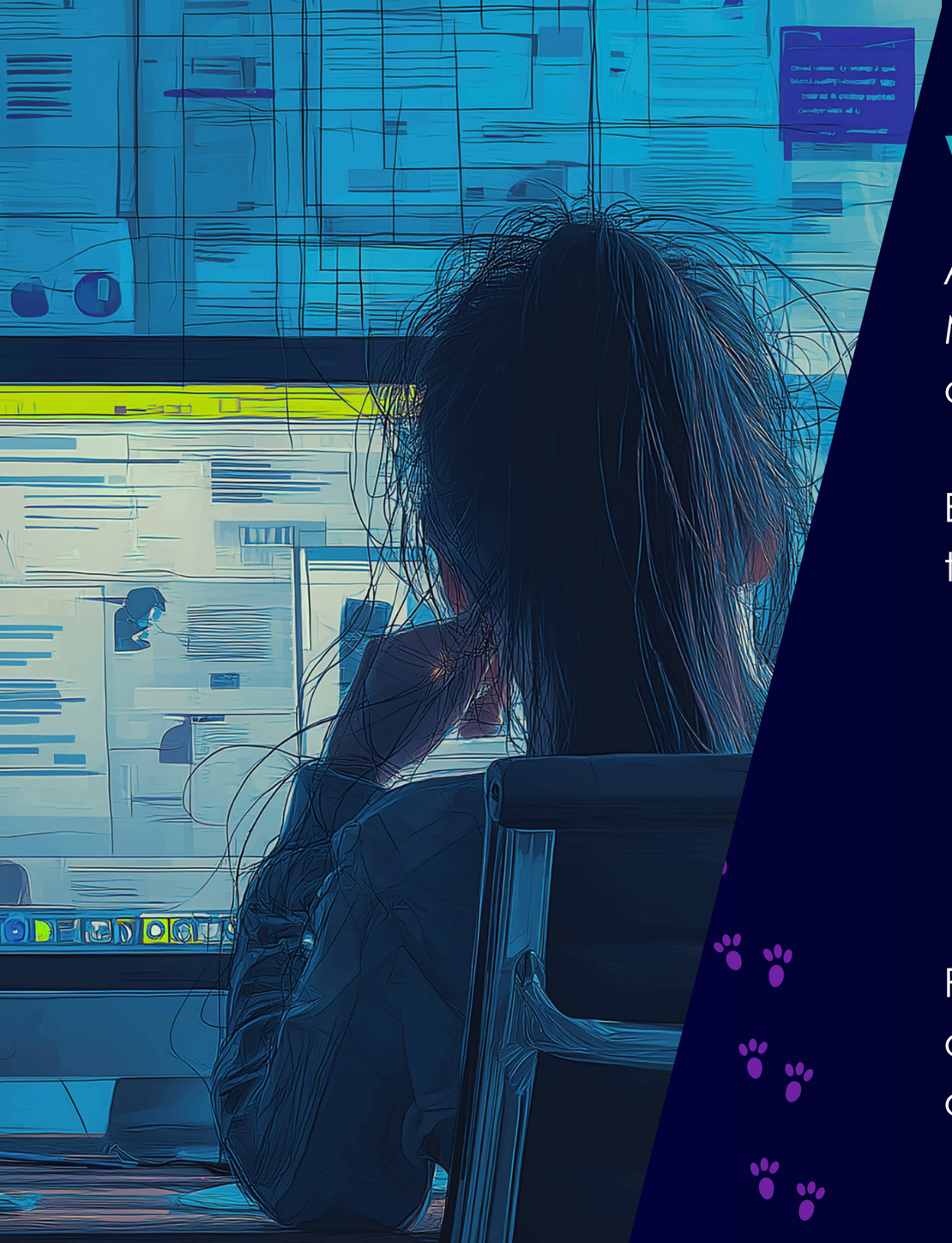
SECURE YOUR OUT OF OFFICE MESSAGES

Sharing your holiday countdown online might seem harmless, but cyber criminals love knowing when your home is empty or that you are away from the office. Information like this can give attackers clues they can use for impersonation or social engineering attacks

Keep your travel plans offline until you're back, and make sure your OOO message doesn't give too much away.

Tips for OOO Messages:

- Don't share personal info, phone number, or location.
- Use a general email or number for responses.
- Keep internal structure private to prevent exploitation.



VERIFY THE REQUEST

AI is making impersonation scams far more convincing. Messages that appear to come from colleagues, managers or trusted contacts may not be what they seem.

Before responding or taking action, take a moment to verify the request.

- Pause if a message feels urgent or unusual.
- Verify requests using known contact details.
- Ask verification questions only the real person would know.
- Avoid sharing personal information and treat AI-generated content as a draft that requires human judgement.

Pausing to verify can stop you from going down a rabbit hole that puts you and your organisation at risk.

Phriendly Phishing

BE CAREFUL ON PUBLIC WI-FI

Free public Wi-Fi is convenient, but it can also expose your activity to cyber criminals. Unsecured or fake networks can be used to intercept data or capture login details.

When possible, use your mobile hotspot instead of connecting to public networks.

Tips for Safer Connections:

- Use your mobile hotspot for a more secure connection.
- Avoid accessing sensitive accounts on public Wi-Fi.
- Disable auto-connect to unknown networks.
- Confirm the correct network name before connecting.

Phriendly Phishing

phriendlyphishing.com