Phriendly Phishing

Holiday Cyber Safety

5 TIPS TO STAY CYBER SAFE ON YOUR BREAK

1

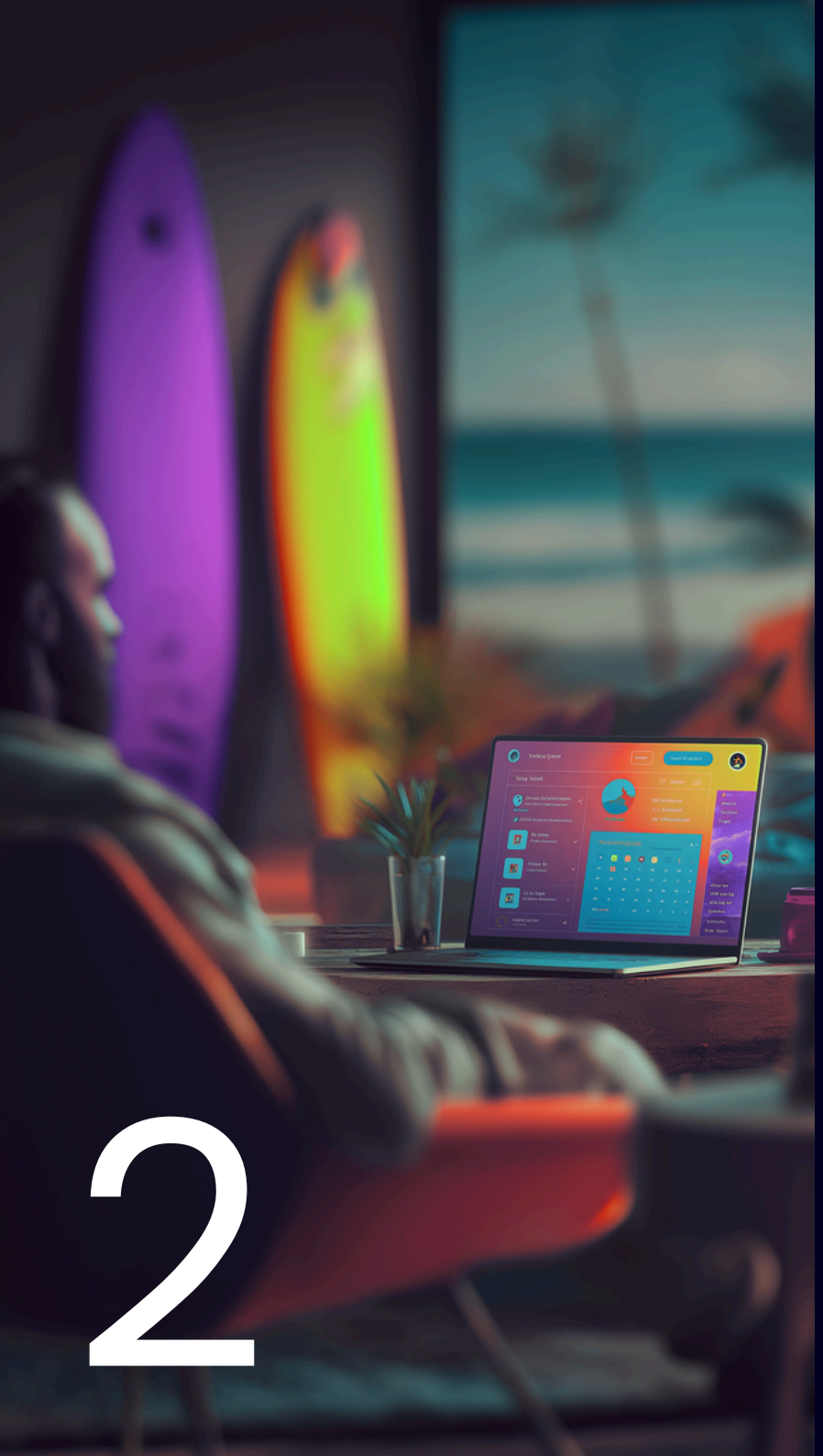
Phriendly Phishing

DON’T OVERSHARE INFORMATION ONLINE WHILE YOU’RE AWAY.

Oversharing online makes you a target. Scammers use fake support accounts and deepfakes to trick you.

- Don’t post travel plans or updates while away.
- Ignore sponsored ads — go direct to the source.
- Verify unusual requests through trusted channels.

Stay private. Stay sceptical. Stay safe.



2

KEEP YOUR OUT OF OFFICE STRAIGHT TO THE POINT

- Create a different out of office message for inside and outside your organisation.
- Avoid personal details, don’t share your travel destination or length of holiday.
- Don’t provide insight into chain of command - send queries to a general email if external.

Phriendly Phishing

BEST PRACTICE:
OUT OF OFFICE MESSAGE

Subject: Out of Office

Hi,

Thank you for your email. I am currently out of the office and unable to respond at this time. For urgent matters, please contact [General Email Address] for assistance.

Kind regards,
[Your Name]

3

THINK TWICE BEFORE BUYING OR SENDING GIFT CARDS

Gift cards are a scammer's favourite holiday trick.

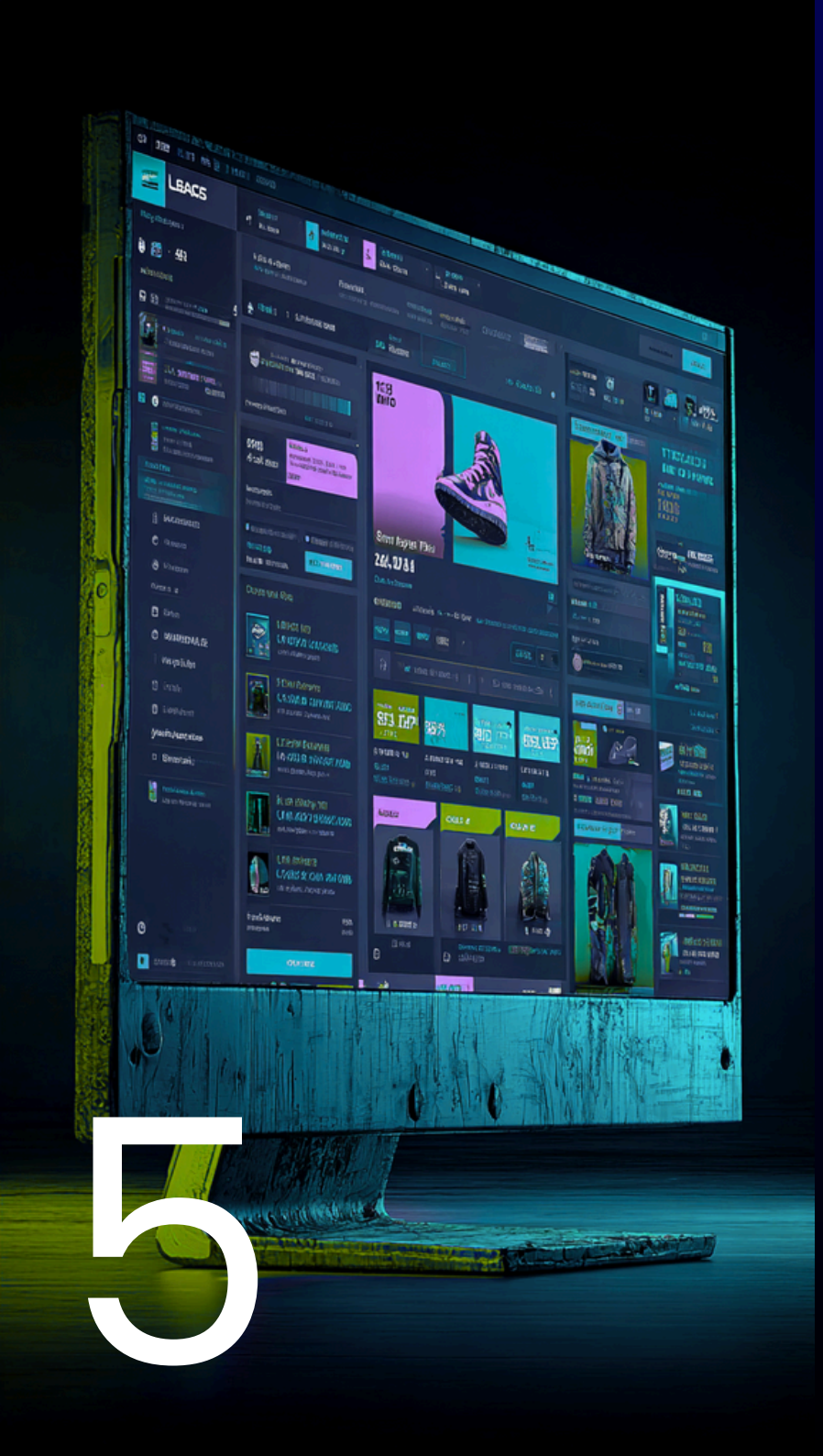
- Only buy from official retailers or trusted platforms.
- Never send gift cards as payment or donations.
- Verify any gift card requests — even if they seem to come from someone you know.
- If it feels off, it probably is. Pause and check.

CLICK WITH CAUTION: ADS CAN BE DECEPTIVE

Malvertising hides malware in online ads — even on trusted sites.

- If you click or even view these ads you may be sent to dangerous websites, that have malware automatically downloaded to your devices.
- Watch for pop-ups, redirects, and low-quality graphics.
- Keep browsers and plugins updated.
- Use ad blockers and web filters on personal devices.

If an ad looks off, close it — don't click it. Better safe than compromised.



5

PAUSE BEFORE YOU PURCHASE: SHOP SAFELY ONLINE

Online shopping is convenient — but scammers love a holiday bargain too.

- Stick to trusted sites. Check reviews and make sure the website address starts with “https://”
- Beware of deals too good to be true. Scammers often use fake discounts or urgency to trick shoppers.
- Pay securely. Use credit or debit cards and avoid unusual payment requests.
- Meet safely. For marketplace sales, inspect items in person before paying.

A few smart moves now can save you a holiday headache later.

ALWAYS REMEMBER TO SCAN FOR S.C.A.M.

Scan any email, SMS or website for common phishing tactics, just ask yourself these questions and check if it is a scam!

S Sender
Who is really sending you the email?

C Content
What's in the contents of the email?

A Action
What does the email want you to do?

M Manage
It's a SCAM! Manage & report it!

PhriendlyPhishing.com