

Phriendly Phishing

Holiday Cyber Resilience

5 TIPS TO STAY CYBER SAFE ON YOUR BREAK



1

Phriendly Phishing

KEEP YOUR OUT OF OFFICE SIMPLE AND SECURE.

Your Out of Office can reveal more than you realise. Scammers may use details about your absence or colleagues to create convincing impersonation scams.

- **Keep it private:** Avoid sharing holiday destinations, travel plans or personal details.
- **Separate your replies:** Use different messages for internal and external contacts.
- **Keep contacts general:** Direct external enquiries to a shared inbox rather than individual colleagues.

Keep scammers out of the loop while you're out of office.



Phriendly Phishing

BEST PRACTICE: OUT OF OFFICE MESSAGE

For customer-facing roles *Customer Success, Sales and Support*

Subject: Automatic reply: limited email access

Hi,

Thanks for your email. I have limited access to email at the moment and will reply by **[day, date]**.

If you need help sooner, our team monitors **[shared inbox]** and **[phone number]** from 8:30am to 5:30pm AEST, Monday to Friday. They can pick up your request straight away, so you won't need to explain it twice.

Kind regards,
[Name]



Phriendly Phishing

BEST PRACTICE: OUT OF OFFICE MESSAGE

For Higher-Risk Roles *Executives, finance, payroll, privileged IT*

Subject: Automatic reply: limited email access

Hi,

Thanks for your email. I have limited access to email at the moment and will reply when I can.

If you need help sooner, please contact **[shared inbox]** or **[phone number]**, monitored 8:30am to 5:30pm AEST, Monday to Friday.

Kind regards,
[Name]



Phriendly Phishing

HOLIDAY MODE ON. OVERSHARING OFF.

Sharing holiday updates can reveal when you're away, where you're staying and who you're with. Scammers can use these details to impersonate you or create convincing messages.

- **Be mindful of what you share:** Avoid posting travel dates, destinations or your location in real time.
- **Check your audience:** Review who can see your social media posts and updates.
- **Think before posting:** Keep travel documents, personal details and sensitive information out of photos.

Enjoy the moment now. Share the memories later.



3

Phriendly Phishing

THINK BEFORE YOU BUY: SPOT AI-POWERED SHOPPING SCAMS

AI is making fake online stores, product images and reviews more convincing than ever, making it harder to tell genuine bargains from scams.

- **Check the retailer:** Look for independent reviews and verify the official website.
- **Question the bargain:** Be wary of unusually low prices and pressure to buy quickly.
- **Pay securely:** Use trusted payment methods and avoid unexpected bank transfers.

Just because a store looks legitimate doesn't mean it is.



Phriendly Phishing

KEEPING KIDS SAFE IN A DIGITAL WORLD

School holidays often mean more time gaming, chatting and exploring online. Children can encounter fake profiles, suspicious messages and scams without recognising the risks.

- **Talk about online risks:** Discuss suspicious messages, strangers and unsafe interactions.
- **Check their settings:** Review privacy controls, in-app purchases and who can contact them.
- **Encourage speaking up:** Remind children they can ask for help without fear of getting into trouble.

Online safety starts with conversations, not just controls.



5

Phriendly Phishing

YOUR PARCEL IS ARRIVING. OR IS IT?

Expecting holiday deliveries? Scammers send fake tracking updates and missed-delivery alerts to trick shoppers into revealing personal information or making payments.

- **Check the source:** Track deliveries through the retailer's or courier's official website or app.
- **Question unexpected fees:** Be cautious of requests for redelivery payments or personal information.
- **Avoid suspicious links:** Don't follow unexpected tracking links in emails or SMS messages.

When in doubt, track it yourself.



Phriendly Phishing

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!



Phriendly Phishing