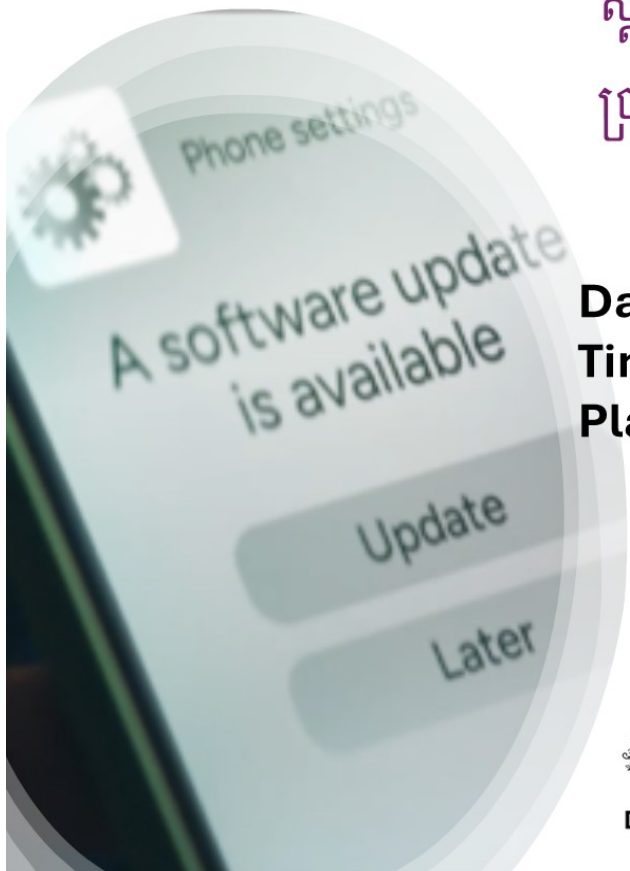


Community Forum
On
Cybersecurity



វេទិកាសន្ទនាសហគមន៍
ស្តីពីសន្តិសុខ ក្នុងការប្រើ
ប្រាស់ប្រព័ន្ធ Internet.



Date: Thursday 26/06/25

Time: 10:00pm -12:00 pm

Place: Bonnyrigg Heights Community
Centre, 46 Simpson Rd,
Bonnyrigg Heights



Australian Government

Department of Home Affairs



ក្រុមប្រឹក្សាសុខុមាលភាពខ្មែរ-អូស្ត្រាលីនៃរដ្ឋញូវសៅវែល សាធារណៈ
CAMBODIAN-AUSTRALIAN WELFARE COUNCIL OF NSW INC.

Our aim today is to address pressing
issues in cybersecurity while building
resilient mechanisms to safeguard digital
ecosystems.

គោលបំណងរបស់យើងថ្ងៃនេះគឺដើម្បី លើកយក
cybersecurity មកពិភាក្សាបញ្ហាសំខាន់ៗនៅ
ក្នុងសន្តិសុខអ៊ីនធឺណិត។

Community
Forums on
Cybersecurity



Building Resilient
Digital Networks
Together

Types of Scams

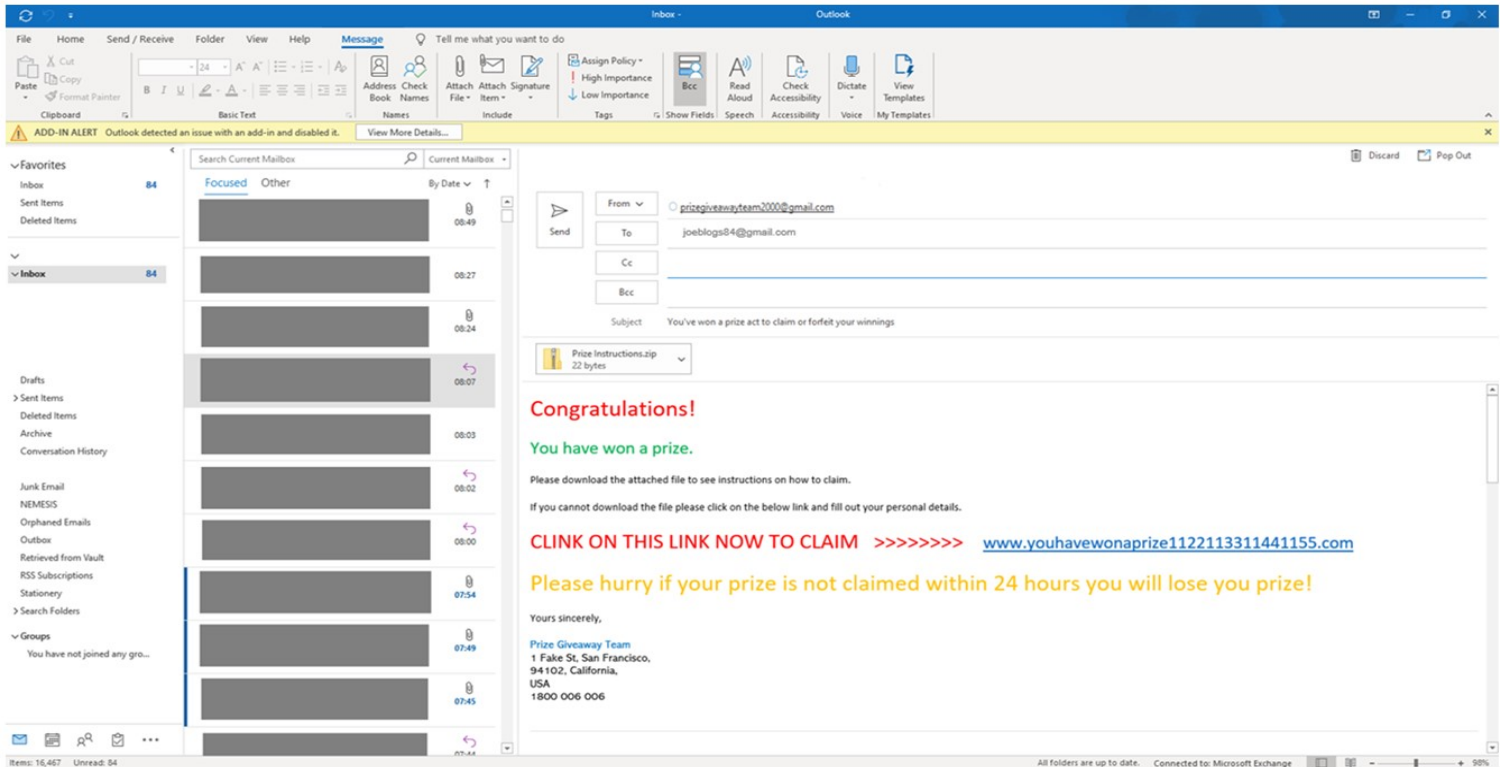
1. Dating and romance ការណាត់ជួបនិងស្នេហា
2. Investment scams ការបោកប្រាស់វិនិយោគ
3. Buying or selling ការទិញប្រលក់
4. Threats and extortion គំរាមកំហែងការជំរិតទារប្រាក់
5. Job and employment ការងារ
6. Unexpected money លុយដែលមិននឹកស្មានដល់
7. Fake charities សហគមន៍ឥតឈ្មោះក្លាយ
- 8. Text or SMS អត្ថបទឬសារ SMS**
- 9. Email and website អ៊ីមែល និងគេហទំព័រ**
- 10. Phone ទូរស័ព្ទ**
11. Cryptocurrency រូបិយប័ណ្ណគ្រីបតូ
12. Social media, app-based and online messaging ប្រព័ន្ធផ្សព្វផ្សាយសង្គម កម្មវិធីផ្ញើកំណត់ត្រា និងការផ្ញើសារតាមអ៊ីនធឺណិត
13. Attempts to gain your personal information ការព្យាយាមដើម្បីទទួលបានព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក។
14. Travel, prizes and lottery scams ការធ្វើដំណើរ រង្វាន់ និងការបោកប្រាក់ឆ្នោត

EMAIL PHISHING SCAMS

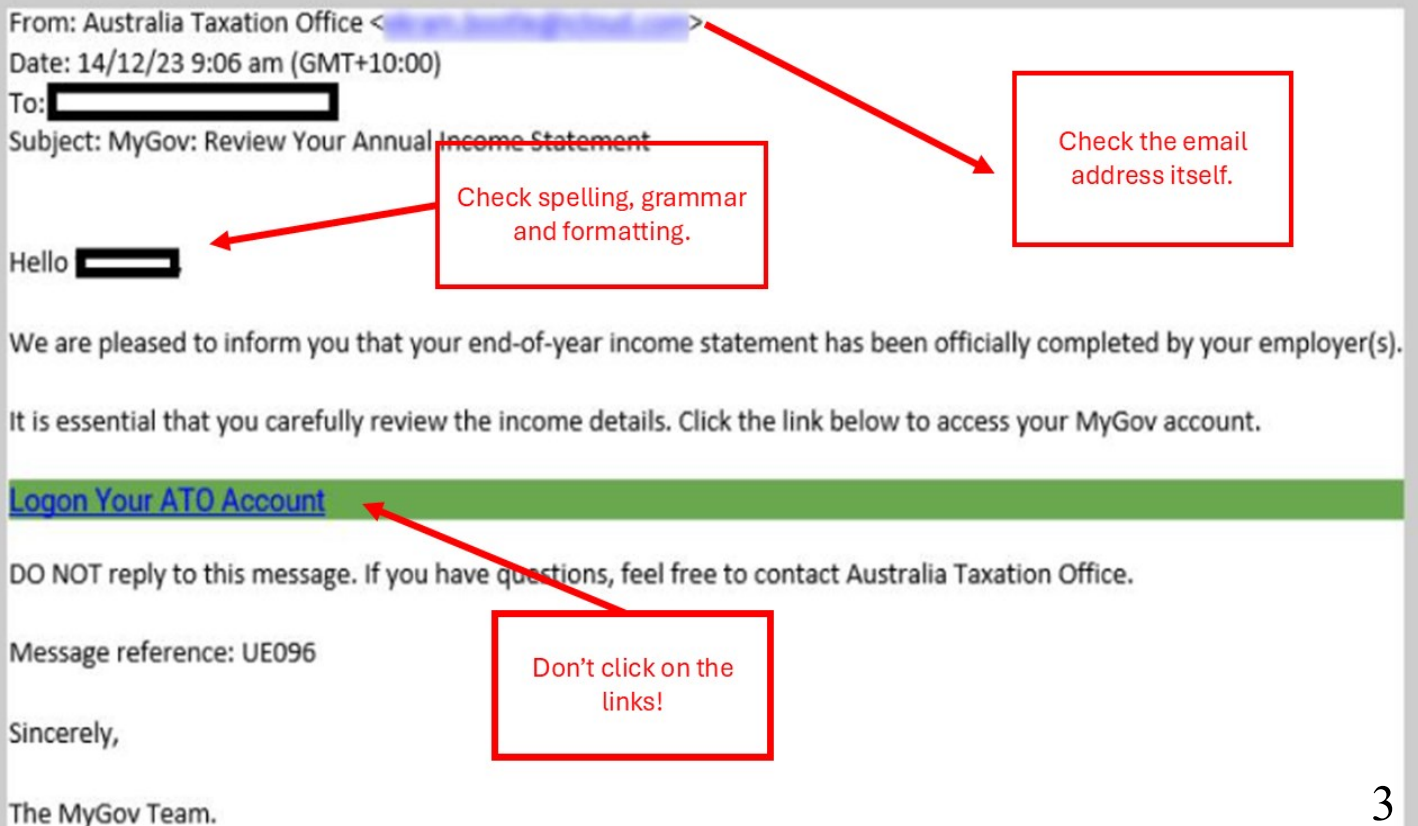


- Catchy subject line.
- Asks you to download an attachment or click on a link.
- Doesn't address you by name.
- Comes from a free provider email like Gmail/Outlook.
- Creates urgency to act now.

EMAIL PHISHING/PRIZE GIVEAWAY SCAM



ATO email



Fake invoice sent to CAWC

cawcns@bodianwelfare.org.au

From: Wix.com Inc <info.hxg000y6wseb@urweiblich.com>
Sent: Friday, 7 February 2025 12:24 PM
To: cawcns@bodianwelfare.org.au
Subject: Your Wix payment method was declined



Sender email is not belonged Wix

There Was a Problem with Your Renewal Payment

Amount is wrong format

We ran into some trouble processing the renewal payment for your Premium Plan.

Here are the details:

Transaction Date: February 7, 2025
Transaction Amount: 12,18 \$

We encourage you to contact your bank or credit card company for more information.

[Complete Your Payment](#)

Wix never sent the link to be paid

SCAM

OPTUS yes **SCAM ALERT**

Dear Customer:

Your account has been flagged and temporarily limited, several errors were detected when processing your previous monthly bill.

Let's get it fixed, please visit [Optus Account Ownership Portal](#)

Note: You have been strictly advised to complete this measure before 48 hours to avoid account closure.

Thank you,

Singtel Optus Pty Limited

OPTUS

Your details need to be updated !

Hello,

Due to the latest security breach all our customers are required to update their details to regain access to our services.

[Update !](#)

P.S: All clients who do not proceed with the verification of their details will be suspended temporarily until further notice.

ATO EMAIL SCAM

From: Australia Taxation Office <[redacted]>
Date: 14/12/23 9:06 am (GMT+10:00)
To: [redacted]
Subject: MyGov: Review Your Annual Income Statement

Check the email address itself.

Hello [redacted]

We are pleased to inform you that your end-of-year income statement has been officially completed by your employer(s).

It is essential that you carefully review the income details. Click the link below to access your MyGov account.

[Logon Your ATO Account](#)

DO NOT reply to this message. If you have questions, feel free to contact Australia Taxation Office.

Message reference: UE096

Sincerely,

Don't click on the links!

The MyGov Team.

Text message SCAMS អត្ថបទប្រសាវ

Text Message
Today 2:39 AM

[Aus Post]:Address label is not recognised, post office delivery has been suspended. Please correct it as soon as possible:<https://auspost.mypost.gov.au>

AUTH-ATO >

Text Message
Monday 11:33 PM

New notification in your MyGov inbox, head to <https://my.gov.au> to resolve.

W App: A friend from null has sent you a compliment!

Tap to view: <https://g-arakotsis21791/bl9kpk>

W App: A friend from null has sent you a compliment!

Tap to view: <http://arakotsis21791/m1ea6>

< Spam and blocked

52jelz9 Missed Call: You have a missed call. Caller left you a message: <https://bestreviewx.co...>

ce9jpc Voicemail: You have 1 new Voicemail(s). Go to <https://devl.oneedsvoice.com/n.php?...>

Hey mum it's me. I got a new number, you can delete the old one 🙏❤️ 2:22 pm

Which me is it????? 2:22 pm ✓

Your oldest and cutest child xx 2:23 pm

I got a new phone. I'm still transferring everything 2:23 pm

Good luck x 2:23 pm ✓

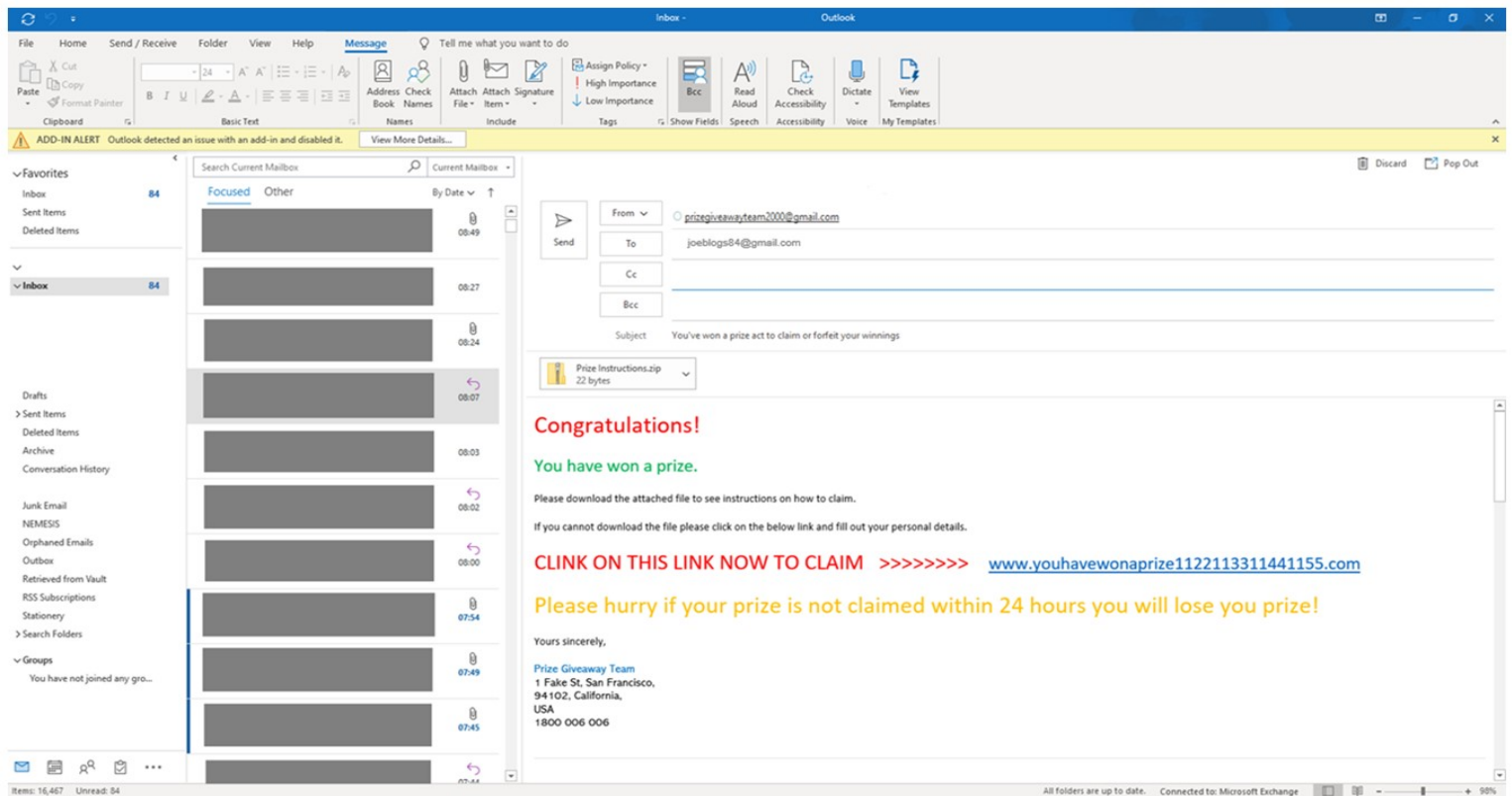
I have a little problem I can't solve...Can you help me with it? 2:24 pm

What is it hun? Just got to work but you can message for the best half hour or chat if you need xxxx 2:24 pm ✓

Well because of the new device I have to transfer all apps, but the banking app has put a 48-hour security on the app due to fraud. All nice but I have to pay 2 payments 🤔. Very annoying because I can't do anything about it. Could you possibly pay for me and I'll return it as soon as possible??? 2:24 pm

Sorry to bother you with this 2:24 pm

EMAIL PHISHING/PRIZE GIVEAWAY SCAM



Electricity Email Scam

cawcns@w@camboianwelfare.org.au

From: Origin Energy <origin@mvvnews.com.br>
Sent: Thursday, 6 February 2025 12:05 PM
To: cawcns@camboianwelfare.org.au
Subject: Please confirm your refund!

Your Origin refund bill

Account number A-*****16

Billing reference 6*****04

Hi Valued Customer,

Your latest electricity bill from Origin is has been paid twice due to a system error.

Please complete a claim to get the refund.

You can find copies of your earlier bills in My Account. Any questions, send us an email at hello@origin.com.au or give us a call on **13 24 61**.

All the best,
The Origin Team

Amount refund

\$196.12

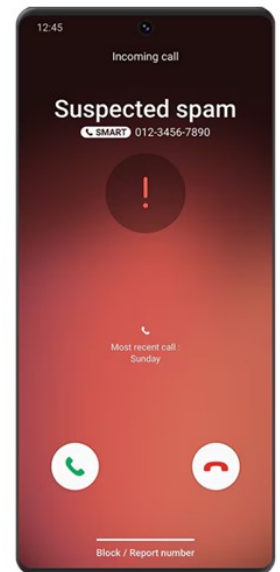
Claim now

10. Phone ទូរស័ព្ទ

Scammers often pose as representatives of familiar organizations, such as government agencies, banks, or charities, to gain the trust of their targets.



AUTOMATED PHONE CALL/VOICE
MESSAGE SCAM



Hello, your
telecom service
will be suspended.
Please press

1. Verify Claims: Always verify the authenticity of the claims independently. Contact the organization or department directly using official contact information.

ត្រូវតែផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវនៃការទាមទារ
ដោយឯករាជ្យ។ ទាក់ទងអង្គការ ឬនាយកដ្ឋាន
ដោយផ្ទាល់ដោយប្រើព័ត៌មានទំនាក់ទំនងផ្លូវការ។

មានបី

1. Set up multi-factor authentication
2. Install software updates regularly
3. Create strong and unique passphrase

STAY SECURE CAMPAIGNE

Our Stay Secure Campaign is dedicated to raising awareness about the importance of cybersecurity in today's digital age. By educating individuals and organizations on best practices, we aim to reduce the risk of data breaches and cyber attacks. Join us in making the internet a safer place for everyone.

យុទ្ធនាការរក្សាសុវត្ថិភាពរបស់យើង គឺខិតខំដល់ការលើកកម្ពស់ការយល់ដឹងអំពីសារៈសំខាន់នៃសុវត្ថិភាពអ៊ីនធឺណិតនៅក្នុងយុគសម័យឌីជីថលនាពេលបច្ចុប្បន្ននេះ។ តាមរយៈការអប់រំបុគ្គល និងអង្គការអំពីការអនុវត្តល្អបំផុត យើងមានគោលបំណងកាត់បន្ថយហានិភ័យនៃការបំពានទិន្នន័យ និងការវាយប្រហារតាមអ៊ីនធឺណិត។ ចូលរួមជាមួយពួកយើងក្នុងការធ្វើឱ្យអ៊ីនធឺណិតក្លាយជាកន្លែងមានសុវត្ថិភាពជាងមុនសម្រាប់អ្នករាល់គ្នា។

Install software updates regularly to keep your devices secure

អាប់ដេតកម្មវិធីនៅលើឧបករណ៍របស់អ្នកឱ្យទៀងទាត់ ដើម្បីឱ្យមានសុវត្ថិភាព

Set up multi-factor authentication



Install software updates regularly to keep your devices secure

អាប់ដេតកម្មវិធីនៅលើឧបករណ៍របស់អ្នកឱ្យ
ទៀងទាត់ ដើម្បីឱ្យមានសុវត្ថិភាព



Create strong and
unique passphrase

បង្កើតឃ្លាសម្ងាត់
strong and
unique passphrase



**កុំបណ្តោយខ្លួនអ្នក
ឱ្យទទួលរងប៉ះពាល់។**

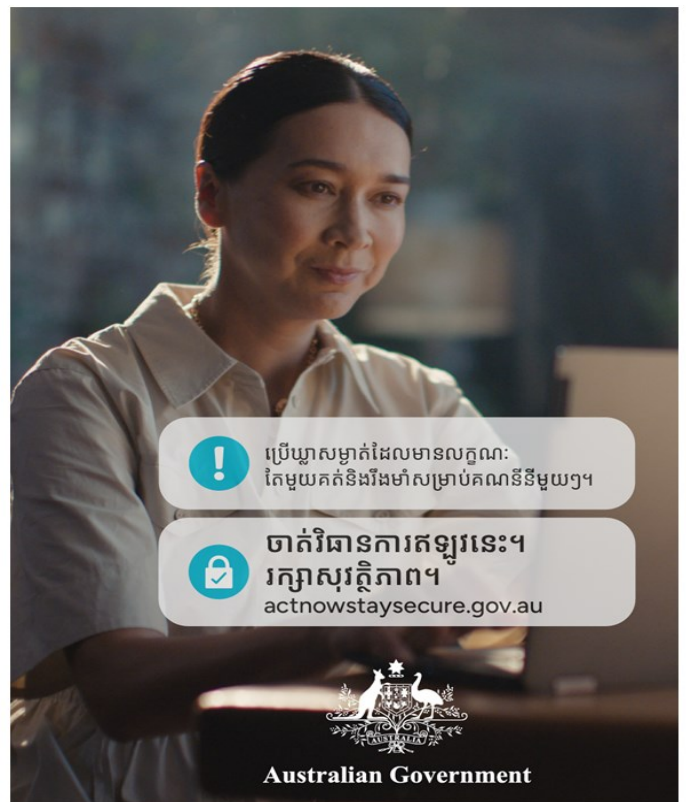
ប្រើឃ្លាសម្ងាត់ដែលមានលក្ខណៈ
តែមួយគត់ និងរឹងមាំសម្រាប់
គណនីនីមួយៗ។

តើអ្នកកំពុងប្រើយ៉ាងណាទៅតាមអនឡាញ?

 ចាត់វិធានការឱ្យបានរឹងមាំ
រក្សាសុវត្ថិភាព។
actnowstaysecure.gov.au



ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។
Authorised by the Australian Government, Canberra.



ប្រើឃ្លាសម្ងាត់ដែលមានលក្ខណៈ
តែមួយគត់និងរឹងមាំសម្រាប់គណនីនីមួយៗ។



ចាត់វិធានការឱ្យបានរឹងមាំ
រក្សាសុវត្ថិភាព។
actnowstaysecure.gov.au



Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។



ដំឡើងការផ្លាស់ប្តូរឯកតាធានី។



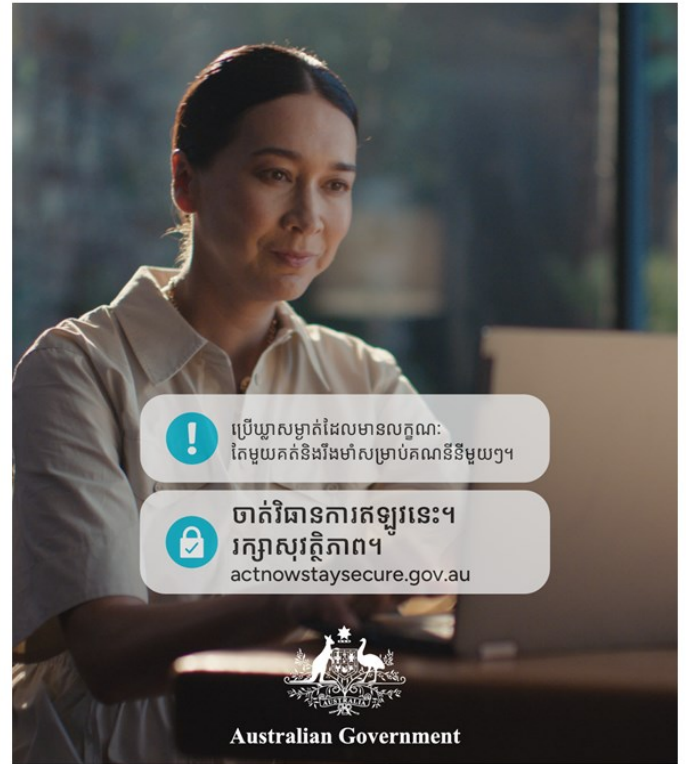
ចាត់វិធានការធានាសុវត្ថិភាព។

actnowstaysecure.gov.au



Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។



ប្រើប្រាស់ម្ចាត់ដែលមានលក្ខណៈ
តែមួយគត់និងវិធីសាស្ត្រប្រាប់គណនីនីមួយៗ។



ចាត់វិធានការធានាសុវត្ថិភាព។

actnowstaysecure.gov.au



Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។



ដំឡើងបច្ចុប្បន្នភាពសូហ្វ្វែរទាំងអស់
ដើម្បីរក្សាខ្លួនបរិច្ចាគនាបស្ថានភាព
ឱ្យមានសុវត្ថិភាព។



ចាត់វិធានការធានាសុវត្ថិភាព។

actnowstaysecure.gov.au



Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។



ដំឡើងការផ្លាស់ប្តូរឯកតាធានី។



ចាត់វិធានការធានាសុវត្ថិភាព។

actnowstaysecure.gov.au



Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។



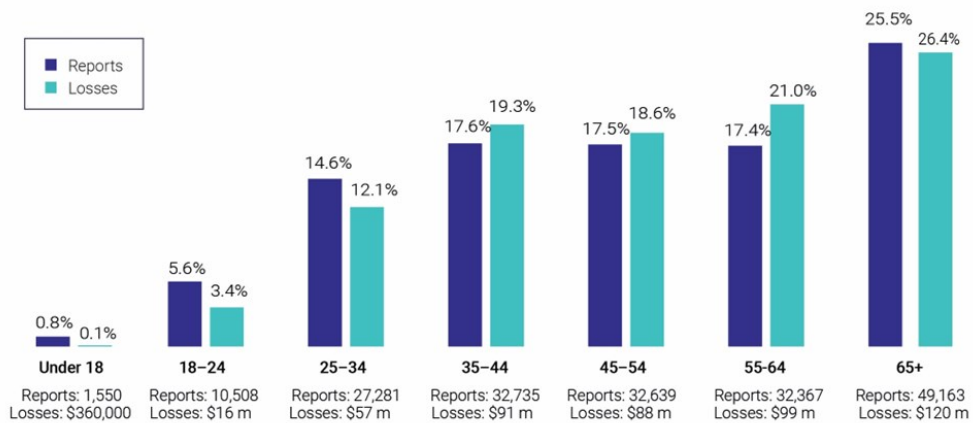
 តើអ្នកកំពុងប្រថុយនឹងអ្វីខ្លះ នៅតាមអនឡាញ?

 ចាត់វិធានការធានារួមនេះ។ រក្សាសុវត្ថិភាព។
actnowstaysecure.gov.au


Australian Government

ផ្តល់សិទ្ធិអនុញ្ញាតដោយរដ្ឋាភិបាលអូស្ត្រាលី Canberra។

Age

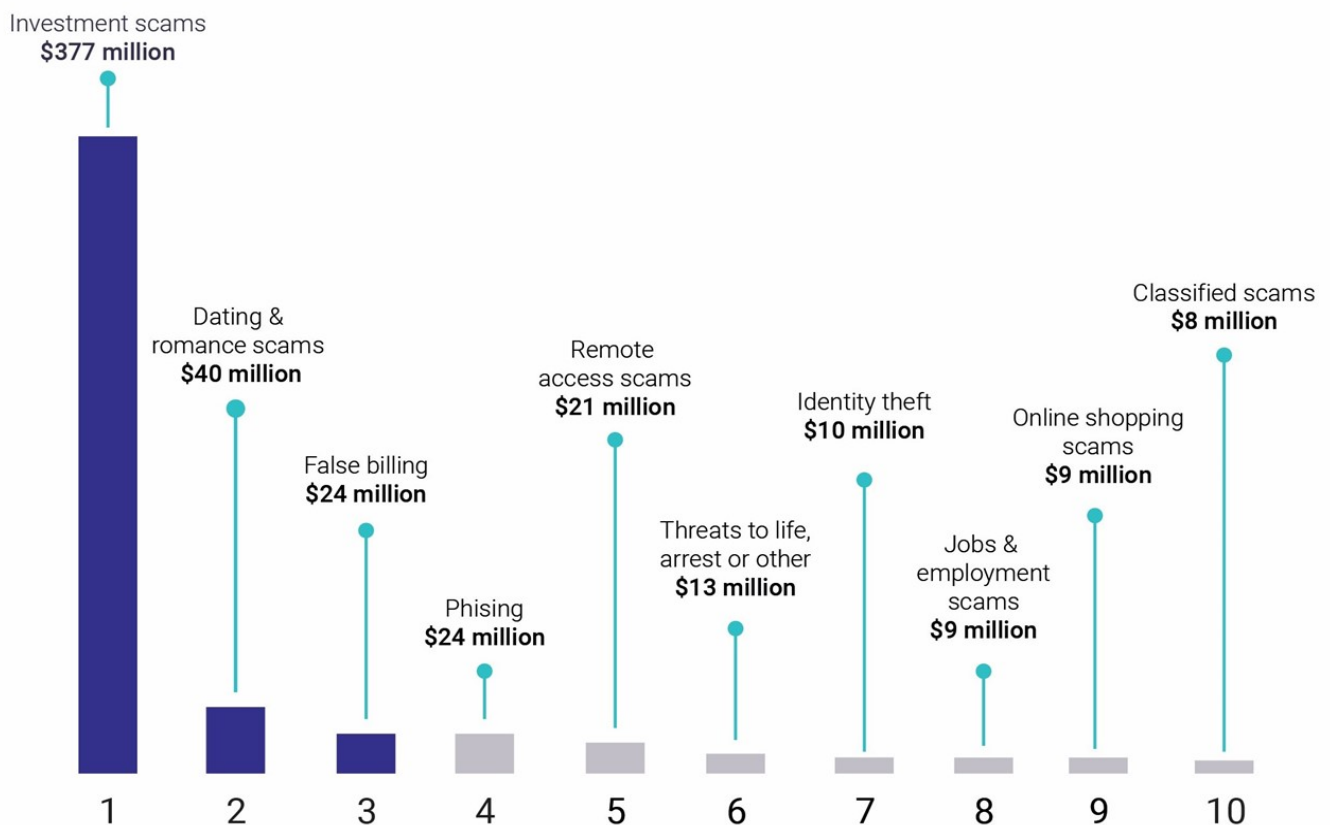


ACCC
 AUSTRALIAN COMPETITION
 & CONSUMER COMMISSION

Top contact methods

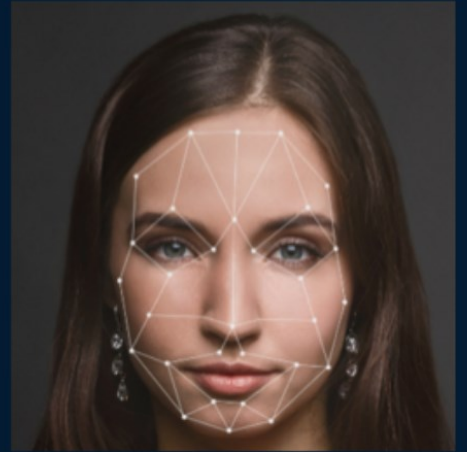


Top scams by loss as reported to Scamwatch



EMERGENCE OF DEEP FAKES

- They look real.
- They sound real.
- They can be based on a real person.
- But they are not real.



- HOW DO YOU SPOT A DEEPPFAKE?.
- BAD LIP SYNCING.
- PATCHY SKIN TONE.
- BLURRED EDGES AROUND THE FACE.
- STRANGE REFLECTIONS

Blurring, cropped effects or pixilation (small box-like shapes), particularly around the mouth, eyes and neck

Skin inconsistency or discoloration

inconsistency across a video, such as glitches, sections of lower quality and changes in the lighting or background

Badly synced sound

Irregular blinking or movement that seems unnatural or irregular

Gaps in the storyline or speech.

Unexpected requests for personal or financial information.

Offers that seem too good to be true.

Unusual or suspicious email addresses and URLs.

High-pressure tactics urging immediate action.

Spelling and grammatical errors in communications.

Recognizing Warning Signs

Top tips to avoid scams

STOP – Don't rush to act. Scammers will create a sense of urgency.

THINK – Ask yourself if you really know who you are communicating with? Scammers can impersonate others and lie about who they are – especially online.

PROTECT – Act quickly if something feels wrong. If you have shared financial information or transferred money, contact your bank immediately. Help others by reporting to [Scamwatch](#) .

Preventative Measures

1. • **Verify Claims:** Always verify the authenticity of the claims independently. Contact the organization or department directly using official contact information.
2. • **Stay Calm:** Do not let the scammer's threats pressure you into making immediate decisions. Take time to think and assess the situation.
3. • **Report Incidents:** Report any suspicious activity to the appropriate authorities to help prevent further victimization of others.
4. • **Educate Yourself:** Stay informed about common scam tactics and share this knowledge with friends and family to raise awareness.