



Could you get scammed? ... online safety part 2

Mark Dixon

for ASA, 3rd September 2024

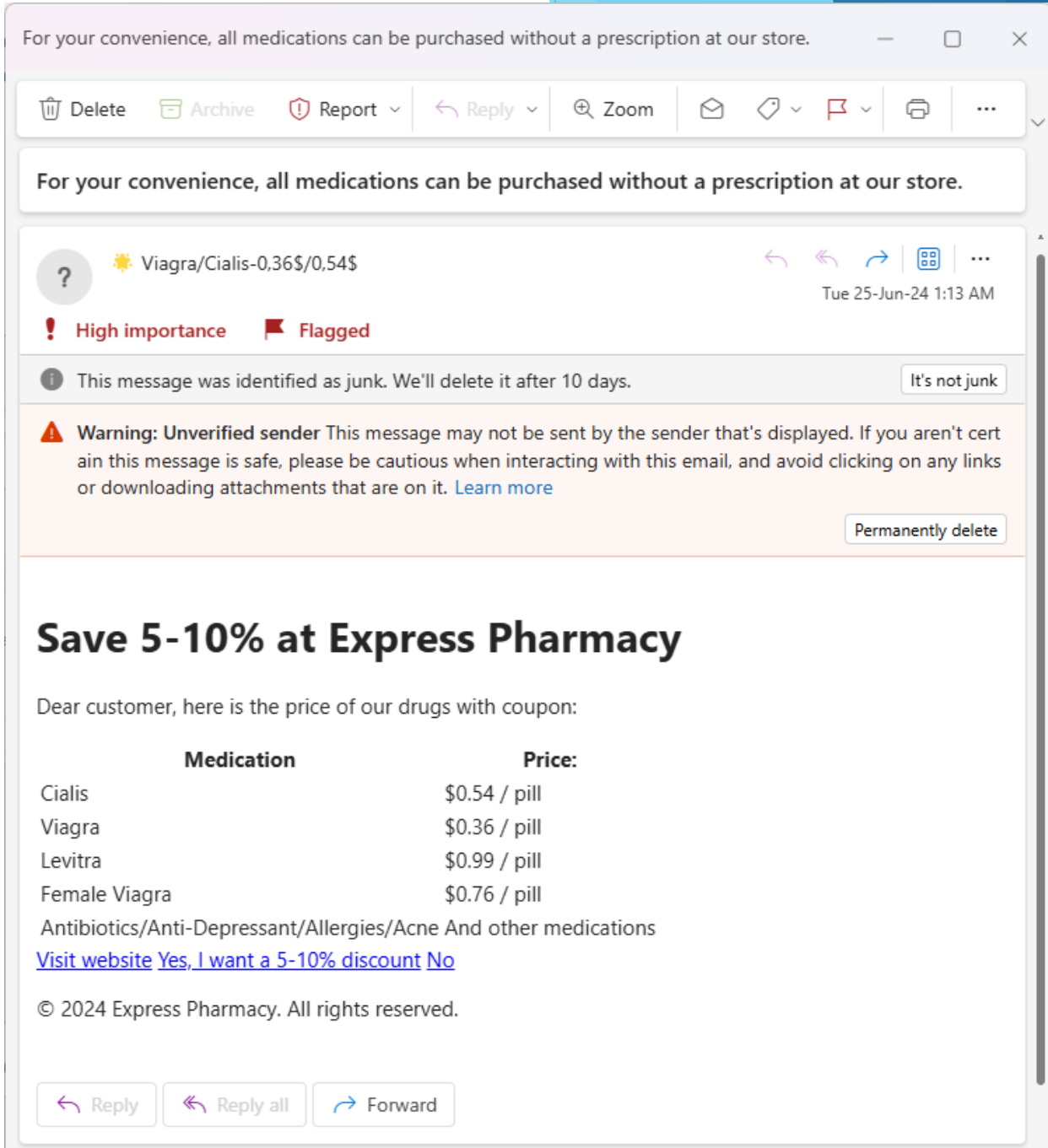
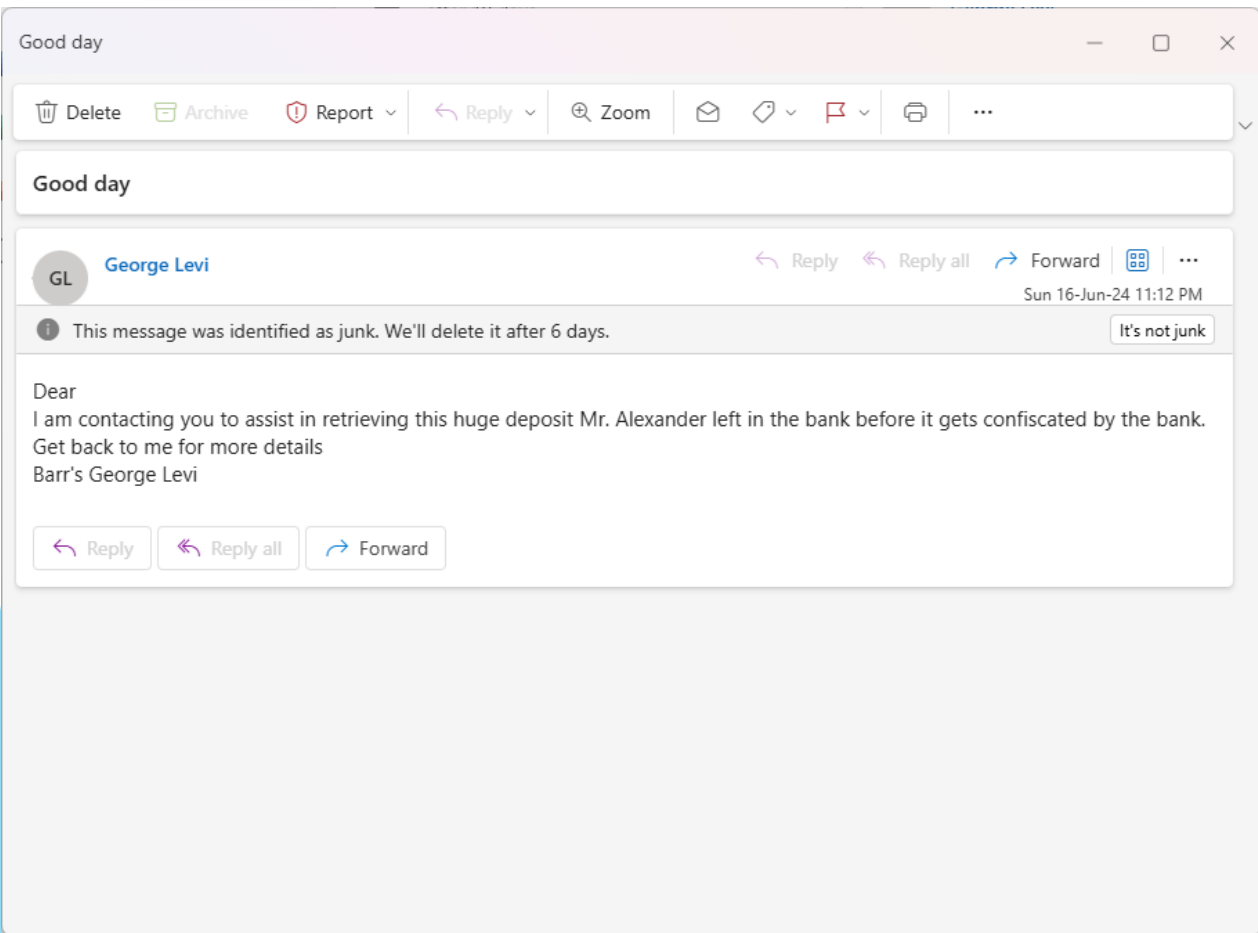
What will we cover today

- ▶ Very quick review - email scams, SMS scams, phone scams - see notes from last time
- ▶ Social media scams (e.g. on FaceBook) such as romance scams
- ▶ Deepfake audio & video
- ▶ Password ideas
 - ▶ Pwned? - <https://haveibeenpwned.com/>
 - ▶ Hackers & hacker tools.
- ▶ Miscellaneous scams:
 - ▶ Public computers, e.g. libraries, cafes - KeyLoggers (vampire in the house)
 - ▶ Broker scams (unsolicited offers that sound great) - most unsolicited are scams
 - ▶ Online shopping - some vendors are not legitimate
- ▶ Ideas for keeping safe
- ▶ Questions and (*short*) comments welcome during presentation




Examples of email scams


- some are obvious



email & SMS scams, maybe less obvious

DOCUMENTS

 E_document <dupchak@fastmail.fm>(E_document via re)
To [redacted] 7:37 AM

 If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.


Your Document is available

[View Documents](#)

Thanks
E-document



Paid Invoice

 Amelia Charles <swansjuniors@outlook.com>
To: mdofperth@outlook.com Wed 17-Jul-24 8:17 AM

 Signed.shtml
Saved





Hello mdofperth,
Please find attached paid invoice.
Many Thanks
-----Receipt Summary-----
Date: Wednesday, July 17, 2024 12:9 a.m. The complete version
of this receipt
has been attached to this e-mail: mdofperth@outlook.com

 Reply  Forward

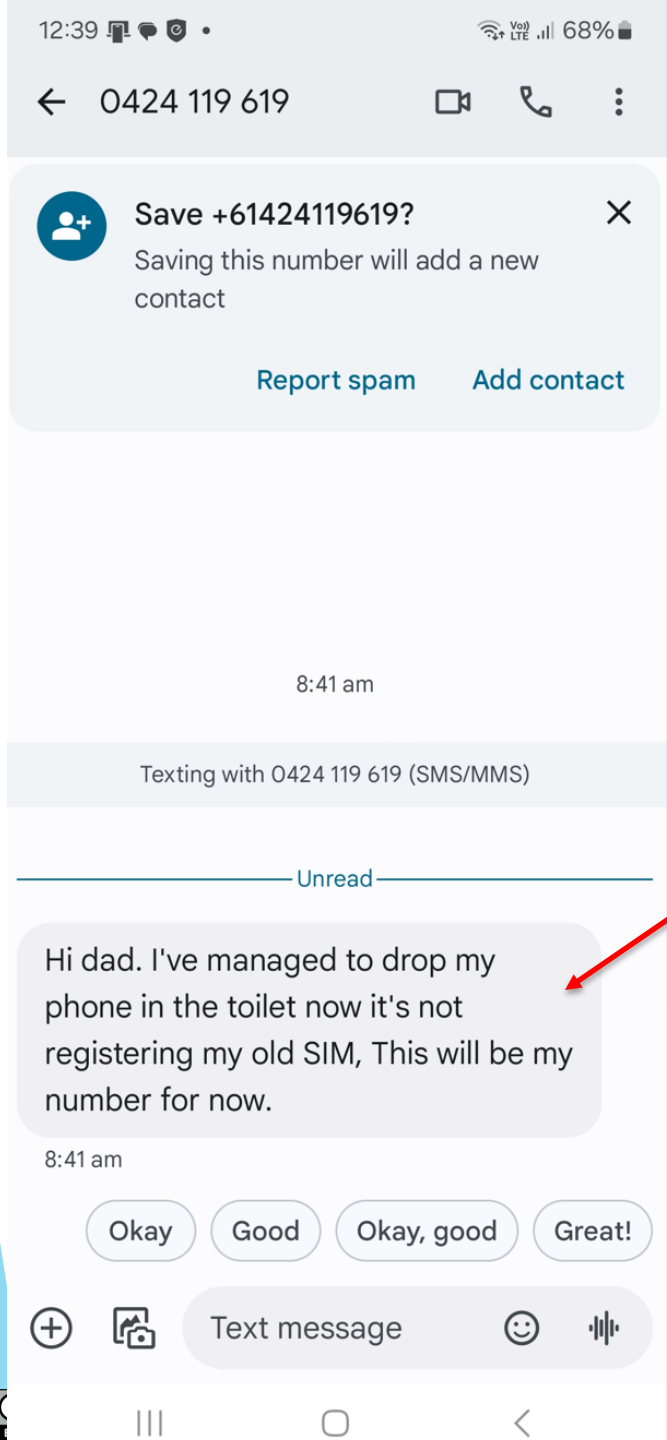
5:40 [signal icons] 89%
← +63 910 815 2160  

Hello. Sorry to bother you.
My name is Lee Soo Yeon. A girl from Korea.
I'm traveling in Australia. I'm looking for my soul mate.
My sister says Australian men are gentle, respectful, positive and trusting.
You can add my Whatsapp:
<https://wa.me/61413769728?IHy=tXd4NSPZXP>
Share our photos and lives. Get to know each other.

Texting with +63 910 815 2160 (SMS/MMS)

  Text message  





SMS claiming to be family on new phone.

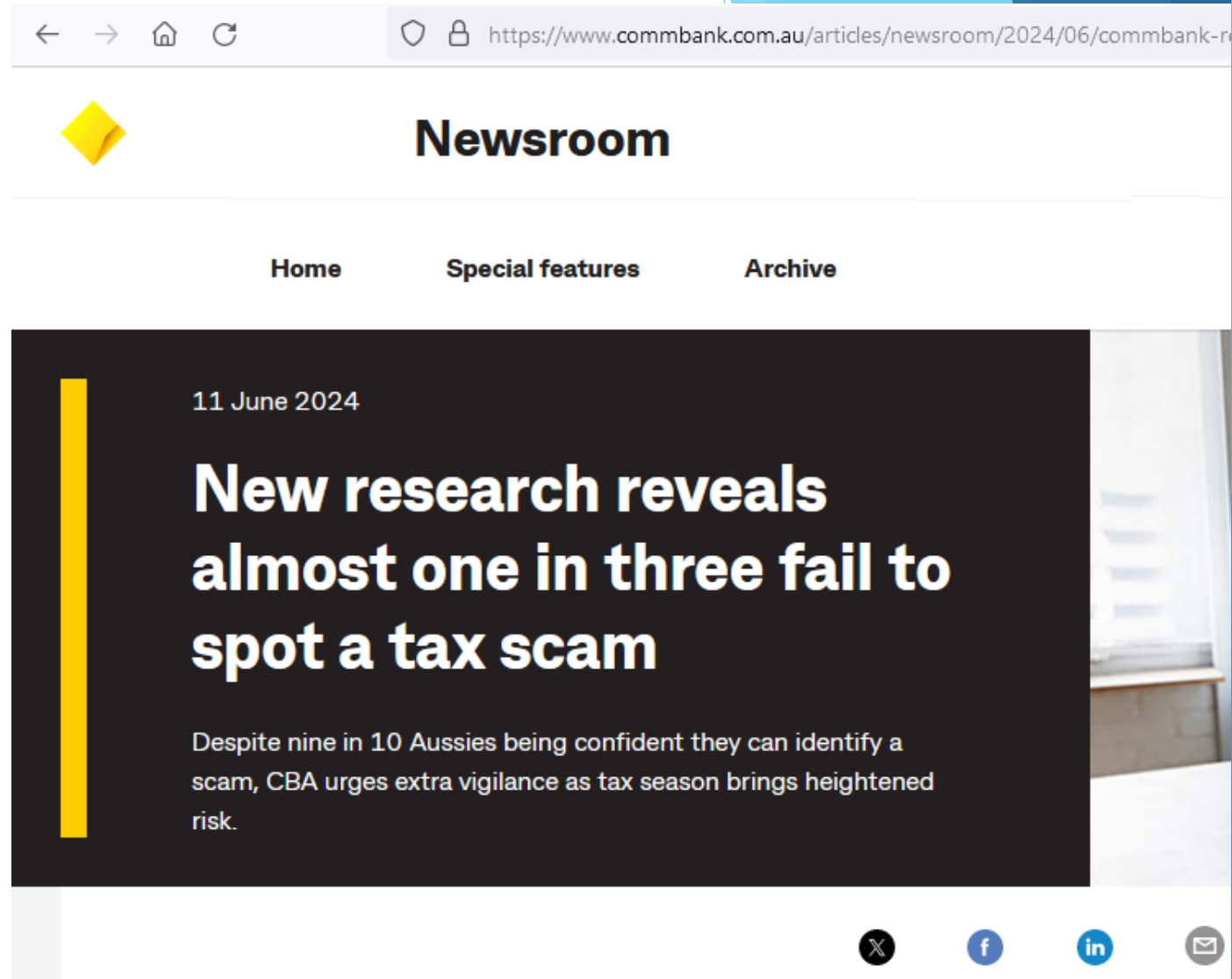


CBA says: Aussie taxpayers need to stay alert during tax season. New research¹ reveals almost a third fail to spot a tax scam. When multiple tax phishing scams were tested with Australians over the age of 18, only 69 per cent could successfully identify all of them.

Interestingly, nine in 10 believed they were confident they could spot a fake SMS or email.

The research also showed around one in four Australians have been exposed to a tax-related scam. As millions of people wait for a tax return over the next few months, scammers will be keen to capitalise on the moment.

¹YouGov research comprised of a nationally representative sample of 1,023 Australians aged 18 and above, conducted online between 20 May and 23 May 2024.



The screenshot shows a web browser displaying a news article from the CBA Newsroom. The URL in the address bar is <https://www.commbank.com.au/articles/newsroom/2024/06/commbank-...>. The page features a yellow diamond logo and the word "Newsroom" in a large, bold font. Below the logo, there are navigation links for "Home", "Special features", and "Archive". The main content area has a dark background with a yellow vertical bar on the left. The article is dated "11 June 2024" and has a headline that reads "New research reveals almost one in three fail to spot a tax scam". A sub-headline below the headline states: "Despite nine in 10 Aussies being confident they can identify a scam, CBA urges extra vigilance as tax season brings heightened risk." At the bottom right of the article, there are social media sharing icons for X, Facebook, LinkedIn, and Email.



This ASIC boss was scammed. She has a warning for you



Hannah Wootton

Reporter

When former Australian Securities and Investments Commission deputy chairwoman Karen Chester tried to buy shoes in a sale last month, she thought they would be a nice surprise for her daughters.

She did not expect them to be part of a scam, or that she and two friends, who are also executives, would fall victim to it.

Social Media scams

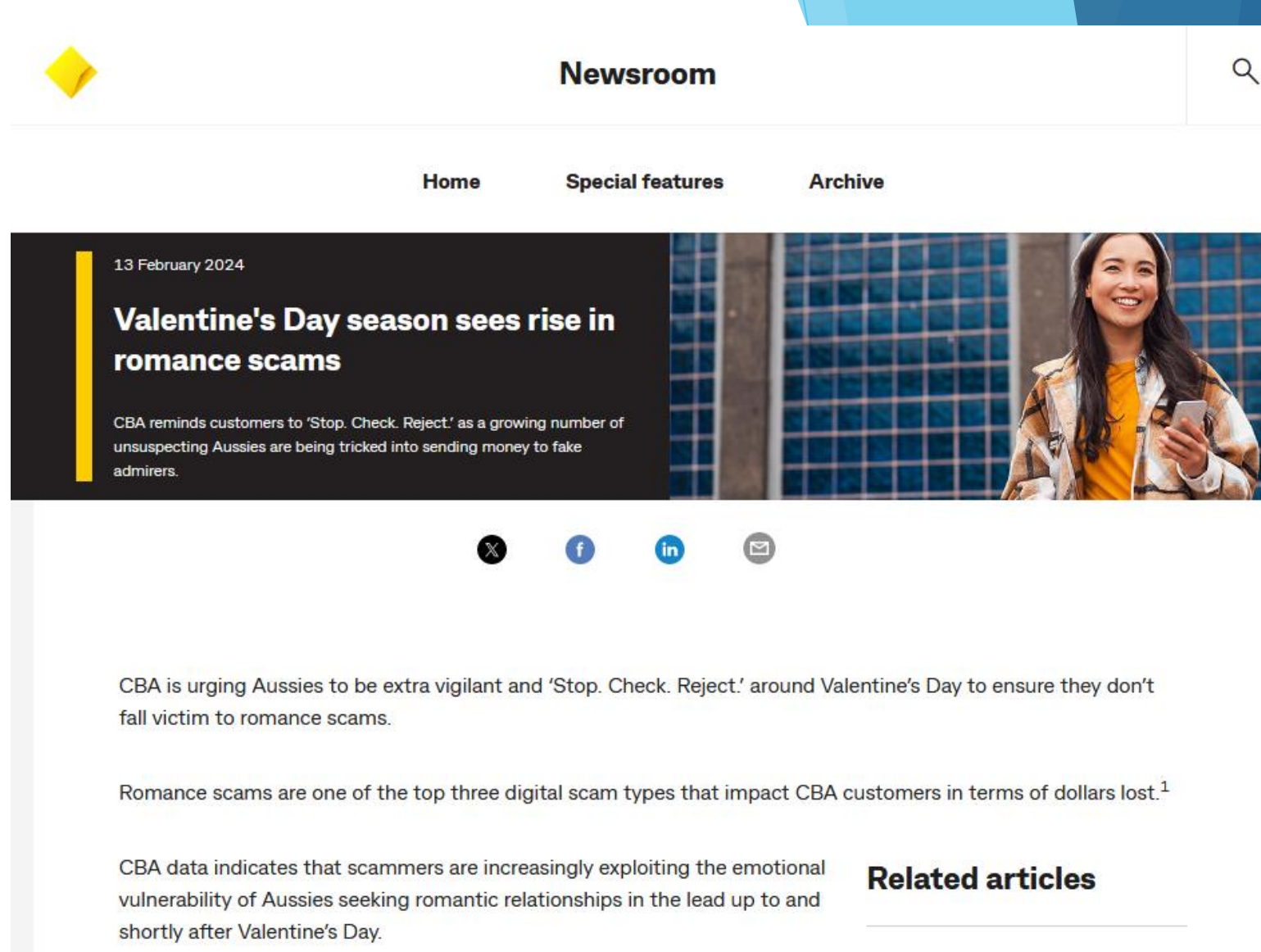
- ▶ Impersonating friends, family, others - “friend” requests.
- ▶ Investment “opportunities”
 - ▶ Often link to an official looking site, e.g. a fake newspaper or other endorsement
 - ▶ Starting to use DeepFakes (e.g. Vid of Warren Buffet endorsing bitcoin - April 2024)
- ▶ Offers to help you get your money back from a scam, that is itself a scam.
- ▶ Travel / holiday / time-share offers.
- ▶ Claims of hardship / GoFund-me abuse.
- ▶ Romance scams, especially via Messenger and SMS.
- ▶ **Misinformation:** especially medical & political.

Romance Scams

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

They often use Dating Websites and social media like FaceBook.

Mark Dixon grants a Creative Commons Attribution-ShareAlike licence on this material



Newsroom

Home Special features Archive

13 February 2024

Valentine's Day season sees rise in romance scams

CBA reminds customers to 'Stop. Check. Reject.' as a growing number of unsuspecting Aussies are being tricked into sending money to fake admirers.

CBA is urging Aussies to be extra vigilant and 'Stop. Check. Reject.' around Valentine's Day to ensure they don't fall victim to romance scams.

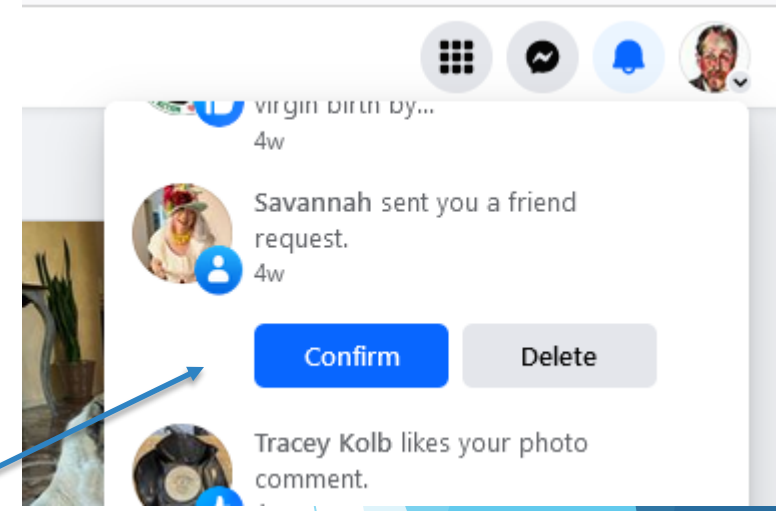
Romance scams are one of the top three digital scam types that impact CBA customers in terms of dollars lost.¹

CBA data indicates that scammers are increasingly exploiting the emotional vulnerability of Aussies seeking romantic relationships in the lead up to and shortly after Valentine's Day.

Related articles

<https://www.commbank.com.au/articles/newsroom/2024/02/romance-scams-around-valentines-day.html>

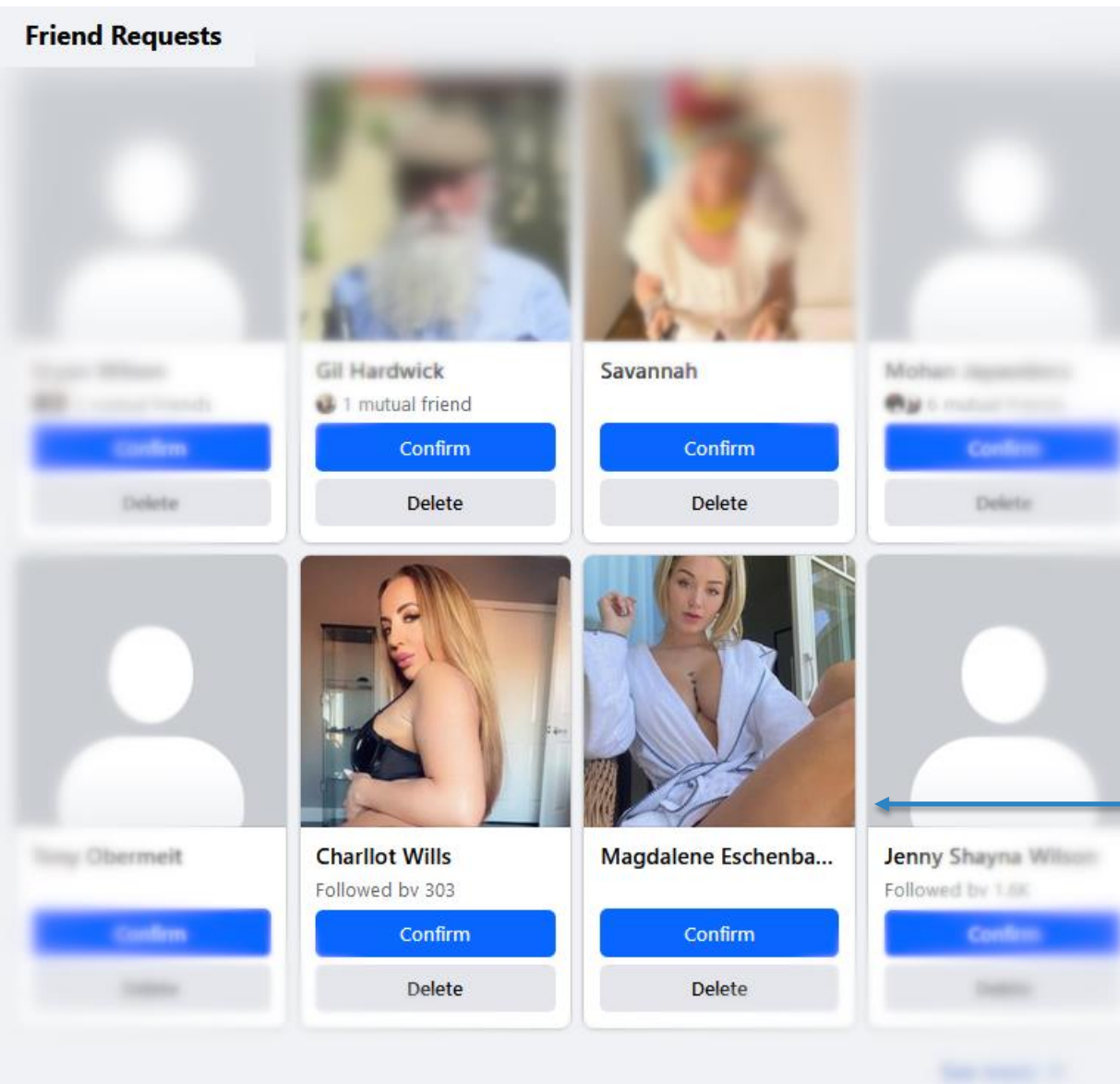
Facebook Scams



“Friend Request” from someone who is already a FaceBook Friend - i.e. this is a fake of an actual friend, who will try to scam me if I accept this duplicate request.

“Friend Requests” from people I have not met. Likely to turn into a Romance Scam if I accept. Romance Scams target both men and women.

These came to me, my wife says those targeted at her looked like successful business or military men.



What is a deepfake?

**Warren Buffett decided to
whiten his reputation by
just giving money away at
the end of his life...**



**May sounds fun, but don't
lose the f*cking
opportunity!
ENJOYER**

<https://cloudfront.mediamatters.org/static/D8Video/2023/12/04/warren-buffett-deepfake.mp4>

“pwned” or “poned”
is geek-speak for
“owned” or
compromised.

<http://haveibeenpwned.com>

Mark Dixon grants a Creative Commons Attribution-ShareAlike licence on this material

The screenshot shows the homepage of the website 'Have I Been Pwned'. The browser address bar shows the URL 'https://haveibeenpwned.com'. The navigation menu includes 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main heading is 'Have I been pwned?' with a subtext 'Check if your email address is in a data breach'. A search input field contains the email address 'mdixon@dixemail.com' and a 'pwned?' button. Below the search, a red banner displays the message 'Oh no — pwned!' and 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. There are social media icons and a 'Donate' button. The section 'Breaches you were pwned in' lists a breach by 'epik' with a detailed description: 'In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.' The compromised data includes 'Email addresses, Names, Phone numbers, Physical addresses, Purchases'. At the bottom, statistics are shown: 777 pwned websites, 13,517,282,665 pwned accounts, 115,770 pastes, and 228,884,645 paste accounts. The footer includes 'Largest breaches' and 'Recently added breaches'.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



› Learn about our methodology at hivesystems.io/password

Common password mistakes

- ▶ Using dictionary words.
- ▶ Replacing letters with digits and symbols. This technique is well known to hackers so swapping an “E” for a “3” or a “5” for a “\$” doesn’t make you much more secure.
- ▶ That meeting the minimum requirements for a password makes it strong. By today’s standards, an 8-character password won’t make you very secure.
- ▶ Using the same password a lot as long as it’s strong - what if the website is hacked? Do you know how the website stores your password? With your name, address, DoB and credit-card?
- ▶ Storing written copies of your password near your computer, or in a spreadsheet - what if your computer is stolen along with everything on/in your desk? Cliché: on a post-it note under the keyboard.
- ▶ Consider a password manager (e.g. LogMeOnce) with a (long) PassPhrase - or use acronyms of (unique) long phrases as passwords.

Climbing Mount Everest takes my breath away literally and figuratively ▶ CMEtmbalaf (10 characters)
Common security practices are good for online safety and peace of mind ▶ Cspagfosap\$69 (add a symbol & favourite number)

<https://www.passwordmonster.com/>

“TestPassword#1”

Upper, lower, number, special character, long (14 characters)

Yet it is still weak and would not take long to crack by a hacker with the right software.

Mark Dixon grants a Creative Commons Attribution-ShareAlike licence on this material



The screenshot shows a web browser window with the URL <https://www.passwordmonster.com>. The page title is "PasswordMonster" and the contact email is info@passwordmonster.com. The main heading is "How Secure is Your Password?". Below this, there is a section titled "Take the Password Test" with a tip: "When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end". A checkbox for "Show password:" is checked. The password "TestPassword#1" is entered in a red-bordered box, and the result is "Very Weak". Below the password box, it says "14 characters containing: Lower case Upper case Numbers Symbols". The time to crack the password is listed as "2.58 seconds". A review section states: "Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains 2 common passwords and a dictionary word." At the bottom, there is a footer: "Your passwords are never stored. Even if they were, we have no idea who you are!". A blue banner at the bottom contains the text: "Do you want to find out more about password best practices, cyber risks, and the most common mistake people do when creating password?" with a button labeled "Scroll to Find More".

General tips:

- ▶ **Verify Independently**: Contact official organizations through their known websites or phone numbers, **never** through links or numbers given in email or SMS.
- ▶ **Slow Down**: Scammers rely on urgency to stop victims from thinking critically.
- ▶ **Never share financial details** or passwords over unsolicited calls, emails, or texts. DO NOT FOLLOW DIRECTIONS ON YOUR COMPUTER FROM THEM.
- ▶ **Use a different password for each** bank, broker, email service, and shopping.
- ▶ **Keep Software Updated**: Updates often contain patches for security vulnerabilities that scammers exploit. Windows, and Android are fairly proactive about that, if you let them.
- ▶ **Be Sceptical**: If something sounds too good to be true, it likely is.
- ▶ **Report Scams**: Help authorities track scammers by reporting any scam attempts. In Australia, you can use Scamwatch: <https://www.scamwatch.gov.au/>