



Could you get scammed? ... online safety

Mark Dixon

for ASA, May 2025

Hackers struck customers

Brute force attack

Paul Smith

The cyberattack that has robbed an unknown number of Australians of hundreds of thousands of dollars from their superannuation accounts began about a month ago, when the criminals tried to access millions of individual accounts armed with credentials that would let them in to a small percentage of them.

The attempts happened mostly in the dead of night, and relied on a subset of a branch of cyberattacks called brute force attacks, which is known as credential stuffing.

No official cause for the success of the co-ordinated attack against major industry funds Australian Retirement Trust, AustralianSuper, REST and Hostplus has been revealed yet, but well-placed sources, who spoke on the condition of anonymity to speak freely, said they are not hunting for some previously undiscovered technology trickery.

Rather the attacks are the highest profile example yet of nobody listening

to the countless warnings we all hear, about not using the same password across multiple accounts. They are also an example of superannuation funds seemingly failing to have rudimentary procedures in place.

Credential stuffing is where cybercriminals use account usernames and passwords stolen in a data breach and try them on the login systems of different organisations. It works because people use the same password across multiple accounts, and often ignore emails from organisations such as the affected super funds.

The identity or location of the hackers is not known yet, but they knew the way Australian super funds manage their accounts, and when most of us are asleep. Armed with credentials that were probably bought in bulk on the dark web, the hackers used automated systems to try to log into the websites of the different funds. When they got in they sought to change details in the accounts, such as mobile phone numbers, which are used to verify online transactions via an SMS.

The customers would have received

How the *Financial Review* broke the story



an email asking them to confirm that they meant to change their phone numbers, but the hackers acted in the middle of the night, safe in the knowledge that plenty of people ignore most of the many emails that clog their inboxes when they're awake.

It seems that if that double-check email is ignored for long enough then the phone number change went

Are you vulnerable?

AFR, 07 Apr 2025
Cybercriminals mimicked super chiefs

“Cybercriminals impersonated superannuation executives in a sophisticated mail scam that rocked the industry’s top organisations in the same week hackers compromised the largest retirement savings fund managers and siphoned money out of member accounts.”



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.

What will we cover today

- ▶ Email scams, SMS scams, phone scams
- ▶ Social media scams (e.g. on FaceBook)
- ▶ Broker scams (unsolicited offers that sound great)

- ▶ Password ideas
- ▶ Pwned? - <https://haveibeenpwned.com/>

- ▶ Questions and (*short*) comments welcome during presentation



Jargon alert! What are we talking about?

- ▶ **Phishing** (fishing) - emails and other offers fishing for victims.
- ▶ **Spear-phishing** - very targeted fishing, aimed specifically at You!
- ▶ **Advance Fee** - fantastic offers that require a “small” payment from you first.
- ▶ **Identity theft** - getting enough of your personal details to pretend to be you.
- ▶ **Hacking** - can mean just programming, here it means infiltrating your computer.



Send	From ▾	mdofperth@outlook.com
	To	mdixon@dixemail.com
	Cc	
Subject		URGENT - confirm details to prevent fraud

Incoming email?

What do I do with this?



Dear Sir/Madam

Our security department has evidence that your bank account has been targeted for fraud.

Please login via this link <http://commbank.com.au/>, enter your login id and password, to ensure you still have access to your account.

We apologize for any inconvenience this security measure may have caused.

Sincerely, CommonwealthBank

© 2024 Commonwealth Bank of Australia ABN 48 123 123 124 AFSL and Australian credit licence 234945

----- Original Message -----

From: ATO myGov
"myGov - team" <support@govinfo.com>

Sent: Sun 2 October 2022 16.23.38 - 0500

Subject: You have a pending payments by medicare funds transfer



This is a message from the Mygov team

With the new improved **Medicare** updated service you can now receive your **Medicare** payment for benefits and claims promptly and directly into your bank account.

Please Kindly update your Electronic Funds Transfer (EFT) payment with **Medicare** by signing into your [myGov](#) account and updating your **Medicare** account to start receiving prompt medicare payments for benefits and claims.

Regards,
myGov team

1 New myGov Notification

Delete Archive Report Reply Zoom

1 New myGov Notification

(A-T-O)-Notification<al_iquammauris.40@icloud.com>
To: mdofperth@outlook.com.
Tue 23-Apr-24 10:00 AM

You have a new message in your inbox

[Click](#) to view

Regards, myGov team.

Reply Forward

Two recent examples
in my InBox

1 New Secure Message

Delete Archive Report Reply Zoom Read / Unread Categorize Flag / Unflag Print

1 New Secure Message

Flag for follow up.

AO Australian Taxation Office (ATO)<nduminminimstet.8@icloud.com>
To: mdofperth@outlook.com.
Fri 17-May-24 10:39 AM

A new secure message regarding your MyGov

To review please

[Read Message](#)

Thanks.

The ATO Account Team.

Reply Forward

Email - warning signs

Contains a link, or attachment, or “click here” that asks you to log on to an online service with your username and password or to provide other personal information.

Requests a payment but the bank account and BSB details are new or have changed since the last payment you made.

Claims to be from a well-known organisation or government agency but is sent from a free webmail address (for example @gmail.com, @yahoo.com.au)

Common scams via email include:

- ▶ asking you to confirm your banking details so they can give you a ‘refund’
- ▶ providing you with a phone number to call urgently
- ▶ making a threat such as immediate arrest, deportation, ...
- ▶ threatening to stop a service or charge a fine if you don’t act
- ▶ **stating you’ve been a victim of identity crime and offering compensation or help to recover money lost to scams. ◀ fooled you twice!**

Send From To Cc Subject URGENT - confirm details to prevent fraud

Is the From:
address credible?



CommonwealthBank

Dear Sir/Madam

Does it ask you to
login/provide
personal info?

Our security department has evidence that your bank account has been targeted for fraud.

HOVER to
Check Link!!!

<http://commbank.com.au/>
Ctrl+Click to follow link

Please login via this link <http://commbank.com.au/>, enter your login id and password, to ensure you still have access to your account.

We apologize for any inconvenience this security measure may have caused.

Sincerely, CommonwealthBank

----- Original Message -----

From: ATO myGov
"myGov - team" <support@govinfo.com>

Is From: address credible?

Sent: Sun 2 October 2022 16:23:38 - 0500

Subject: You have a pending payments by medicare funds transfer

medicare

Does it want you to login?
(Hover to see link)

This is a message from the Mygov team

With the new improved Medicare updated service you can now receive your

Medicare payment for benefits and claims promptly and directly into your bank account.

Please Kindly update your Electronic Funds Transfer (EFT) payment with Medicare by signing into your myGov account and updating your Medicare account to start receiving prompt medicare payments for benefits and claims.

Regards,
myGov team

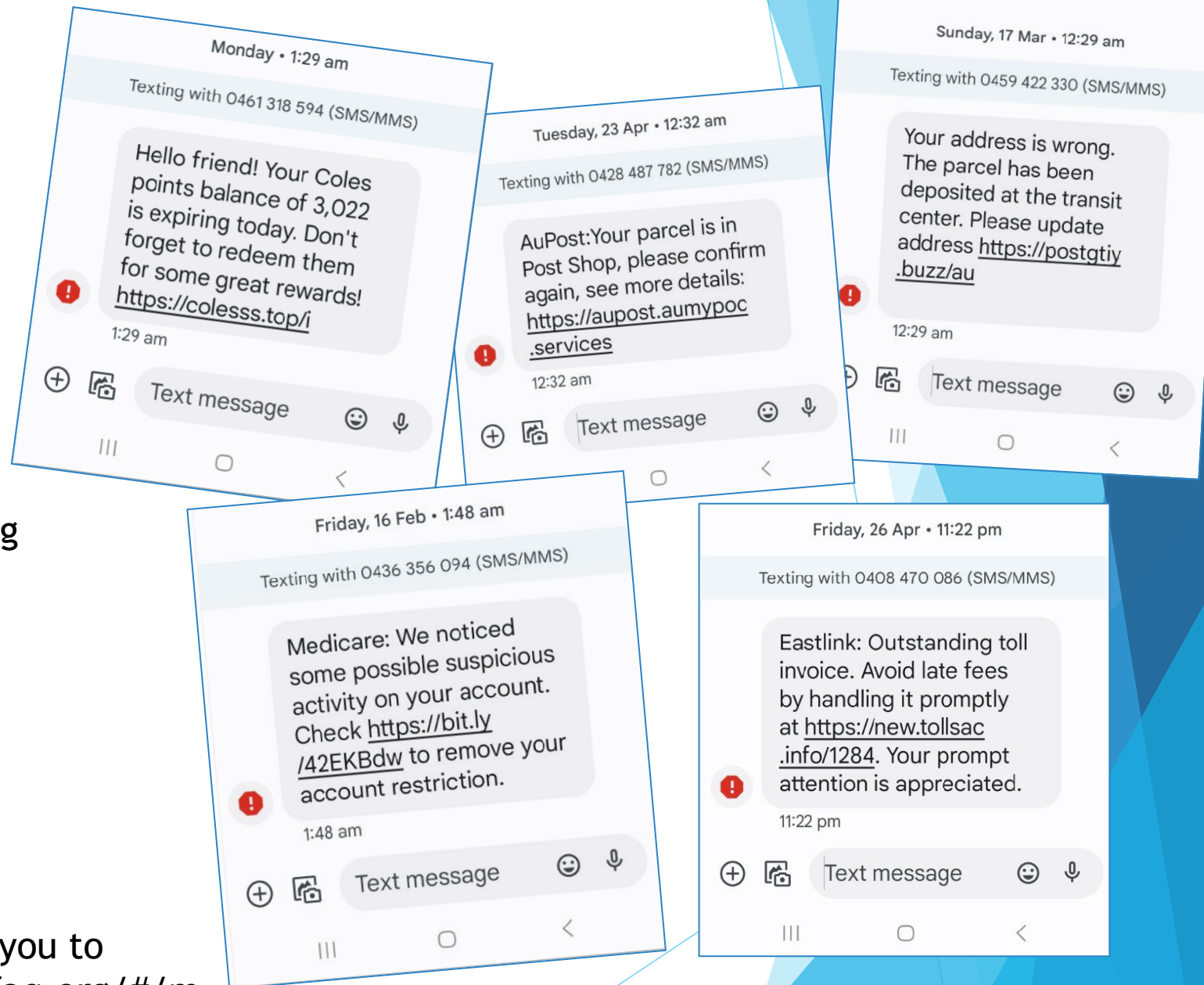
Scam SMS

Pretending to be Australia Post; Medicare, ATO, myGov, Coles, Toll managers.

Sometimes the language is “off” but scams are getting better at producing convincing text.

Fortunately, some phones will filter and flag these.

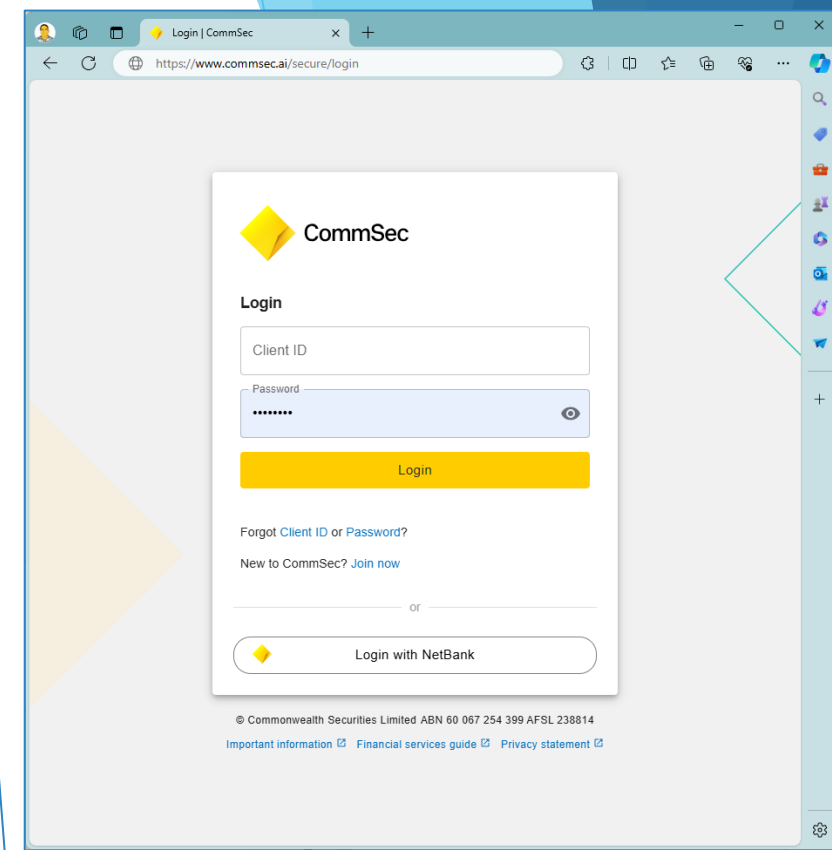
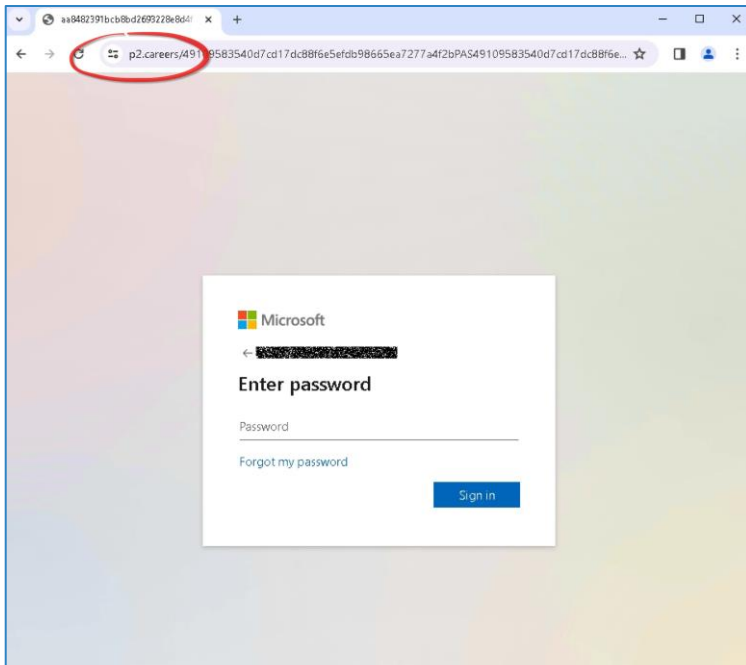
Redirection link: takes you to <https://m.i-medicare-faq.org/#/m>



Those links take you to something that can look authentic.
You can check the link. But it is better to just go to the known address of the valid site instead.

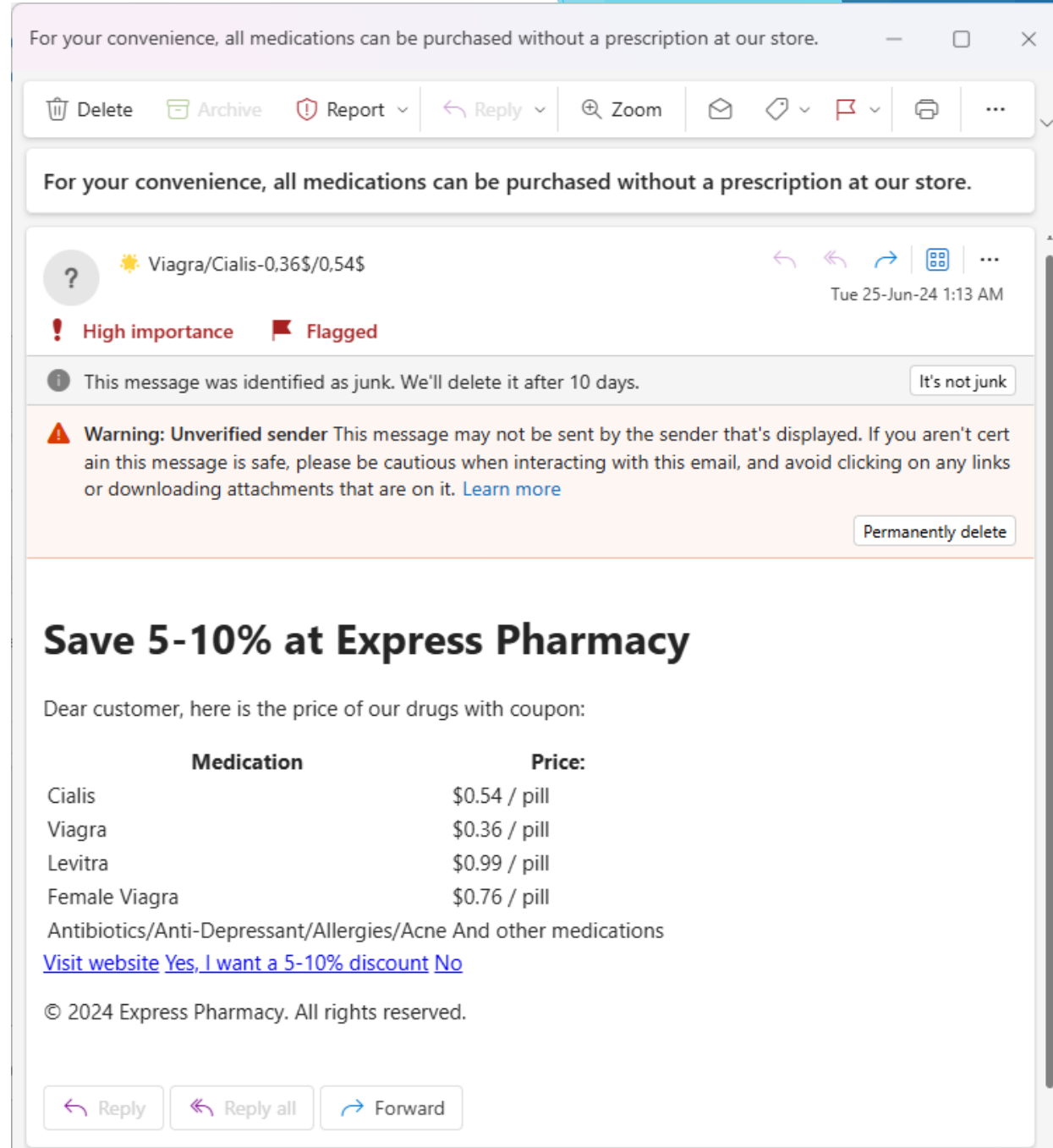
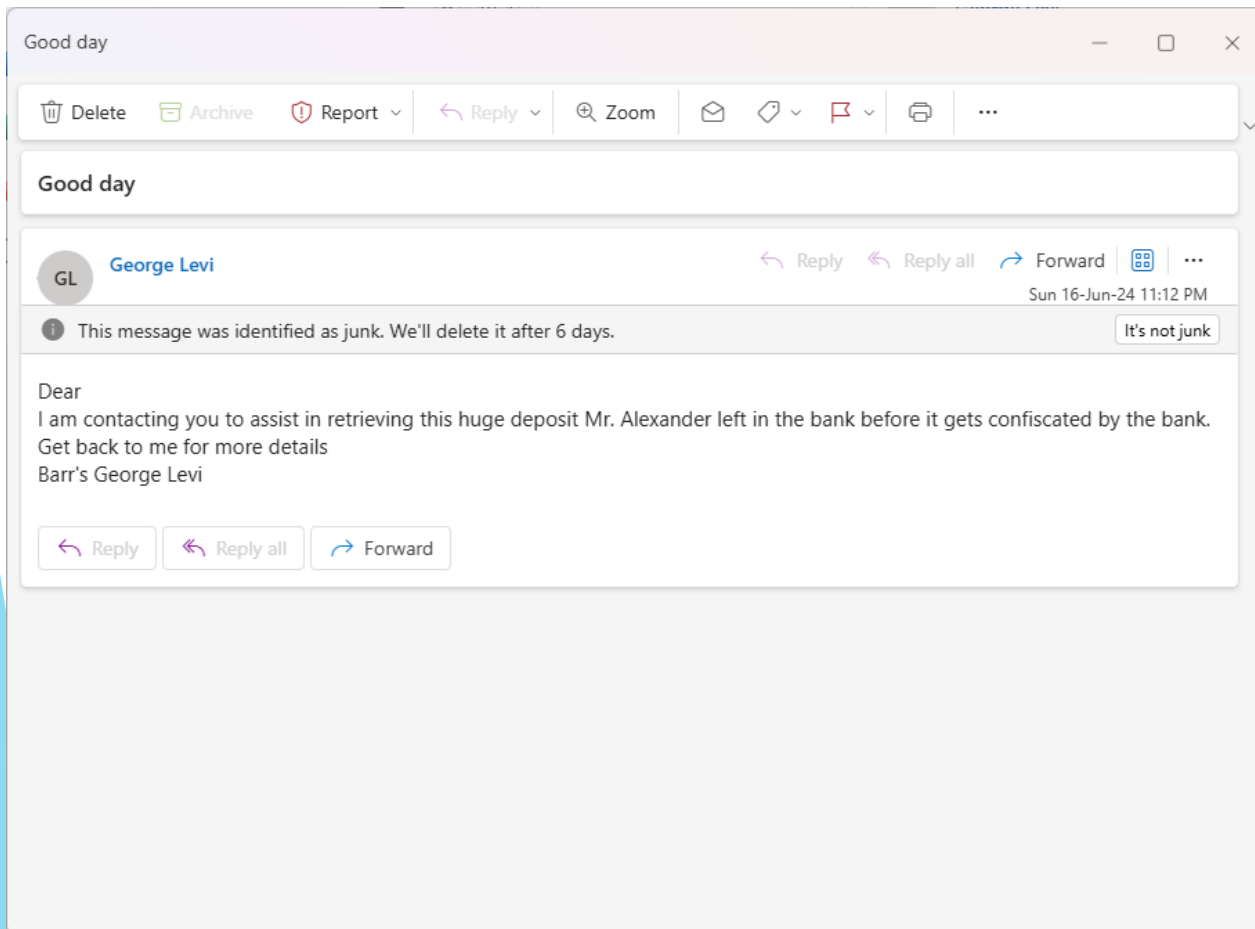
Once you type in your userid and password, it will be in the hands of criminals within seconds, and they can/will clean you out.

And maybe change your pwd too!




Examples of email scams

- some are obvious




email & SMS scams, maybe less obvious

DOCUMENTS

 E_document <dupchak@fastmail.fm>(E_document via re)
To



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

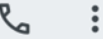
has been attached to this e-mail: mdofperth@outlook.com

 Reply

 Forward

5:40  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?IHytXd4NSPZXP>
Share our photos and lives. Get to know each other.

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



Text message



Save +61424119619? Saving this number will add a new contact

Report spam Add contact

8:41 am

Texting with 0424 119 619 (SMS/MMS)

Unread

Hi dad. I've managed to drop my phone in the toilet now it's not registering my old SIM, This will be my number for now.

8:41 am

Okay Good Okay, good Great!

Text message

SMS claiming to be family on new phone.



Remote access scam:

- ▶ **Legend of the Vampire** - in order to enter a home, they have to be invited. Once in, you can't make them leave.
- ▶ If you get a **phone call** saying there is something wrong with your computer or your internet, the caller will ask you to open a program that gives them access (e.g TeamViewer, GoToAssist, LogMeIn, ...).
- ▶ Once they are in they can:
 - ▶ Use your computer as if they were you, especially if you save passwords for your bank, etc. in your browser. They can also blank it so you can't see what they are doing.
 - ▶ They will often install a “**key-logger**” which is a program that runs in the background and sends everything you type, including user-ids and passwords, to the criminals. This **keeps running even after the remote access**. These are very hard to exorcise!



Remote access scam:

THIS WILL ALSO HAPPEN IF YOU DOWNLOAD SOFTWARE FROM AN UNSAFE SOURCE

Of if you use a service like that to download a key-generator

(e.g. PirateBay or Warez sites).

The download might appear to work but it will also install a key-logger and/or Zombify your PC and/or encrypt & ransom your data.



Remote access scam:

If you fall for either of the above:

1. Power off your computer.
2. Immediately contact your financial service providers (banks, brokers, super-fund) by phone and tell them what happened.
3. Consider using a professional service centre and have them fix it, possibly by re-installing your operating system.

Remote access software is ok ONLY if you have initiated a request to a legitimate IT support service.

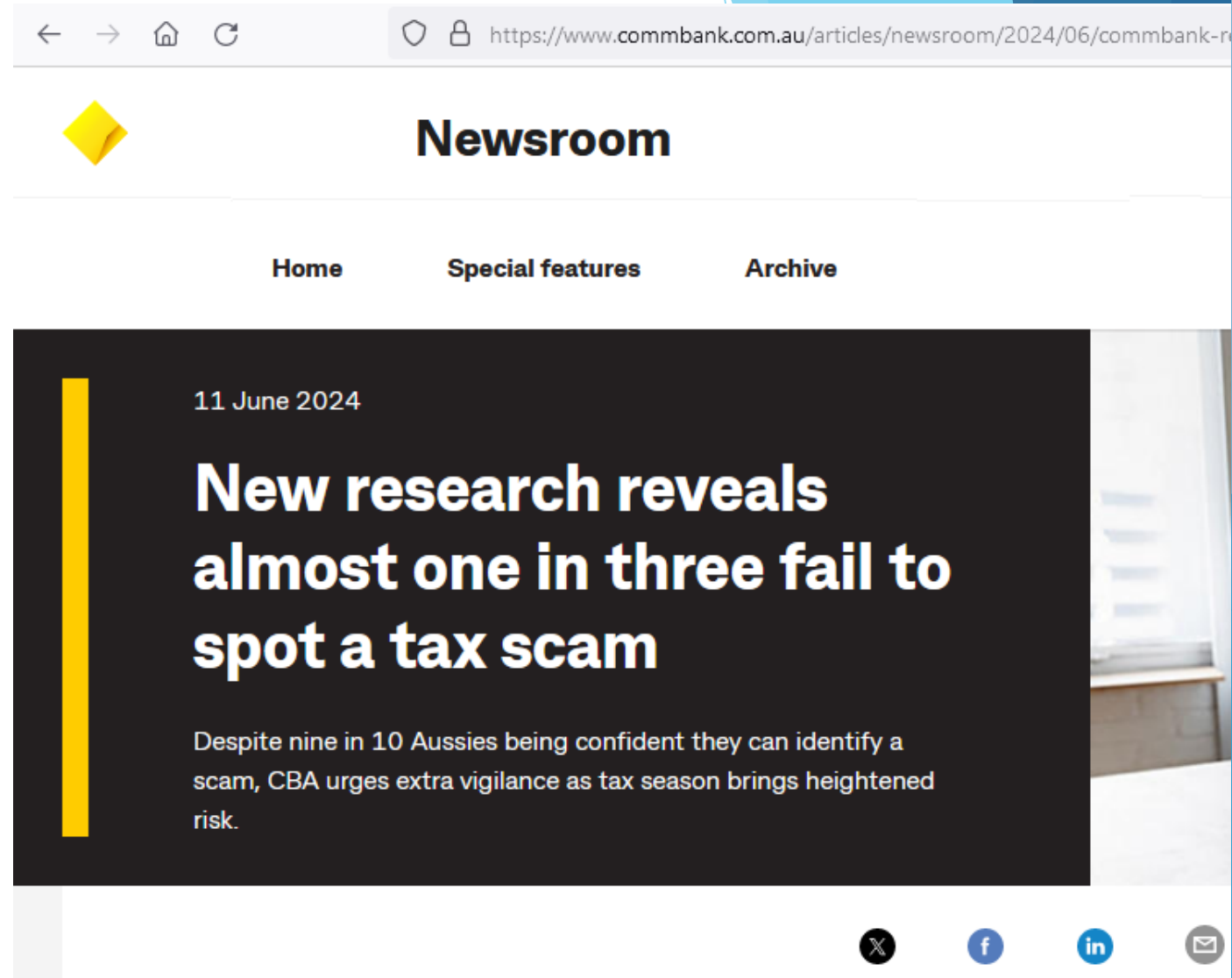


CBA says: Aussie taxpayers need to stay alert during tax season. New research¹ reveals almost a third fail to spot a tax scam. When multiple tax phishing scams were tested with **Australians over the age of 18**, only **69 per cent** could successfully identify all of them.

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.



Social Media scams

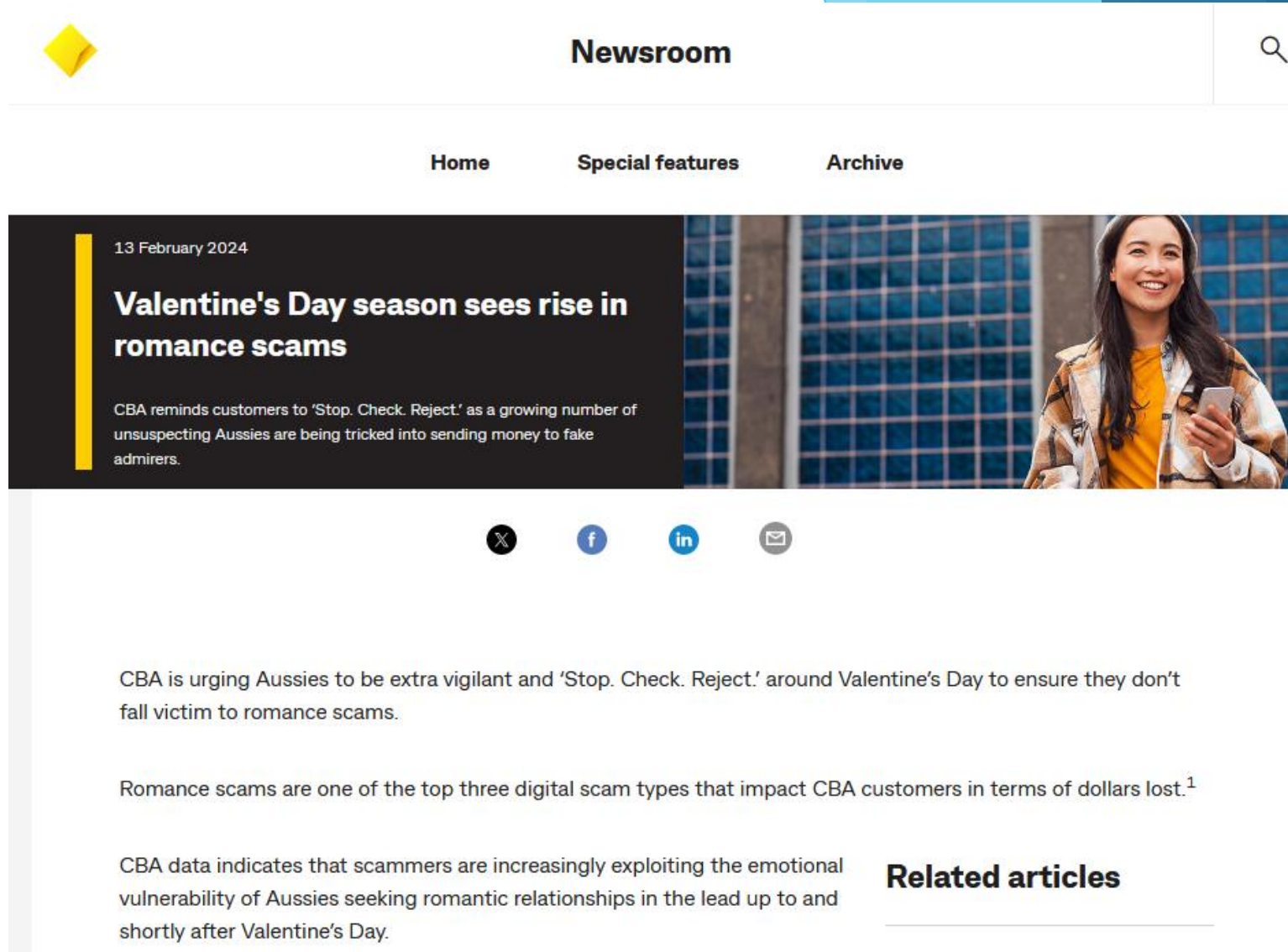
- ▶ Impersonating friends, family, others - “friend” requests.
- ▶ Investment “opportunities”
 - ▶ Often link to an official looking site, e.g. a fake newspaper or other endorsement
 - ▶ Starting to use DeepFakes (e.g. Vid of Warren Buffet endorsing bitcoin - April 2024)
- ▶ Offers to help you get your 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



The screenshot shows a news article from a website. At the top, there is a yellow diamond logo and the word "Newsroom" in a search bar. Below the search bar are navigation links: "Home", "Special features", and "Archive". The article is dated "13 February 2024" and has the title "Valentine's Day season sees rise in romance scams". The sub-headline reads: "CBA reminds customers to 'Stop. Check. Reject.' as a growing number of unsuspecting Aussies are being tricked into sending money to fake admirers." To the right of the text is a photo of a smiling woman with long dark hair, wearing a yellow shirt and a patterned jacket, holding a smartphone. Below the photo are social media sharing icons for X, Facebook, LinkedIn, and Email. The main body of the article contains the following text: "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." and "Romance scams are one of the top three digital scam types that impact CBA customers in terms of dollars lost.¹". At the bottom of the article, it says "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." To the right of this text is a section titled "Related articles" with a horizontal line underneath.

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.

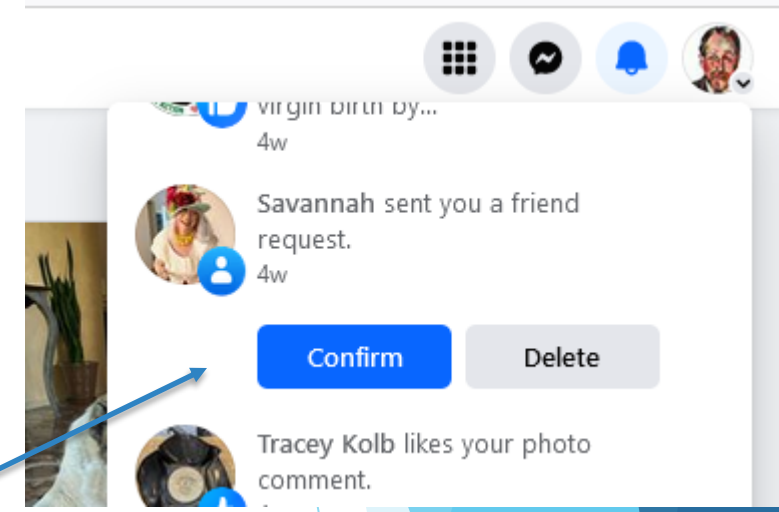
Romance scams are one of the top three digital scam types that impact CBA customers in terms of dollars lost.¹

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>

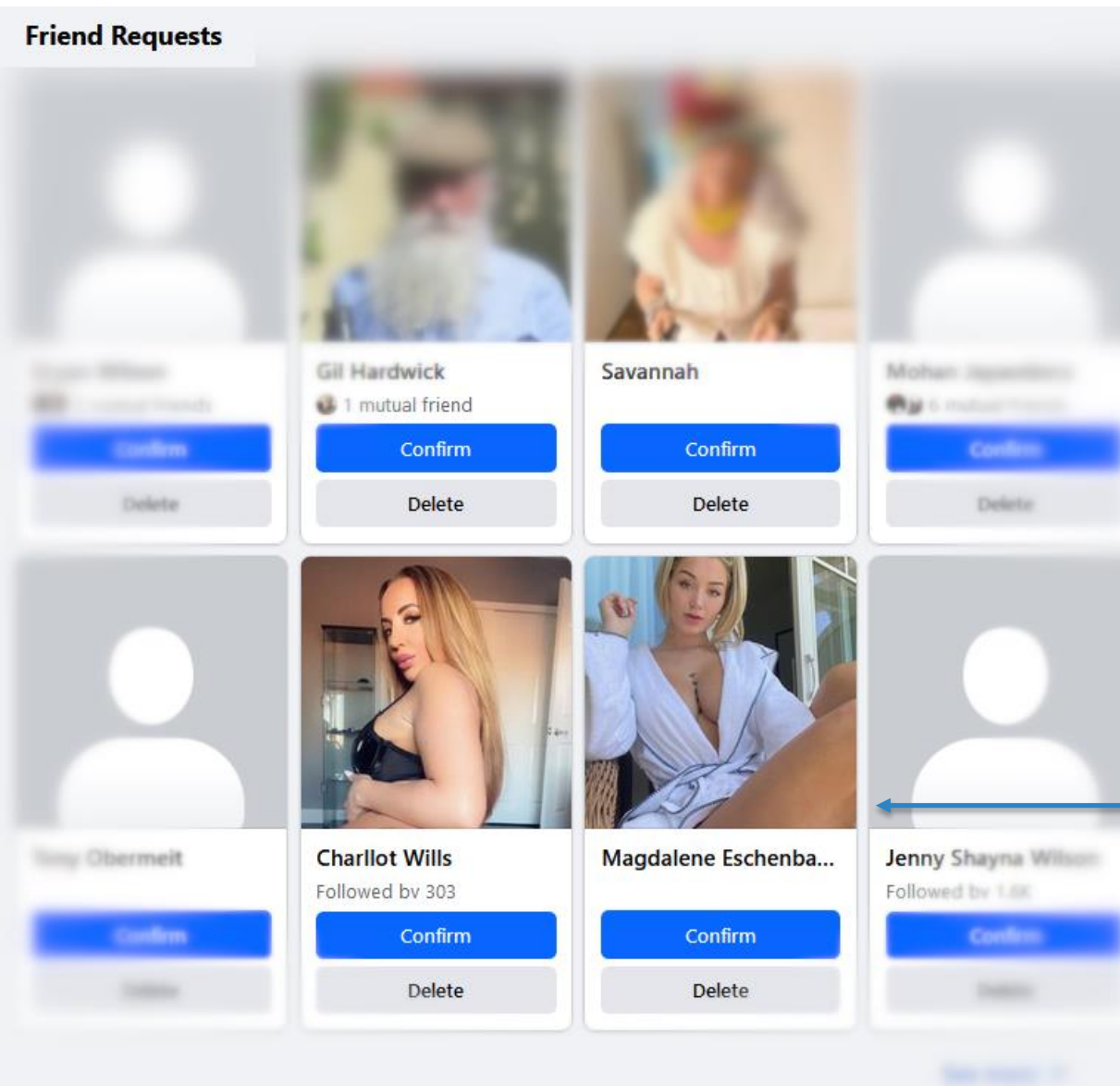
Facebook Scams



“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 'Have I Been Pwned' website interface. At the top, the navigation bar includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'Have I been pwned?' with the subtitle 'Check if your email address is in a data breach'. A search bar contains the email 'mdixon@dixemail.com' and a 'pwned?' button. Below the search bar, a red banner displays the message 'Oh no — pwned!' and states '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' includes a definition of a breach and a list of breaches. The first breach is 'epik', which occurred in September 2021, exposing data for domain registrars and web hosts. The compromised data includes email addresses, names, phone numbers, physical addresses, and 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 lists 'Largest breaches' and 'Recently added breaches'.

Have I Been Pwned: Check if you've been pwned

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email address is in a data breach

mdixon@dixemail.com pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

epik

Epik: 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.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases

777 pwned websites 13,517,282,665 pwned accounts 115,770 pastes 228,884,645 paste accounts

Largest breaches 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

<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 has a blue header with the site name and email. The main heading is "How Secure is Your Password?". Below this, a section titled "Take the Password Test" provides a tip and a "Show password" checkbox. The password "TestPassword#1" is entered and highlighted as "Very Weak" in a red box. A breakdown shows it contains 14 characters: 7 lower case, 4 upper case, 2 numbers, and 1 symbol. It estimates the password can be cracked in 2.58 seconds. A review states the password is very weak due to common words and a dictionary word. A footer note says passwords are not stored. A blue footer bar contains a call to action to find more about password best practices, with a "Scroll to Find More" button.

Have I Been Pwned: Check if yo X PM Password Strength Meter

https://www.passwordmonster.com

PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

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 Show password: ☒

TestPassword#1

Very Weak

14 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
2.58 seconds

Review: 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.

Your passwords are never stored. Even if they were, we have no idea who you are!

Do you want to find out more about **password best practices**, **cyber risks**, and the most **common mistake** people do when creating **password**?

[Scroll to Find More](#)

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 one 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)



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/>