



Could you get scammed?

Mark Dixon

for ASA, 4th June 2024



What are the most common scams in 2024?

- ▶ Email scams - very common
- ▶ SMS scams - very common
- ▶ Phone - very common
- ▶ Social media scams - very common
- ▶ Foot-shooting by downloading dodgy stuff
- ▶ Hacking - less common, except ... if you use the same password in many places.

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



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



CommonwealthBank

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

Incoming email?

What do I do with this?

----- 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 servise you can now receive your

Medicare payment for benefits and claims proptly 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.

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, or blackmail
- ▶ 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.**

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>

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

Subject: You have a pending payments by medicare funds transfer

The Medicare logo consists of the word "medicare" in a bold, yellow, sans-serif font, set against a dark green rectangular background with rounded corners.

This is a message from the Mygov team

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

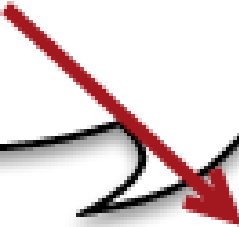
Medicare payment for benefits and claims proptly and directly into your bank account.

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



Is From: address credible?



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

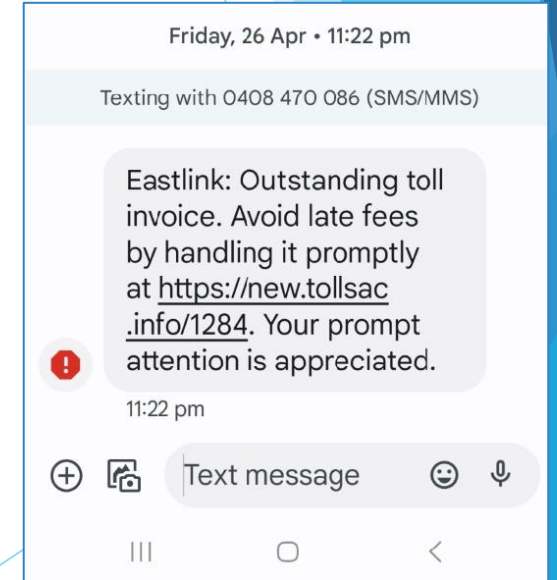
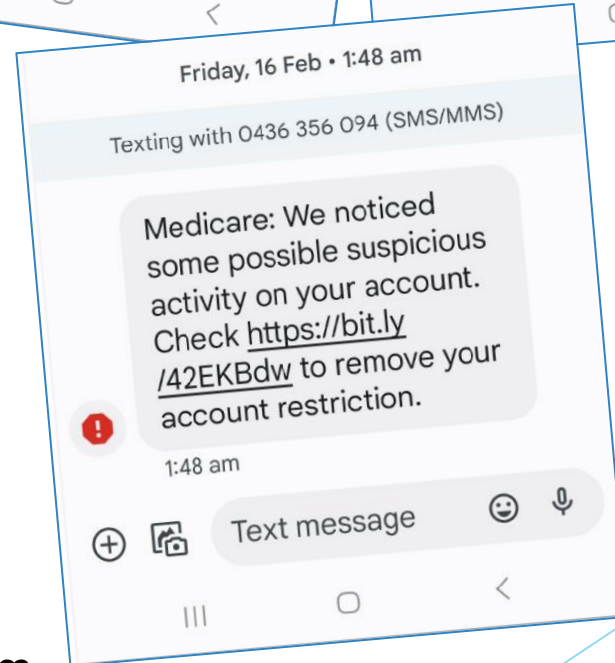
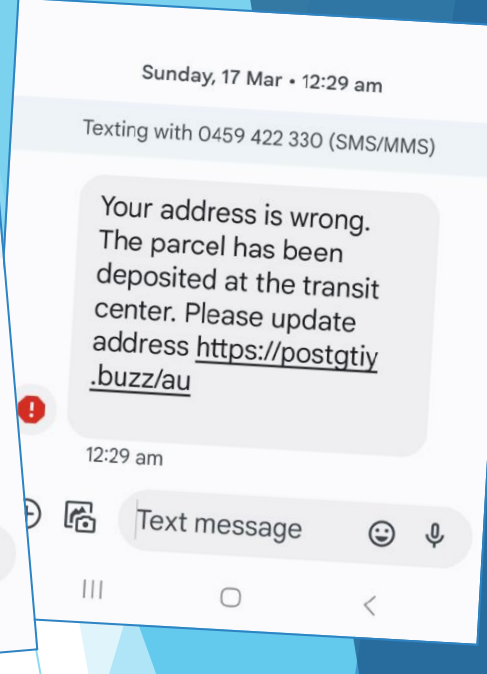
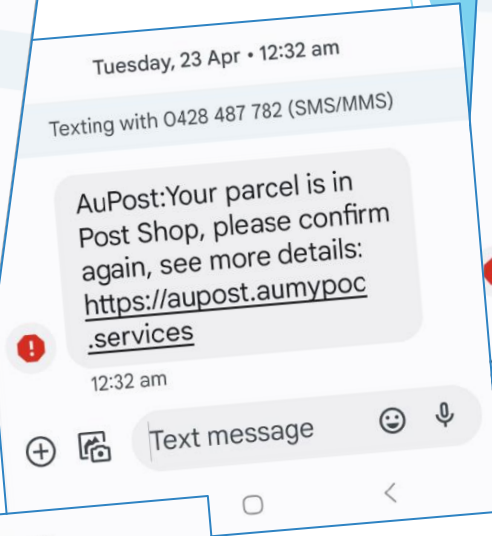
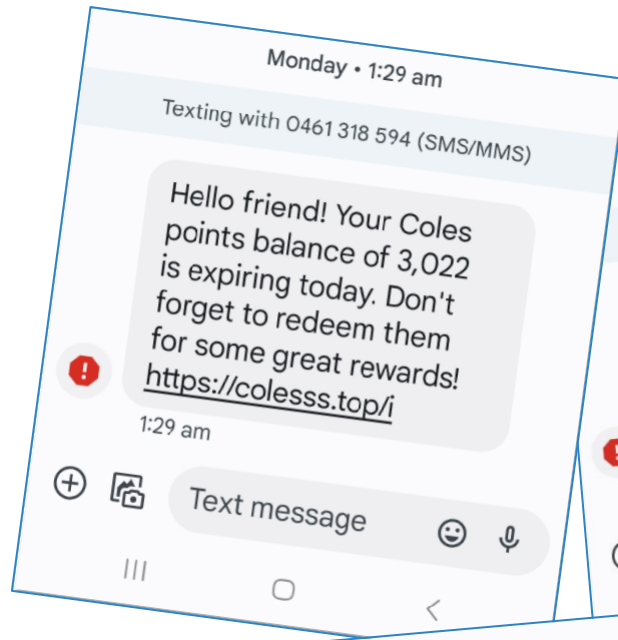
Scam SMS

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.

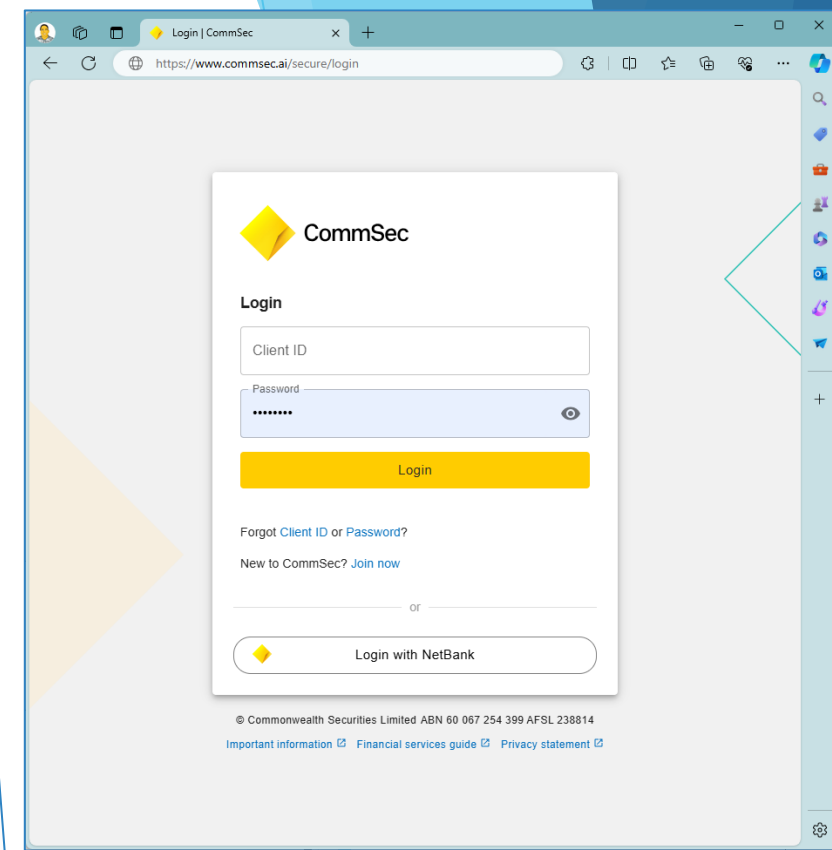
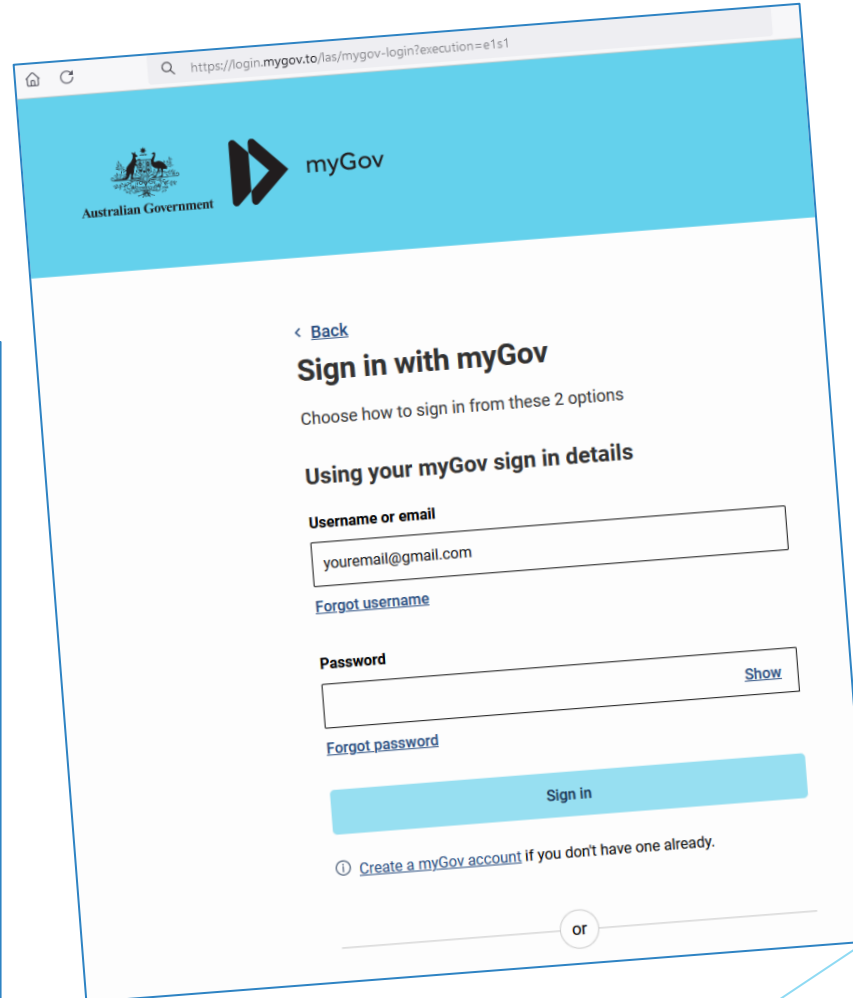
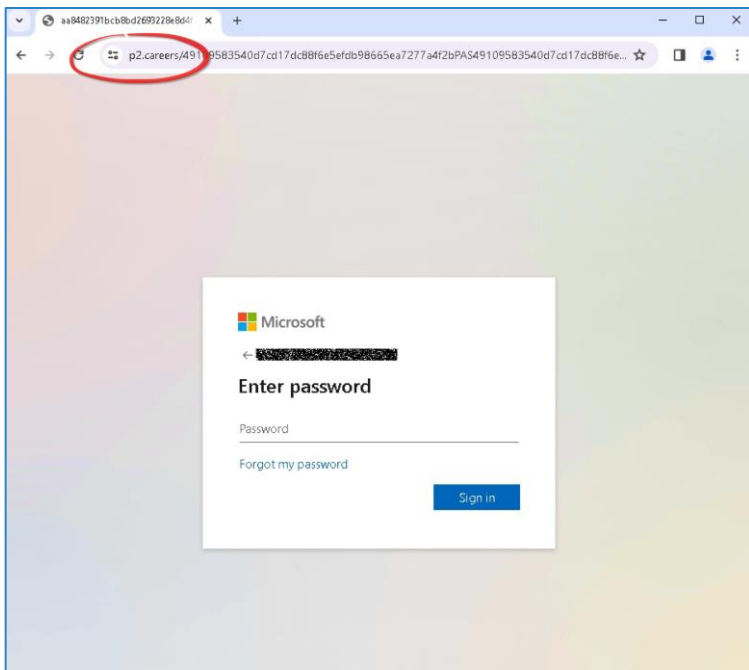
Redirection link: takes you to <https://m.i-medicare-faq.org/#/m>



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!



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 it 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 if you have initiated a request to a legitimate IT support service.



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.
- ▶ **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/>

