

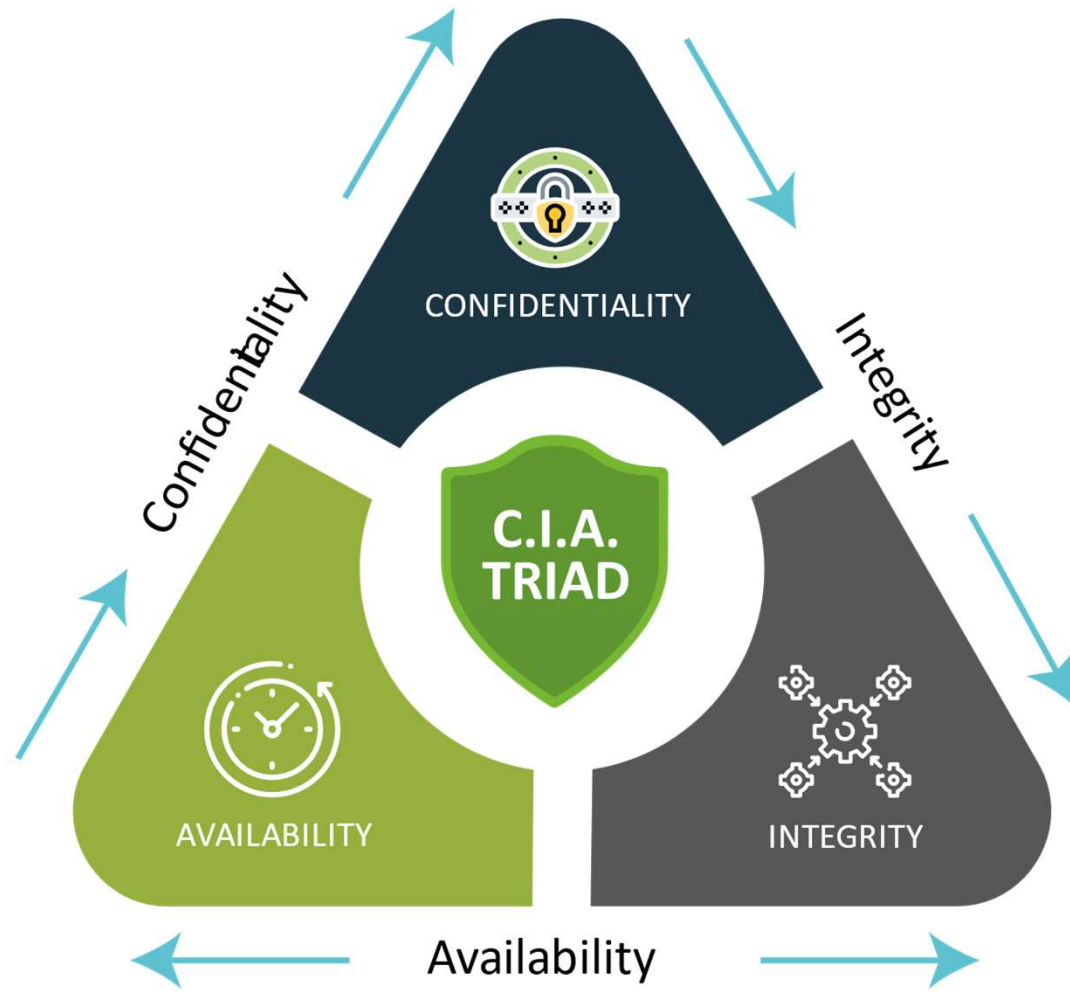
Security Awareness Training



Edition - March 2023

Can you find the
the **mistake**?

<https://www.instagram.com>



This Security Awareness Covers The Following Topics

- *What is phishing vs spear phishing*
- *What is smishing, vishing and QR Code phishing*
- *What is Google Search Phishing*
- *Examples of phishing scams including a screenshot*
- *Social Media Scams and how to identify fake accounts*
- *How to protect yourself from phishing attacks*
- *How to create and manage strong passwords*
- *What is Multi-Factor Authentication and which to use*
- *How to avoid getting hacked on public Wi-Fi*
- *What is Ransomware and how to avoid it*
- *How to use USB Safely*
- *What is CEO Fraud and how to avoid it*



Social Engineering

Is about

Distraction and *Misdirection*



Phishing

When Scammers **fool you** to think they are someone you trust in order to make you **do something**.



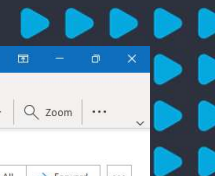
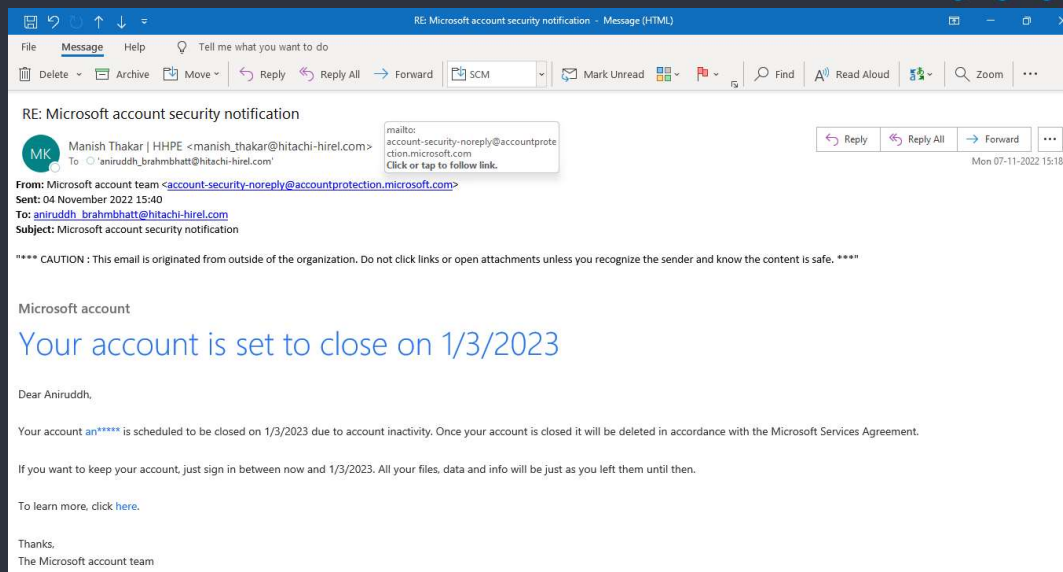


7 **Types** of Phishing Scams You **Should Know About**



Email Phishing Scams

It may look like an email from your bank, Paypal, Google, Amazon, or even your CEO. Or even you IT Administrator



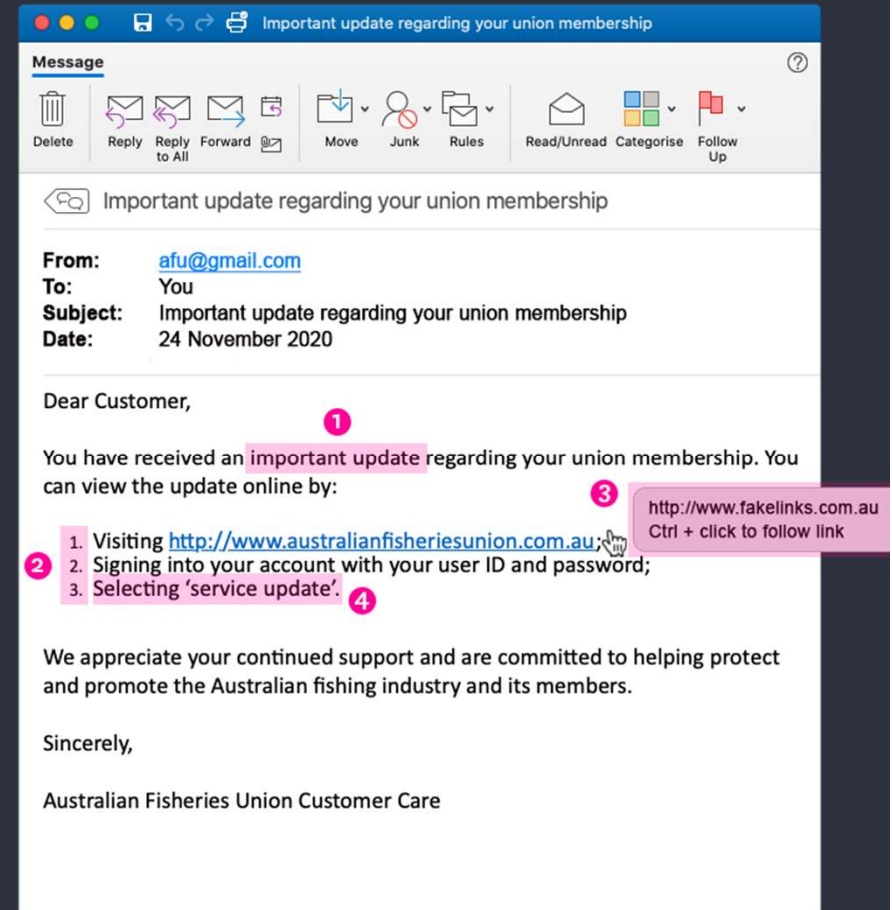
Email Phishing Scams

(1) Check the Email Actually sent from the address

(2) Check for the wording and normal Email writing pattern and mostly they Will show some urgency to do

(3) Check the Fake Link in the email

(4) Check the Signature at last



Important update regarding your union membership

Message

Delete Reply Reply to All Forward Move Junk Rules Read/Unread Categorise Follow Up

Important update regarding your union membership

From: afu@gmail.com
To: You
Subject: Important update regarding your union membership
Date: 24 November 2020

Dear Customer,

You have received an **important update** regarding your union membership. You can view the update online by:

1. Visiting <http://www.australianfisheriesunion.com.au>;
2. Signing into your account with your user ID and password;
3. Selecting 'service update'.

<http://www.fakelinks.com.au>
Ctrl + click to follow link

We appreciate your continued support and are committed to helping protect and promote the Australian fishing industry and its members.

Sincerely,

Australian Fisheries Union Customer Care

Spear Phishing Scams

1 Account payroll question External Inbox x

2 Ann Carlisle <homeofficeinternal19@gmail.com> Fri, May 27, 3:31 PM (3 days ago) ☆ ↶ ⋮
to me ▾

3 Hello April,

4 Please I would like to change the account on my payroll to a new account. Would it be effective next payday?
Thanks.

5 Ann Carlisle
Customer Success Specialist

1 Subject line: Sense of familiarity

2 Sender Name & Email: Sender Name is trusted name in Contacts. Email is generic Gmail instead of company email.

3 Greeting: Personalized

4 Message: Starts a conversation to build trust before a phishing link is sent or action is requested.

5 Correct Job Title Contact name has correct job title. Spearphish attackers do their homework to look as legit as possible.

This is when they target you specifically. They have researched you, they know your family members, where you work, and who is your boss. The chances of fooling you are higher.



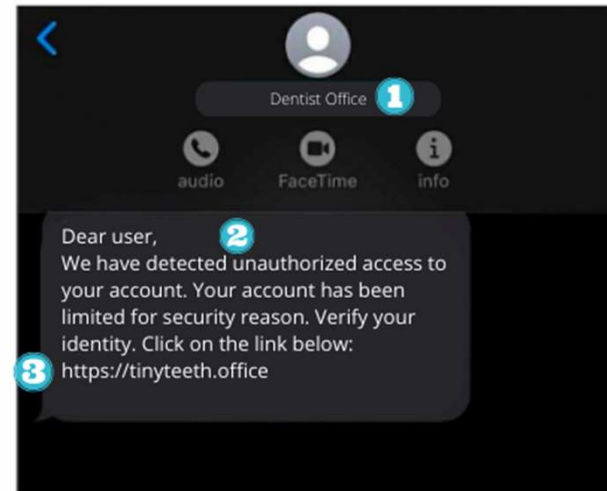
Smishing

Scams

These are text message phishing scams. Criminals know people respond to text and instant messages faster than email.



 **TINY TEETH
CHILDREN'S DENTISTRY**
tinyteeth.com



- 1 Lookalike Contacts**
Generic Contact Name is similar to Trusted Contact role.
- 2 Message**
Message conveys sense of urgency and fear.
- 3 Lookalike URL**
Scammers buy lookalike domains similar to, but different from, the real company site.



Google Search Scams

You may be surprised, but some of the top search results in Google are phishing links.

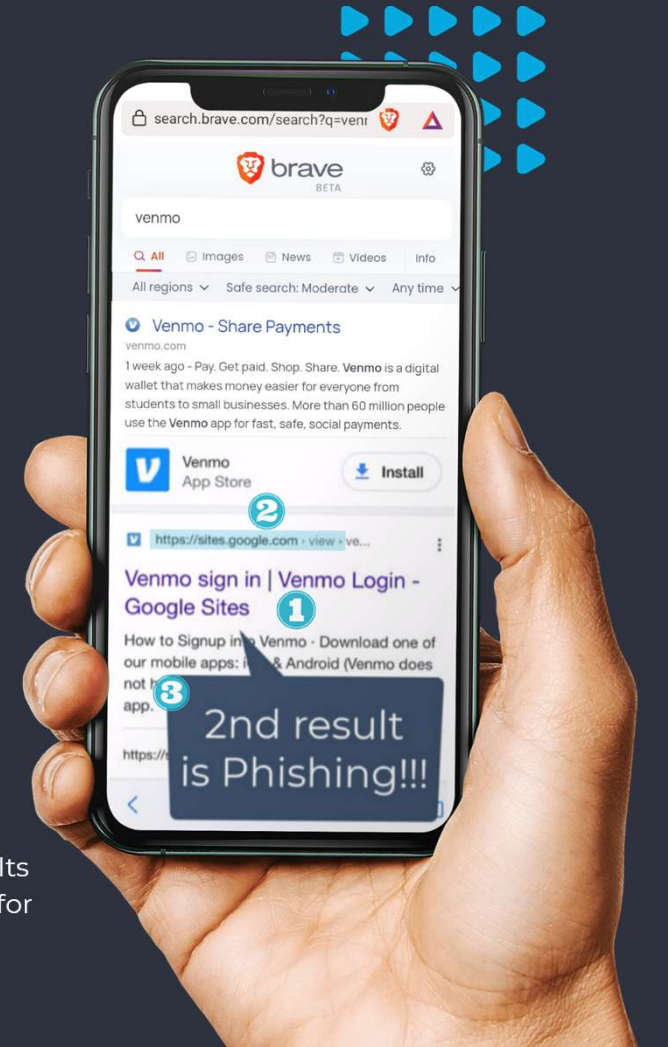
Scammers also invest in search engine optimization and work hard to rank their scam sites in the top search results.



1 Search Result Shows Brand
Title displays correct brand name

2 URL Mismatch
Title says Venmo but URL is a generic sites.google.com

3 2nd Result for Organic Search
Even top search results can be manipulated for fake sites



Social Media Scams

Social media is full of fake accounts. It could also be a fake account with the same name and photo as one of your real friends that will later try to scam you.



The screenshot displays the Instagram 'Requests' section and two message conversations. In the 'Requests' section, two requests are shown: one from 'Roger H. Poast' and another from 'Susan Beck', both with the text 'How are you doing - 5w' and '7w' respectively. A blue circle with the number '1' is placed over the 'Roger H. Poast' request. The first message conversation is with 'Susan Beck' (susan_beck), showing a 'Hello' message and a reply 'How are you doing'. A blue circle with the number '2' is placed over the text 'You don't follow each other on Instagram'. The second message conversation is with 'Roger H. Poast' (roger_h_poast), showing a 'Hello' message and a reply 'How are you doing'. A blue circle with the number '3' is placed over the text 'You don't follow each other on Instagram'.

- 1 Known Contacts**
Friend requests from people already connected with you.
- 2 Inactive Following**
Zero or low followers is a flag especially if you know these people have been active a long time.
- 3 Odd Characters in Handle**
Both use name of the Contact with minor variation to try and avoid notice '._' or '!.'



QR Code Scams

Who thought a QR code could be dangerous?

They are everywhere, especially in restaurants. Criminals can place their own sticker over the legitimate one. So that when you scan it, you will be redirected to a fake site.


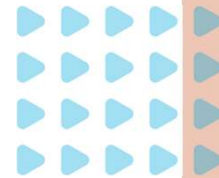


Vishing Scams



Vishing (voice phishing) is a type of phishing attack made over the telephone.

Scammers can spoof a phone number that looks identical to a known number, like your bank.



1 **Trusted Brands**
Numbers for personal and commercial contacts can be spoofed.



What Helps Protect You From Phishing Attacks?

- ▶ If it's urgent, don't let the emotions cloud your judgment
- ▶ Call and verify! - Verify that you are talking to the correct person
- ▶ Check the address - Always check the email address and URL for spelling mistakes
- ▶ Enable Multi-Factor Authentication
- ▶ Look at the style of the message
- ▶ Ask questions



How long will it take to crack your password

7 characters	1 minute
8 characters	1 hour
9 characters	3-4 days
10 characters	7 months
11 characters	40 year
12 characters	2000 years



Passwords include - Lowercase, Uppercase and Numbers



How to create a **strong** Password:

- ▶ Passwords need to be **long!**
- ▶ Use a phrase (**NO** personal info like your name or B-Day)
- ▶ **Don't** reuse passwords!



HOWEVER....

11 BILLION Accounts were stolen from hacked sites and apps.

So even if you have a **STRONG PASSWORD**, it may still not be enough.

You can check if yours was leaked at haveibeenpwned.com



604

pwned websites

11,833,420,729

pwned accounts

114,666

pastes

222,848,990

paste accounts



And That is Why...

... You should enable **Multi-Factor Authentication**

This will help to **protect your account** if your password was stolen or leaked in a data breach.



What type of Multi-Factor Authentication to use?

- ▶ Most common is text based (SMS), but it's the least secure
- ▶ It's better to use authenticator apps like Google or Microsoft Authenticator
- ▶ Or even better yet, a physical USB key



How to avoid getting hacked on public WiFi:

- ▶ If you have the option to **use** your **mobile data plan**, that's better than public WiFi
- ▶ Criminals often setup hotspots with fake Wifi Names, so **ask** the Barista or Receptionist for the **Official WiFi Name**
- ▶ Enable the Firewall on your device and **use a VPN**
(Try to avoid Free VPN's - some are owned by criminals)





Ransomware

When criminals hack your computer or network, lock you out, and demand a ransom to let you back in.





How to Avoid Ransomware

- ▶ **Don't download** files from random websites
- ▶ **Beware** of phishing emails with attachments
(See phishing section)
- ▶ **Don't use** your company email or password for personal stuff
- ▶ **Don't store** password in text files or spreadsheets





How to use USB Safely

- ▶ **Avoid** public charging stations. They may be compromised.
- ▶ **Don't plug** any USB that isn't yours into your device
- ▶ **Encrypt** the data on the USB device in case you lose it or it gets stolen.





What is **CEO (wire) Fraud**?

It's when you're tricked into wiring money to a fraudulent bank account.
For example:

- ▶ An urgent request to wire money from a criminal who impersonates your CEO through hacking your CEO's email account.
- ▶ They hacked one of your vendors and sent you an invoice with fake bank information.

If you're tricked into wiring money to a fraudulent bank account, the bank may not be there to help you. After all, it's **you who transferred the money**, not the criminal.



How to Avoid CEO Fraud:

- ▶ **Call and verify** any money Request
- ▶ **Call a known number** that you used before or from the vendor management system
- ▶ **Verify** that the bank info match the one on file
- ▶ **Call and verify** any request to change info on file, like phone number, address or bank info





Questions / Doubts?





Thank You!
You made it.

