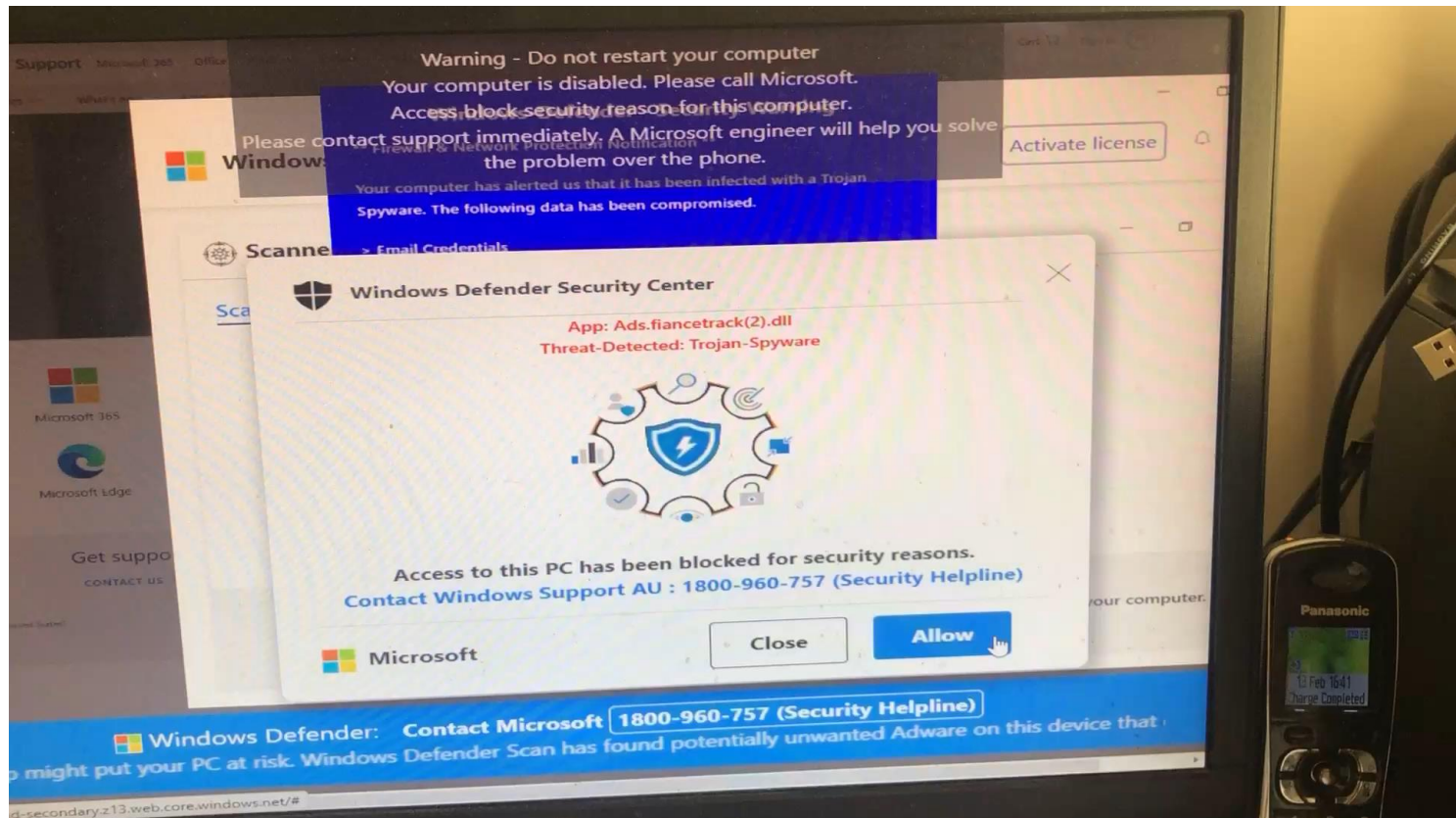


Cyber Security Awareness



Technical Support Scams

1. Usually a fake message on your computer screen directing you to call a specific number (see real example below).
2. Can also be someone that randomly called you on the Telephone.



Technical Support Scams

Protection Strategies

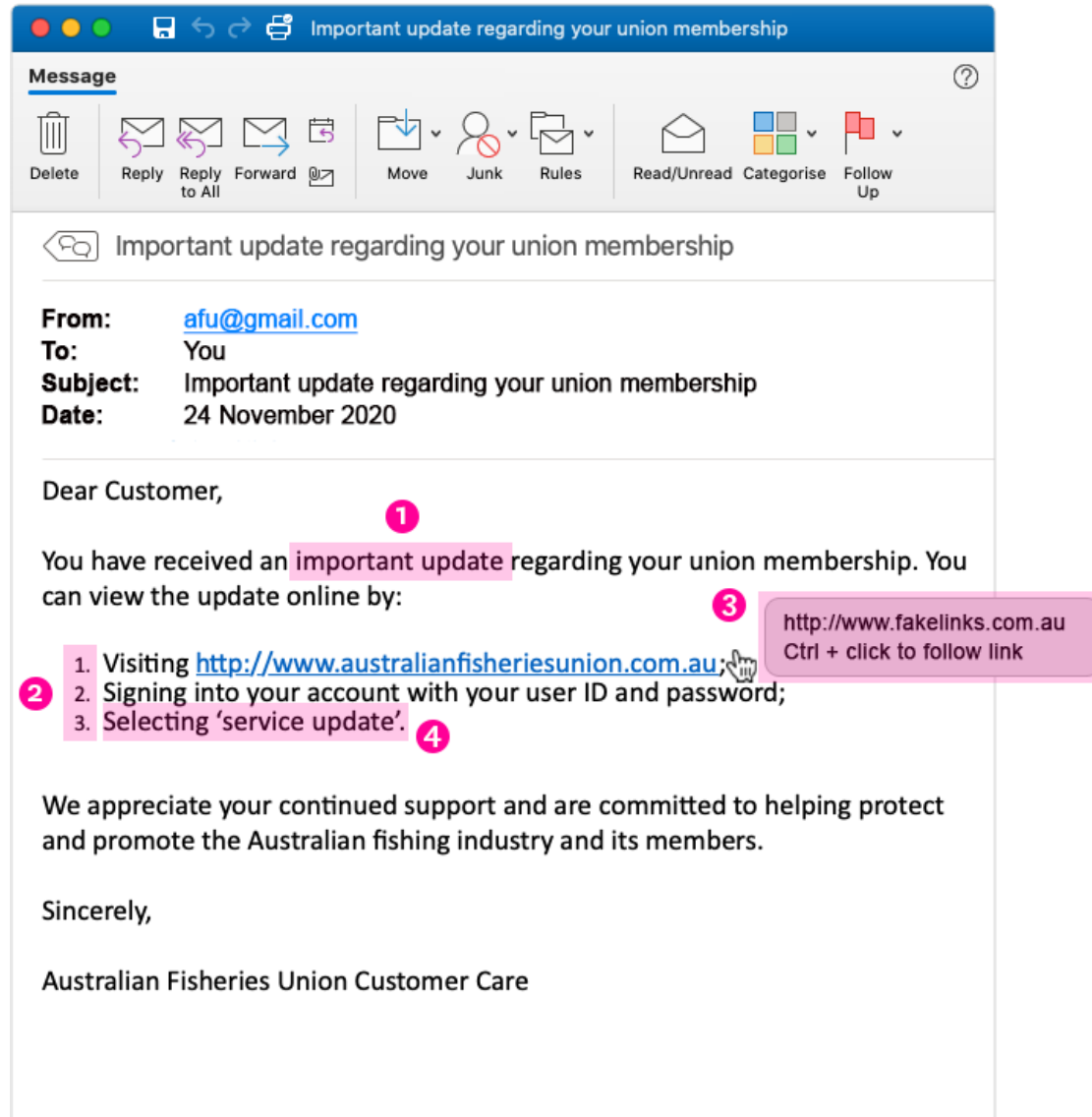
1. **VERY IMPORTANT:** Never actually call the 1800 number.
2. **Restart** computer and run a virus scan.
3. **Reset** your Browser (to clear cache & junk).
4. **NEVER** call any number provided to you by a random computer pop-up screenshot.
5. **Red flags to look for:**
 - Screen won't go away easily.
 - Screen tries to scare you.
 - Screen has a sense of urgency.

Phishing Scams

- Fake emails or phone calls purporting to be from DHL, FedEx, Netflix, Amazon, Paypal, Banks, and others.
- For the purpose of tricking you into getting access to your online bank account, or providing your personal details like Passwords, Credit Card Numbers, etc.



Example of Phishing email



Phishing Scams

Protection Strategies

1. **NEVER** click on a link directly from an **informal** email or phone text message, purporting to be from your bank, a courier company, Transurban Tolls, etc. They want you to log on to their fake website to steal your username & password. Real companies address you by your name, and **never ask you to click links**.
2. **NEVER** call any number randomly provided to you by a computer screenshot.
3. **NEVER** give your Credit Card number or allow remote access of your computer to anyone, unless you initiated the contact yourself.
4. **Reset** your Browser (to clear cache & junk).

Ransomware Threat

- Malicious code infects your computer and encrypts all your personal data, making them inaccessible to you (photos, PDF's, all Word/Excel/Powerpoint files, TXT files, and much more). The encryption is real, not a bluff, and your files are truly inaccessible.
- Then demands that you pay a “fee” (the ransom) or they will never release your files back to you. A sense of urgency is always included, usually with a countdown showing how many hours remaining before your files will be lost forever.



Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

11/25/2024

Time Left

02:23:53:13

Your files will be lost on

11/28/2024

Time Left

06:23:53:13

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

115p7UMMngoJ1pMvkpHijcRdfJNXj6LrLn

Copy

Check Payment

Decrypt

Ransomware Threat

Protection Strategies

1. It is critical to have a complete backup of all your important personal data (like photos, etc), so that you can recover your personal files if you should fall victim to a Ransomware attack. Apart from Ransomware file loss, a good thorough backup is essential for other reasons as well, such as hard drive failures, fire damage, etc. Many people know how to backup files, so if you do not know how to backup your files, consult a knowledgeable friend or relative as your first port of call.
2. Make sure your computer has active Ransomware protection. Some free/cheaper security software don't include it for free and require you to pay to upgrade to include Ransomware. There's a link on that self-help sheet for a very good free Ransomware protection software that you can download and install to your computer, and is designed to work alongside your existing antivirus software.

Hi Mum Scam

- This scam involves the offender sending a text message from an unknown mobile number claiming to be your son or daughter (or just your “child”). Could be via SMS or messaging apps like WhatsApp.
- The message will say they have lost their phone, telling the victim to delete their old number.
- Once the victim replies to the message, the offender will make an excuse about how they are unable to make a payment before asking to borrow money or have a payment made on their behalf.
- The offender will usually state it is a matter of emergency before providing details for the payment.

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



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



Simpler version of the Hi Mum scam (The Grandparent Scam)

Scammers will place a call to an older person and say something along the lines of: “Hi Grandma, do you know who this is?” When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity without having done any research.

As with the Hi Mum scam, the fake grandchild will now proceed to ask for money to solve some urgent problem (medical expense, overdue rent, car repairs, etc).

Hi Mum

Protection Strategies

1. If you get messaged by someone claiming to be your son, daughter, relative or friend, start by calling them on their original number already stored in your phone to confirm if it is indeed no longer in use. If they pick up, then you know it's a scam.
2. Another good idea is just demand that they tell you exactly who they are by name, and request a voice or video communication rather than just text messages.
3. With the phone version of this scam, try not to give out any names if someone wants you to guess who they are. Respond defensively by saying *“who is this please, you don’t sound familiar to me”*.

Confirmation Code Scams

This scam involves receiving a phone call from someone purporting to be from the fraud section of Amazon, Google, Paypal, Apple, or wherever. They will tell a colourful story about how someone tried to hack your account, but they stopped them in time, and now they want to confirm that you are the real owner of the account before they can reinstate it. They ask you to read out a confirmation code that they are sending to you right now. And sure enough, a code arrives on your phone as you are speaking to them. The only problem is that the scammer didn't send that code. He used your phone number as the username, but then pressed "FORGOT PASSWORD" so he can reset your password and steal your account. The website sends a code to the registered owner (you) to insure that it is you resetting the password. He is just tricking you to tell him that confirmation code.

Confirmation Code Scams

Protection Strategies

1. If you get contacted by someone that wants to send you a confirmation code, they are 100% a scammer. Confirmation codes are not used for verbal confirmations over the phone.
2. The code even warns you to never reveal the code to ANYONE else. You can even mention this to the scammer by saying the code message says not to reveal the code to anyone. He will give you a really good excuse why he is the exception to that rule, but at this point it's time to say you will be reporting this phone call to the authorities, and then hang up.

Your computer has been locked

If your computer is locked, and you are seeing a **“Your computer has been locked”** notification, then your computer is infected with a piece of malware known as Trojan Reveton.

There are two variants to this scam, the first one is similar to the “Tech Support” scam we already covered, where they pretend to be from Microsoft, Apple, Google, etc. The second variant appears to come from a law enforcement agency (eg: FBI, Australian Federal Police, Metropolitan Police).

The fake alert comes as a browser-based message that tries to scare you into paying a “fine”, or to call a remote tech support number so the scammer can steal your credit card number by charging you for the “support service” they gave you.



All activity of this computer has been recorded
If you use a webcam, videos and pictures were saved for identification



Video-recording: **ON**



You can be clearly identified by resolving your IP address and the associated hostname

Your IP Address:

Your Hostname:

Location: **Australia**

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

Article 105 – Misuse computer use, restricted access consequences

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **100 AUD**.



You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Where can I buy Ukash

Prepaid4.me



Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code:

1 2 3 4 5 6 7 8 9 0

Submit

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

Your computer has been locked

Protection Strategy

1. **VERY IMPORTANT:** Never actually call the 1800 number.
2. **Restart** computer and run a virus scan.
3. **Reset** your Browser (to clear cache & junk).
4. **NEVER** call any number provided to you by a random computer pop-up screenshot.
5. **Red flags to look for:**
 - Screen won't go away easily.
 - Screen tries to scare you.
 - Screen has a sense of urgency.
 - Payment is wanted in an unusual way (Ukash, Apple Gift cards, Bitcoin, etc).

Compromised Password Scam (or “pwned” email passwords)

- When the password from your username login has been stolen by data breaches from legitimate sources, due to their poor cyber security. The usernames and passwords are then sold on internet black market websites. This has happened to almost every company, including Adobe, Facebook, Yahoo, LinkedIn, Mastercard, and hundreds of other sources.
- Scammers send an email to the compromised accounts, pretending that they are some genius super-villain that hacked your computer, and now have access to your email address. As “proof”, they tell you the correct password for your email address (most people use the same password everywhere).
- Then they pretend that they also used the webcam on your computer to video record you in embarrassing situations.
- Finally, they try to extort money from you by demanding a Bitcoin payment in exchange for them to delete the embarrassing videos of you. Failure to pay them, and they threaten to send the embarrassing videos to everybody on your email’s contact list.

Compromised Password Scam

Protection Strategy

1. First and foremost, the entire threat is a bluff. There is no embarrassing video footage, and they do not have control of your computer. They just purchased a list of millions of stolen usernames & passwords, and used that information to send phony threats to extort money. However, it is disturbing that your correct password is in the cyber criminal public domain.
2. If you received such an email threat, with the correct password showing, it means that your email address has indeed been compromised, and you should immediately change the password.
3. To see if your email account has ever been “pwned”, go to this website: <https://haveibeenpwned.com/> and type in your email address. It will tell you if it has been breached or not. Here’s a screenshot of that website...

FileEditViewHistoryBookmarksToolsHelp

'-- Have I Been Pwned: Check if yo X

https://haveibeenpwned.com

☆🔒📄🔍📄📄

'--

HomeNotify meDomain searchWho's been pwnedPasswordsAPIAboutDonate💰🗨️

'--have i been pwned?

Check if your email address is in a data breach

michael@ncams.com.au

pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

📘

Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

Why 1Password?

851

pwned websites

14,505,253,859

pwned accounts

115,797

pastes

229,161,508

paste accounts

Largest breaches

📄

772,904,991

[Collection #1 accounts](#)

📧

763,117,241

[Verifications.io accounts](#)

Recently added breaches

🌈

436,855

[Otelier accounts](#)

msi

249,990

[MSI accounts](#)

FileEditViewHistoryBookmarksToolsHelp

Have I Been Pwned: Check if yo X

https://haveibeenpwned.com

Have I Been Pwned?

Check if your email address is in a data breach

michael@ncams.com.au


pwned?

Oh no — pwned!


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

3 Steps to better security


Start using 1Password.com



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

[Facebook](#) [Twitter](#) [LinkedIn](#) [YouTube](#) [Instagram](#) [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Oxfam: In January 2021, [Oxfam Australia](#) was the victim of a data breach which exposed 1.8M unique email addresses of supporters of the charity. The data was put up for sale on a popular hacking forum and also included names, phone numbers, addresses, genders and dates of birth. A small number of people also had partial credit card data exposed (the first 6 and last 3 digits of the card, plus card type and expiry) and in some cases the bank name, account number and BSB were also exposed. The data was subsequently made freely available on the hacking forum later the following month.

Compromised data: Bank account numbers, Dates of birth, Email addresses, Genders, Names, Partial credit card data, Payment histories, Phone numbers, Physical addresses

Important Take-Aways

- Never click links in an email or a text message. Scam links from mobile phone SMS messages are getting more dangerous, especially from Android phones.
- Never call any number that appeared in a pop-up screen or text message, trying to scare you. These are all fake and only used by scammers.
- Never talk to anyone calling you out of the blue, or messaging you, claiming to be from Amazon, Netflix, Ebay, Bank, Courier, Transurban Tolls, etc.
- Never tell anyone any confirmation codes that come through your phone as you are talking to the scammer. They are tricking you by using that code to reset your password.
- Be extremely suspicious if the message conveys urgency or incites fear.
- No real company or organisation wants to be paid with Bitcoin or Apple gift cards. Any kind of request for these kind of payments is 100% a scam.
- Don't antagonise or use foul language when talking to scammers, they can be spiteful and can abuse the fact that they know your mobile phone number. Be firm and just let them know you are not going to be their victim, and they will just move on to their next target.
- Do not be overly polite, but don't be rude either. Better to risk offending someone than getting your life savings stolen from you. Assume everyone is trying to scam you. Always tell suspicious callers that as a precaution you will call them back on the official phone number, just in case they might be a scammer. Real employees won't mind, but a scammer will try to talk you out of it. Just hang up if that happens. If they ring back, tell them you have already called the police, and they are tracking your calls for you.

Free Downloads

Go to www.ncams.com.au/security.html
and download:

- This presentation (as a PDF file).
- The link to the free Ransomware Protection Software (and free Antivirus if you need it).
- The “pwned” link to check if your email account has been compromised.
- Video link showing how to reset your Browser.
- Useful Technology Resource Link for Seniors.