Spotting:

Scams & Malicious Acts

Created Date: 10/07/2013
Update Date: 01/07/2024

Ver. 11.0

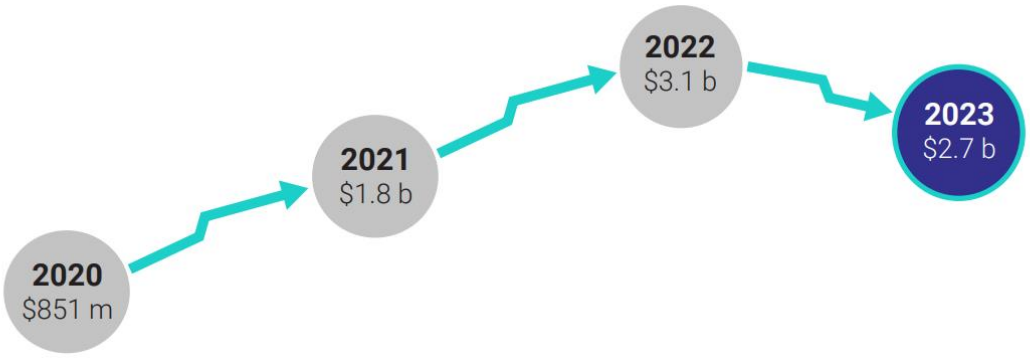
Scams have become more rampant over the years.
They cost organizations around the globe averagely $4.5 billion every year and over half of internet users get at least one phishing email per day.
In -**2023**-, Reported by Organizations like SCAMWATCH, ReportCyber and other entities were combined and shown that Australia reported a loss of -**$2.74 Billion**-, which is a decrease from last year, which is great news!

$2.74 billion in losses

Total combined losses reported to Scamwatch, ReportCyber, IDCARE, Australian Financial Crimes Exchange (AFCX) and Australian Securities and Investments Commission (ASIC)

601,000+
scam reports
▲18.5%

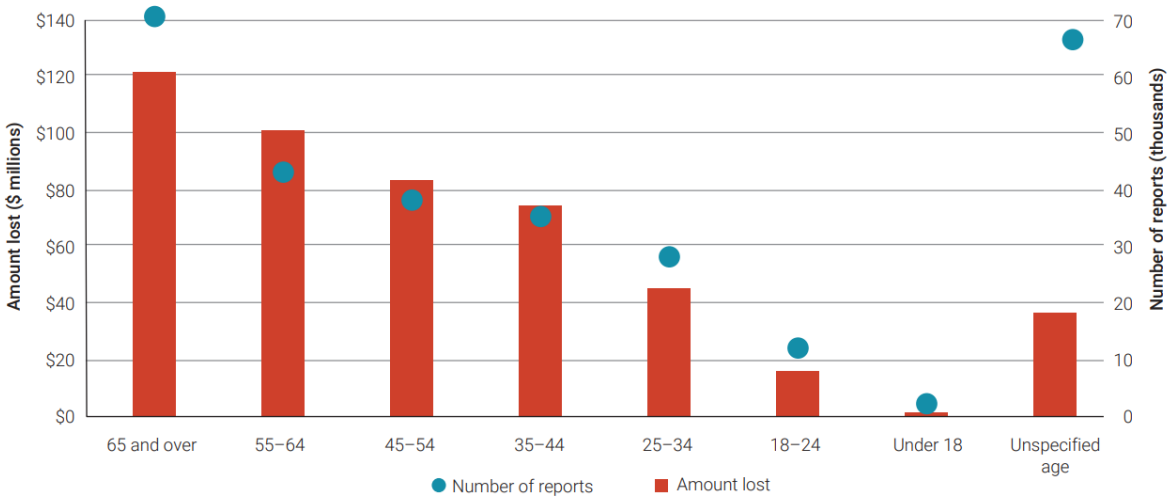
Combined losses over last 4 years



Top 5 scams by loss (combined data)

Investment	Remote access	Romance	Phishing	Payment redirection
$1.3 b	**$256.0 m**	**$201.1 m**	**$137.4 m**	**$91.6 m**

Scam reports and losses by age group



Contact methods by loss and reports

Contact Mode	2022 losses (m)	2023 losses (m)	2022 reports	2023 reports
Phone call	$141.0	$116.0 ▼	63,816	55,418 ▼
Social media[34]	$80.2	$93.5 ▲	13,427	17,542 ▲
Email	$77.3	$80.0 ▲	52,159	85,941 ▲
Internet	$73.5	$69.7 ▼	13,692	17,568 ▲
Mobile apps	$71.7	$64.8 ▼	10,057	8,101 ▼
In person	$30.6	$21.5 ▼	2,186	3,614 ▲
Text message	$28.5	$26.9 ▼	79,835	109,621 ▲

Investment Scams are still the highest of all scams, especially with Cryptocurrency.

Scams are commonly initiated via Phone Calls & Emails, but they also can come from Social Media, Messaging Services, Compromised Website/Computer Devices, Physical Mail and even at your premises.

What Scams can you come across?

There are many different Scams that have been created over the years, many of which have also been changed to match things like Country, Person, World Events etc.

Here is a list of common Scams used in Australia:

Romance Scams

These scams are related to people who find a significant other online, building up a relationship online with someone from another country. The Scammer will put effort in getting the relationship to a high enough level that you are willing to help out with anything they request.

When this occurs, you will be usually asked for “Emergency Funds” to help a sick or dying relative or pet or “themselves” (scammer) or they will ask you to send money or pay for them to come to Australia to meet in person.
They usually ask you to send money to an Overseas Account, in another person’s name or country - Maybe even both.

Remote Access Scams

Commonly, the Scammer will call you for these types of scams. Other ways can include some kind of breach of a website, a fake website or your computer having Malware/Viruses.
These scammers will pretend to be A Company, normally IT Support.
Internet type scams will have a popup or alert saying your computer device is compromised and to call the number on the screen for help.
Call type scams can also be:

- Tech Support like Microsoft, Apple, Google
- Internet Security Companies like McAfee, Norton or Malwarebytes
- Telecommunications Companies like Telstra, iiNet or Aussie Broadband

The Scammer will ask to get Remote Support of your Device, commonly a Computer Device so they can help you “Fix your Problem”. They say issues like you are hacked, your devices are sending malicious things, you have issues with your Internet, anything convincing to initiate a Remote Session.
Scammers use legitimate Software that they make you download like TeamViewer, AnyDesk or LogMeIn.
They will show you the “Event Viewer” on Windows Computers to show all the critical warnings and tell you that its all the bad things like viruses and hackers or the Command Prompt (Black Screen Window) and type in various things to “Run a Scan” and as it shows what you may think is a scan, they are secretly typing an “error” message that shows up at the bottom that you have a virus or something bad.

This is where they will “Clean” your computer from issues and even put on “Protection” AKA Security Software to “Protect you”.

Nobody really knows there are issues but **YOU**. So, if you haven’t actively sought out Technical Support, then it’s likely a Scam!

If you have any weird activity or pop ups that suggest contacting Support, turn off your computer and seek Local Support like from CPKN Computers.

If you get a phone call about issues with your Computer or Internet Connection and they want to remote access your Device, get as much information as you can about the Scammer and give as little as possible to them about you. Get their name, the “Company” they are with, the phone number they used and any other details they may have told you, then tell them you will seek help from your Local IT Support Company. If they try to convince you to stick with them, just tell them it will be ok, you will keep Computer off and contact your Local Business. Hang up if they do not comply.

Refund/Money Mule/Lottery/Inheritance Scams

Scammers have methods to receive money from you without you getting as promised.

Refund Scams are common, particularly Amazon calls, where they tell you that they have a refund for a mistake or "suspicious" activity on your account that they are happy to cancel and refund you.

When you participate in the Refund, then they will commonly use the "Fake Transfer" Technique, which includes Remote Access to your Computer. Any Refunds that require Remote Access is **ABSOLUTELY** a scam. Logically, the company will have access to the bank or card details to refund or ask for your bank transfer details to send it. If they ask for Card Details to Refund, tell them to use Bank Transfer details only.
When they access your device, they get you to log into your Bank Account where they do their disgusting magic.
They will have you navigate to show your history, then black out your screen while they "process" the refund. While you are blank, they use tools in your Web Browser to change the code to change and reflect that you got a Refund.
They use various methods and scripts to how they get to this point, but once it is complete, they bring the screen back to you and then start the "cry baby" script when you both find out that your refund (for example of $250) has a few extra zero's. So, you may see $25,000. They start "panicking" and beg you to help them by sending the money back. They of course make sure you can afford it for how many zeros they add. Sometimes they have a Bank Account you can send the total amount, minus your refund, or they will ask you to buy Gift Cards minus the refund amount.

Money Mule scams can be a once off or ongoing.

You may come across a Job Advert to assist with Account Management. They will offer "work from home", good pay and basic requirements.
Your Job is to basically receive money then send money to another account. Your Account looks legit to Fraud Departments and so you give a clean option to scammers.
For one off, you are offered a large sum of money you likely won't ever get.
For ongoing, they give you nice commissions based on how much you are transferring/handling.

Lottery, Investment & Inheritance Scams often tell you are to be given large amounts of money for a particular reason or ask for help handling/receiving the money.
You will be asked to cover the "transfer fees" that you must pay the scammer first before getting sent the money. Then you will never see your large sum come in.

Tax/Arrest Warrant Scams

The last common scam is getting calls or emails that you Owe Tax or a call saying you have done illegal activity, including Tax related crimes and have an Arrest Warrant.

You will be given the opportunity to pay your Tax Debt via their various means, including **GIFT CARDS!** (**RED FLAG!**) or pay your fine and/or legal fees that removes your Arrest Warrant, or a combo of both.

There are many other scams like Solar scams, Car Insurance scams, door to door scams that are common in Australia.

It makes it hard to know who you can trust.

What can be done to tackle Scams and what are signs its fake?

The most common way the average person gets involved in a scam is via a Phone Call, Text Message and/or Email.
Calls come from all sorts of Scammers, whether it be a Refund Scam from "Amazon" to an Arrest Warrant Scam because you "didn't pay your taxes" or have done "tax fraud".
Text Messages for Refund Scams are the same, but in recent months, Delivery Link Text Messages have been slamming Australian Phones.

Emails can also vary the same sort of scams like phone calls. Commonly, you will have Billing and Bank Scam emails, "owing" money or getting a "credit". There are also Phishing Scams to try and grab your login details for places like Facebook, PayPal, Online Shop sites (eBay, Amazon etc) and Banks.

The internet and websites can play a role in fooling you also. You may get a link, an article etc that points you to a Website that might have something for you to fill out like a form, or download something, this is also where people think its all fine, until it isn't.
Example is a friends compromised Facebook account, who post or message you a link to an article, but to read it, you need to log into your Facebook. Because it is your trusted friend, and nothing seems suspicious, you follow the link and you log in, only to find out that the article didn't actually need you to log in to read, you just filled in a fake log in form, to then losing access to your Facebook.

Websites can be compromised or Spoofed (Cloned). Compromised sites might initiate pop ups that look legitimate, like the Microsoft Scam that tells you something is wrong with your computer and to call them on a particular number provided.
Spoofed websites are used to fool you into thinking you are on a website you visit day to day, like bank scams.

Let's look at signs and solutions:

For emails, the best defence Email Companies have against phishing attacks/Scams is to block malicious emails before they reach customers with the DMARC (Domain-based Message Authentication Reporting and Conformance) standard. DMARC puts kind of a "Ownership" sticker on the Domain used like "@cpkncomputers.com.au". Because our Domain has been attached to our Business and our Server where our email lives, then unless the message comes from our server with our sticker of approval, it should not make it to the other end.
Unfortunately, no matter what companies do, some phishing emails will always make it to the inbox. And those messages are extremely effective—97% of people around the globe cannot identify a sophisticated phishing email.

Don't trust the display name

A favourite phishing tactic among cybercriminals is to spoof the display name of an email. A Security Firm analysed more than 760,000 email threats targeting 40 of the world's largest brands and found that nearly half of all email threats spoofed the brand in the display name.
Here's how it works:

If a fraudster wanted to spoof the hypothetical brand "My Bank," the email may look something like:

"My Bank<accounts@usbank.ru>"

Since My Bank doesn't own the domain "usbank.ru," DMARC will not block this email on My Bank's behalf, because My Bank has set their DMARC policy for mybank.com.au to reject messages that fail to authenticate, but the domain is "usbank.ru".

This fraudulent email, once delivered, appears legitimate because most user inboxes only present the display name, and many people see the name and think it's from the legitimate business or friend/family member. Display Names don't have to match Domains.

Always check the email address.

Look but don't click

Hover your mouse over any links embedded in the body of the email.
What you should find is, a pop-up should show up, floating at your mouse pointer, and it should have a "Click Tip" bubble that gives information on what that link is.
If the link address looks weird, don't click on it. If you cannot get the Click Tip, don't click it.
Phones and Tablets are best to not mess with link peaking, instead, try to copy the link only and use a link checker.
If you want to test the link, visit our website to use the provided link checkers:

cpkncomputers.com.au/scam-support/

Check for Spelling and Grammar

Brands are pretty serious about Email and Text Messages. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails/texts carefully and report anything that seems suspicious.

Analyze the Salutation

Is the email addressed to a vague "Valued Customer?" If so, watch out — legitimate businesses will often use a personal salutation with your first and last name, unless you did not register, so treat it like Junk Mail you get in the Post, just make sure its legitimate stuff before doing anything.

Don't give up personal information

Legitimate banks and most other companies will never ask for personal credentials via email.

Being asked for the passwords to your online accounts? Organisations will never ask for the passwords to your online accounts.

Emails, texts, or calls asking you to “verify” your account or details – don’t respond or click on any links in the communication, even if it looks like it’s from a real organisation. Call them and have **THEM** confirm.

Beware of urgent or threatening language in the subject line

Invoking a sense of urgency or fear is a common phishing tactic.
Beware of subject lines that claim your “account has been suspended” or your account had an “unauthorized login attempt.” Verify it by accessing your accounts directly or contacting the account provider directly to see.

Review the signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details.

Don’t click on attachments

Malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge.

Don’t open any email attachments you weren’t expecting.

Don’t believe everything you see

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it’s legitimate.
Be sceptical when it comes to your email messages—if it looks even remotely suspicious, don’t open it.

The offer seems too good to be true

There is an old saying that “if something seems too good to be true, it probably is”.
That holds especially true for Email & Text messages. If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.

Unrealistic Threats

Phishing artists use intimidation to scare victims into giving up information.
In the US or even here in Australia, scammers call you or email you, stating they are from the Tax Office and they have a Warrant for your Arrest for Fraud or Tax Evasion, pay them IMMEDIATELY to cancel the warrant.

There is even a scam in Australia, that luckily has a small impact due to how we do insurance and dealing with this subject - but scammers will call saying they are from the “Accident Department”, mostly being from the Department of an Insurance Company. They used to act as your Insurance, but when asked what the company is, they would get caught out, so now they are from the “Complainants” Insurance.

Being contacted about something wrong

If you are being contacted by phone out of the blue – even if the person says they’re from a legitimate organisation like the bank, an embassy or your internet provider, to then being told there is a problem with your phone, laptop or internet connections – often they will offer to fix your device or say they are from your phone or internet company and need to rectify the issue.
In a Telstra Scam, they call you to say your “IP (Internet Protocol) Address” has been hacked.
They say your Computer Protection can’t protect you and that they must fix your “Internet” to stop them by putting “Security on your IP”.
It becomes clear that it is a scam when they try to explain to you that you connect to the internet from your connection as if your Internet Company has no control or say in it, and that your connection goes to the internet, to them, then back to the internet. Where they tell you your internet has been hacked, is where they should be responsible and have control over, because where they say you are hacked, is actually saying **THEY** were hacked, but blame you and you must pay... MISSION FAILED!

Money, Money, Money

Scammers may offer money or something else, but you have to make a payment or give information up front – they might say that it's a "processing" fee or something similar.

Friends/partners you've met online asking for money or talking about problems that could be solved with money – this is a very common tactic, do not pay the money.

Unusual ways to pay for something – scammers try to use payments that can't be traced such as pre-loaded debit cards, gift cards, bitcoins, iTunes cards or money transfer systems.

Remote Access

Remote Access to your Devices is a useful tool for Support Providers to assist you without being with you physically, saving time and in some cases, money.
CPKN Computers is an Example of a Support Provider that is able to do work remotely using our Verified, Secure, Remote Access Software.

Scammers, especially in Virus or Tech Issue Scams will likely always ask for remote access to your device – asking to be let "in" to your device when they are in another location – never do this unless you have actively sought out the service they are providing, such as a legitimate Support Provider.

Under Pressure

Scammers tend to start pressuring you to make a decision or take action quickly – this could be to avoid something bad (e.g. account being closed, trouble with computer) or to take advantage of something good (a really good deal or investment).

Dealing with Phone Calls

If you are getting a call from a number you do not know, particularly Mobile Numbers and private numbers, then you will need to remain vigilant on the intentions of the call.

If someone is calling as a Business or Government Entity with a Mobile Number, then this is where suspicion should become high.

If they start with saying your name, do not confirm it, instead politely say “sorry, may I ask who is speaking first?” or something along those lines, to have them identify themselves first and have them tell you what the call is about first.
If it doesn’t sound right in your gut, then keep information to a minimum and try to disengage from the call.

Ask lots of questions, get to know who the person is and their intentions. Note down how they sound, male or female, accent, who they say they are, the number they called you on. Ask for a Reference Number. Give them as little details about you as possible for as long as you can and don’t confirm anything if you can avoid it.
If you feel uneasy, tell them that you will get some information on the matter and call back ASAP. Source out the legitimate Phone Number of the Business or Government Entity and verify if they are legit with their call or if it was a scam. If you feel uneasy full stop and don’t know a number to trust, call a IT Professional or go to a Local Branch directly.

We Recommend the following to help Secure your Devices and Internet:

- **Ensure you have Security Software Installed, working and up to date.**
  → **We can provide recommendations and help install Security Software**
  → **For Businesses, we can provide Business Grade Security with our Managed Services. Get more information – Business Management Service (BMS)**
- **True Caller App for Android & iOS.**
  → **This App can help you identify Spam/Scam Callers, Block Numbers and more.**

If the person contacting you (by email, phone, text, letter or other) has said that they are from a legitimate organisation and you're not sure if it's genuine, you can contact that organisation to check.
Make sure that you use the phone number or email they have on their official website or in the phone book – do not use one given to you by the person or in the email they have sent you.

If you are completely unsure, contact us for support. We provide a Free Scam Check.

Report Scam Attempts to us or visit/report to Scamwatch – An Australian Government Division.

Please refer to the Created Date and Revision Number on the Front of this Document.
If you think you do not have an Up-to-Date Version, please ask for one from CPKN Computers.

ABN: 72 930 048 407
Phone: 02 6138 5012
Web: www.cpkncomputers.com.au
Email: support@cpkncomputers.com.au