Let's Talk: Scams

30 September 2020

Alex Meaney

Assistant Director, Consumer and Small Business Strategies Branch

accc.gov.au

Overview

- Our role
- 2020 scams
- Interactive example usage
- Key messages we recommend
- What to do if scammed + resources advice
- (If time) Other common scams

SCAMWATCH

The role of the ACCC

National regulator – we oversee laws on consumer protection, competition, product safety and infrastructure access

Enforcement of the ***Competition and Consumer Act 2010*** and the ***Australian Consumer Law***

Dual **educative** and **enforcement** function – we do not set policy

Regulation of some industries (energy, telecommunications), **industry codes** (franchising, food and grocery) and price surveillance (airports, postage)

Awareness raising with consumers and small businesses about **scams**

The role of Scamwatch

Report a scam web form

- Scam experiences
- Loss data
- Demographics data

Analysis of scam data

- What are scammers doing?
- How are they doing it?
- Who are they scamming?
- How effective are they?

Education and awareness

- Information on the Scamwatch website
- Public reports
- Media engagement
- Industry engagement – telecommunications, financial services
- Scams Awareness Network

What is a scam?

- A scam is where someone tries to trick you into giving them your money or personal information. Scams often:

  - look real
  - catch you by surprise
  - come with believable stories.

SCAMWATCH

Top 10 scams by losses

Jan – Dec 2019

Scam category	Reports	Losses
Investment scams	5005	$61 813 401
Dating & romance scams	3948	$28 606 215
False billing	11 254	$9 908 756
Hacking	8321	$5 139 414
Online Shopping Scams	9953	$4 845 452
Remote Access Scams	9019	$4 836 812
Identity theft	11 373	$4 311 066
Threats to life, arrest or other	13 375	$4 250 689
Classified scams	4958	$2 816 076
Inheritance scams	2920	$2 622 355

New 2020 scams

Australian Government

Services Australia

Our Reference: 14-A0-931C67
Thursday, May 7, 2020

Subsidy benefit allocation

We are writing to bring to your knowledge the allocation of your subsidy benefit.

Kindly affirm your eligibility by simply replying to this secure message appropriately as listed below.
Please indicate correctly...

Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address (*Street number & name/Subu... Stat... ostcod...*

Enter at least one of the information list... correctly

1. Notice of assessment (one from the last 5 years)
Enter the date of issue from your notice of assessment (DD/MM/YYYY) **:**
& Enter the our reference number from your notice of assessment (no spaces) **:**

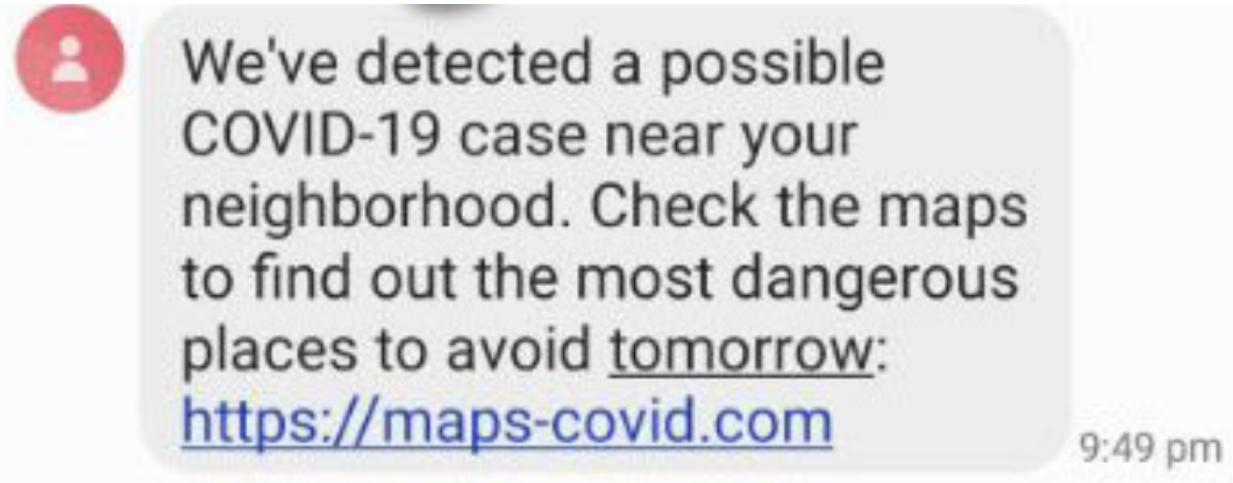
2. Superannuation funds details
Enter Superannuation Issuer & ABN :
& Enter your member account number :
Enter your member client number :

NB:. Attach to your reply, a clear copy of your valid Australian Driver Licence **OR** Australian International Passport **AND** a clear copy of your valid Medicare Card.

SCAM

Top 2020 scams

- Text messages linking to malware pages
- https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams



Most damaging broad category scams in 2020

- In 2020, to the end of August, we have received over 120 000 scam reports with over $100 million in losses.
- Top 3 scams reported in 2020.
- Threats to life, arrest or other have more than doubled since 2019.

Scam category	Reports	Losses
Investment scams	4597	$37.3m
Dating & romance scams	2648	$26.6m
Threats to life, arrest or other	12 615	$7.8m

Investment scams

Common techniques scammers use

- You receive a call or email from someone offering advice on investments.

- You are told that you need to act quickly and invest or you will miss out.

- An advertisement or seminar makes claims such as 'risk-free investment', 'be a millionaire in three years', or 'get-rich quick'.

Case study – Investment Scams

$430 000 Loss – Report from 3 July 2019

During June 2018 **I was contacted by a company** called the Gloucester Group in Hong Kong.

They introduced me to a certain share that have the **potential of big earnings**. I bought some of the share and **it did extremely well**. The guy I was dealing with was Richard Mason. **Later they moved me to a more senior guy** with the name of Christian Langley. There is also a director with the name of Patrick Conway. All the people at the company speak with a clear British accent and they tell you they are remainders of the old British Colony.

They **called me twice a week** and build a strong trust relationship. Their system works that they open an account for you and you can **log in** at any time with a password to **see what is going on in your account**. They kept the account strictly up to date and user-friendly. My first investment was made in June 2018 and for the next six months I invested about $188 000 into their recommended shares. **My investment grew** to just short of US $ 300 000 in six months. Not bad at all!

I then decided to repatriate $100 000 back to South Africa. This is where the problems started. They promised me that it is OK but instead of paying the $100 000 back to me **they closed my account** and **stop all communication** with me. I tried to call them numerous times without success. I emailed them and ask what was going on. They never answered. So I must accept that I have been scammed cleverly by these people. So I need to warn all current and potential Investors.

Dating and romance scams

Common techniques scammers use

- You begin talking to someone online
- They suggest you move the relationship away from the website to a private platform
- They express strong emotions for you after a relatively short period of time
- They ask you to send money for a variety of reasons
- They have an excuse for why they can't meet you in person
- **2020 Development – Romance Baiting**

Case study – Dating & Romance

$73 000 Loss – Report from 1 August 2019

He presents as an Australian living in **Houston Texas**. An oil and gas engineer who **needed money** to secure a loan for a project he was awarded in Cyprus. His passport number and info (as provided) is from Australia: N3419915.

His story is his **wife died** from cancer 16 years ago and he has a 25 year-old daughter who is an engineer in Milan Italy. He has had relationships and the last one ended in or around 2017.

He is **charming** - appears to have high morals and values and at his age 57 he is looking for the right person to settle down with professing love/he found "her".

He is attentive, very good and consistent with his "script". When I told him I couldn't give him money he said he would **lose everything** and would likely go into a **"dark place"** and our relationship wouldn't survive.

He also involved a senior woman posing as his mother who (apparently lives in Melbourne) and with whom I spoke twice.

My family did all they could to open my eyes but they were shut. After "the deal" was done he still wanted me to travel to Cyprus for us to meet which I stupidly did - even 3 hours before my plane landed in Cyprus he texted me claiming he was on his way to the airport. Guess what? I ended up taking a taxi to a hotel for 4 days. **No lover boy showed up and no phone** - in fact he disconnected his phone.

Spotting Romance Scams

- Consider the signs we mentioned previously
- Reverse image search:
  - ‘Right-click Save-as’ their photo,
  - Google.com,
  - Click ‘images’ in the top right,
  - Drop and drag their picture.

- Check the city, state, and country match
- Check that physical details match the ph
- Check the quality of the English matches their education and location.

Getting out

- Cut off all contact:
  - Block their email
  - Block their phone number / all international calls with your provider
- Don’t be tempted. If they respected you they wouldn’t have lied.
- If you’re unsure think about talking to someone you trust.

Threats to life, arrest, or other

Main ones – very diverse though

- Dial ‘1’.
- Chinese Authority scams.

Warning signs

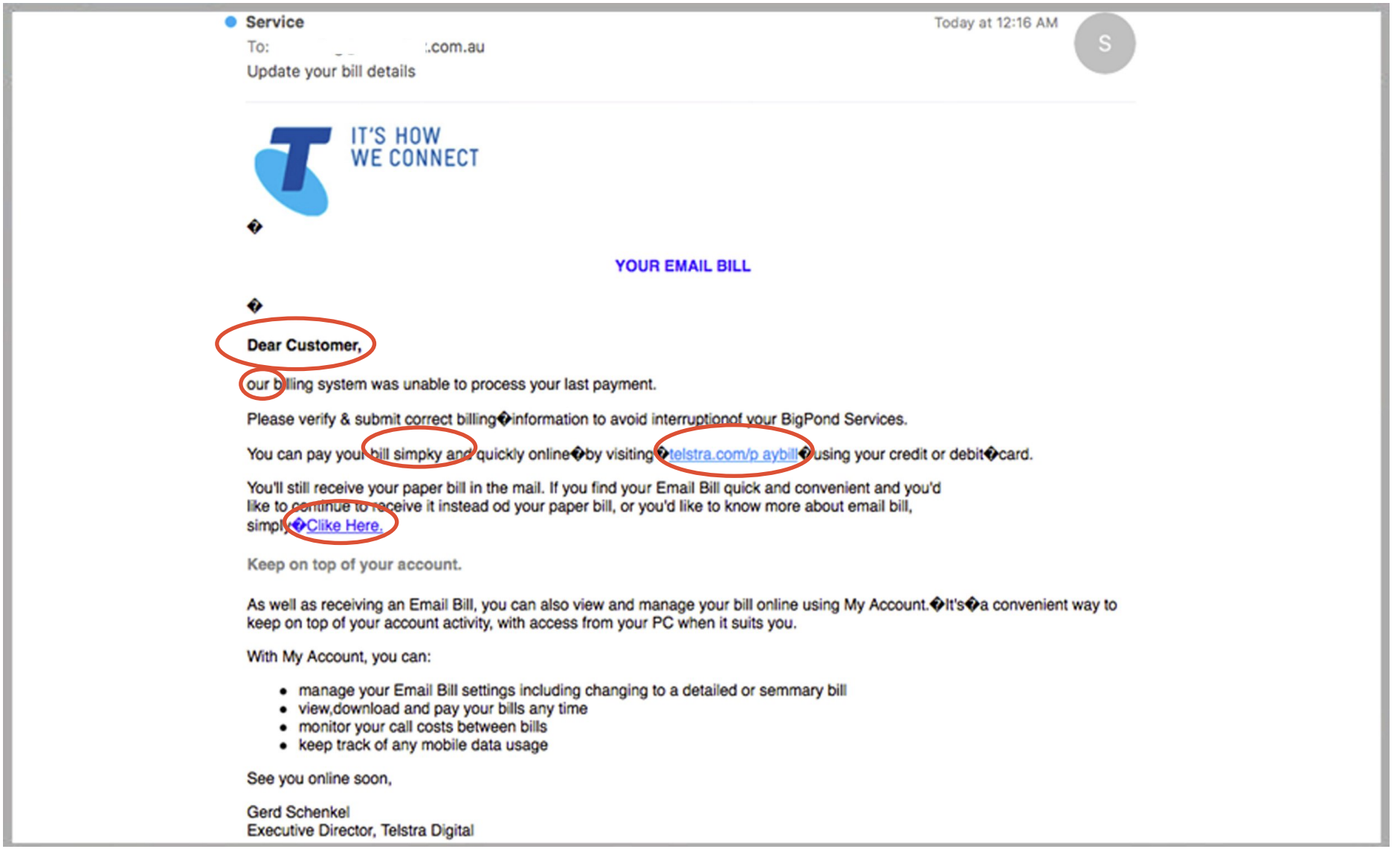
- The contact is unexpected
- Unusual methods like wire transfer or prepaid gift cards
- The person threatens you
- You have never met the person.

SCAMWATCH

Interactive Activity example

- Real life scam examples generally seem to resonate with audiences

- There are red flags; showing people they're not helpless and the internet and phone calls are still navigable is important.
  - The balance is ensuring people don't have a false sense of securoty and overconfidence in being able to spot scams.



Service
Today at 12:16 AM
To: .com.au
Update your bill details

S

IT'S HOW
WE CONNECT

YOUR EMAIL BILL

Dear Customer,

our billing system was unable to process your last payment.

Please verify & submit correct billing information to avoid interruptionof your BigPond Services.

You can pay your bill simpky and quickly online by visiting telstra.com/p aybill using your credit or debit card.

You'll still receive your paper bill in the mail. If you find your Email Bill quick and convenient and you'd like to continue to receive it instead od your paper bill, or you'd like to know more about email bill, simply Clike Here.

Keep on top of your account.

As well as receiving an Email Bill, you can also view and manage your bill online using My Account. It's a convenient way to keep on top of your account activity, with access from your PC when it suits you.

With My Account, you can:

- manage your Email Bill settings including changing to a detailed or semmary bill
- view,download and pay your bills any time
- monitor your call costs between bills
- keep track of any mobile data usage

See you online soon,

Gerd Schenkel
Executive Director, Telstra Digital

Re: [Message report Update statement] || [Accepted login Access] account has added updates -on september 23 ' Microsoft Statement permission address49661650

Be careful. This message looks like a phishing scam. Learn more about phishing

A

AppleID <no-replyojvq3qwq3js@feedbackappld0bi2plpxy8cacjbs.com>
Tue 24/09/2019 3:24 AM
customer@live.com

Apple ID Locked

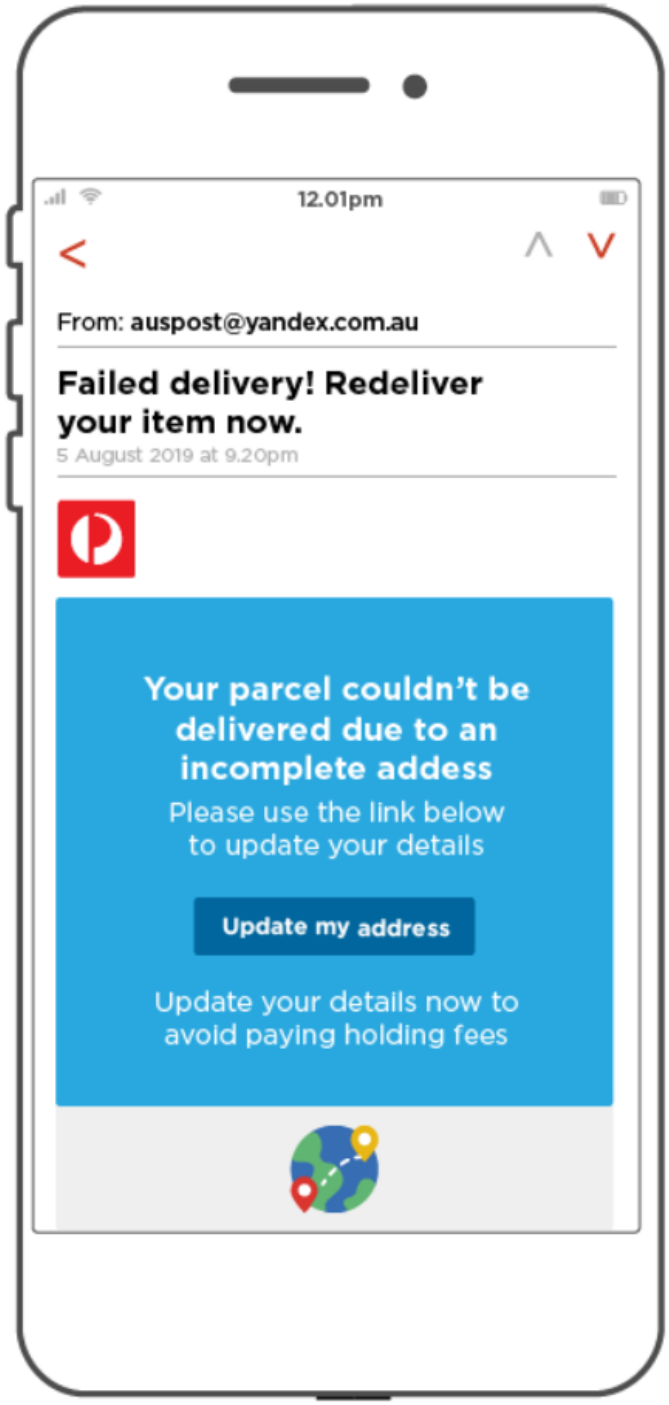
Your Apple ID has been Locked for security reasons. 23 September 2019 , To unlock it, you must verify your identity.

You cannot access your account and any Apple Services, Before completing verification, and you have to completing verification before 12 hours or your account will be permanently Locked.

Unlock Account

Apple ID | Support | Privacy Policy

© 2019 Apple Park California



Quiz:

You've recently purchased something online and are waiting for it to be delivered.

You receive an email about a failed delivery and it's asking you to update your details. Before you click on the link, you carefully consider the email again and realise it's a scam.

What are the five signs that this email is a scam?

From: **auspost@yandex.com.au**

Failed delivery! Redeliver your item now.

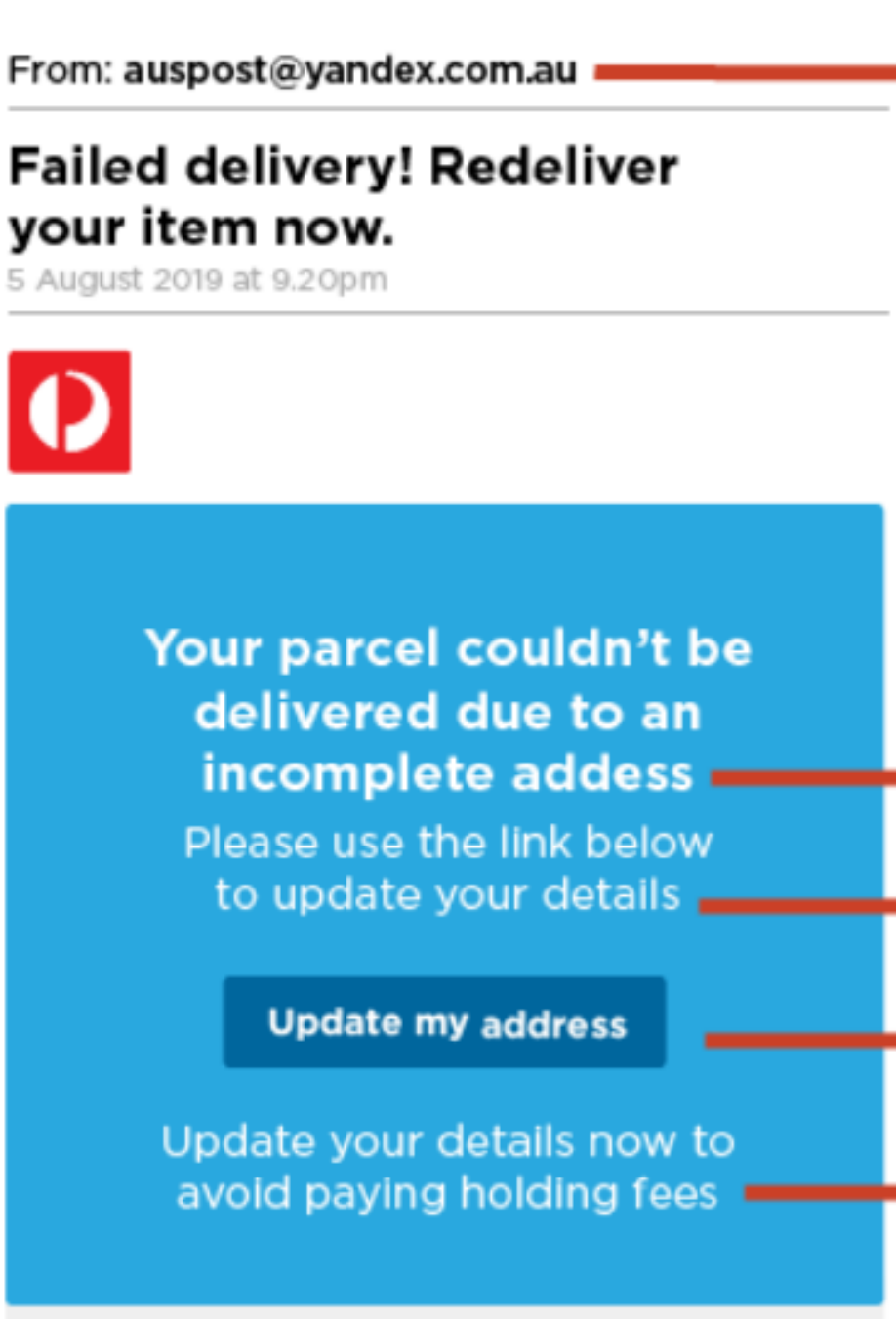
5 August 2019 at 9.20pm

Your parcel couldn't be delivered due to an incomplete addess

Please use the link below to update your details

Update my address

Update your details now to avoid paying holding fees



1. You can't confirm who it's from
2. It has spelling and grammatical errors
3. It has a request for you to do something
4. It has a malicious link
5. There's a sense of urgency

accc.gov.au

SCAMWATCH

Scams are diverse

Puppy scam

- The dog isn't real.

Wangiri scams

- Do you know anyone who lives on Ascension Island (population 806)?

Inheritance scams

- Scammers will go to great lengths to convince you that a fortune awaits if you follow their instructions.

Lottery Scams

- Facebook lottery, like the dog, isn't real.

.

SCAMWATCH

Key Messages – most important

Call your bank

- Call your bank as soon as you can if you think you've paid a scammer.
- Don't be worried; they won't be annoyed; they get these calls all the time.
- Far better to be safe than sorry.

Staying safe online

- The absence of the lock icon matters; it being there doesn't mean anything.
- Don't enter online competitions that want your credit card details.
- Be careful of new contacts.
- Be careful of existing contacts saying strange things (particularly on Facebook)

Post-scam care

- IDCARE
- VEDA/Equifax credit monitoring
- ATO if applicable

SCAMWATCH

Key Messages – most digestible

- If it sounds too good to be true – it probably is!
- Don't be pressured into making a decision.
- Never send money or give personal information to someone you don’t know.
- Scammers will often ask you to use an unusual payment method.
- If you feel something is not quite right – just hang up or delete the email.
- If you’re not sure – take your time and seek help from someone you trust.

Scam detection

- HaveIBeenPwned.com – to see if your data is in any breaches
- Equifax – to see what credit applications have been in made in your name for free once per year

What to do if scammed

Contact your bank first if you think you have given away compromising details to a scammer**.**

Don’t give up and don’t feel ashamed. Most people have fallen victim to a scam.

Where to report:

- https://www.scamwatch.gov.au/report-a-scam
- 1300 795 995 for bushfire scams only
- https://www.scamwatch.gov.au/get-help/where-to-get-help

Aftercare:

IDCARE is a free, expert service at recovering compromised identities:

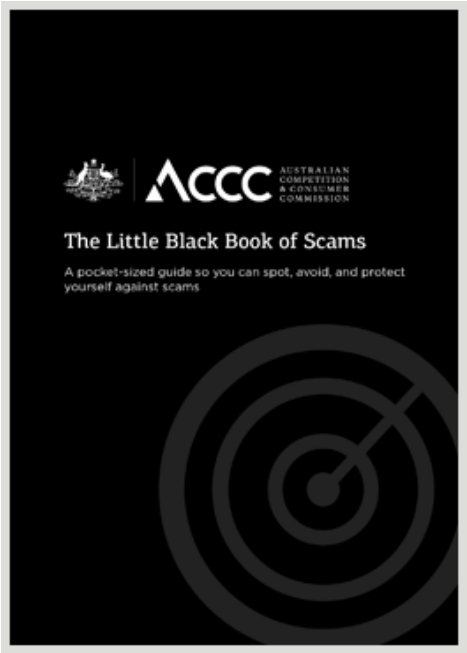
- https://www.idcare.org/
- 1300 432 273 (Mon – Fri 8am – 5pm)

Scam resources

The Little Black Book of Scams

Highlights a variety of popular scams that regularly target Australian consumers and small business and offers guidance on how to protect yourself from scams.

- Physical
- Electronic



Scamwatch Twitter

- @Scamwatch_gov

Scamwatch radar email alerts

- subscribe at www.scamwatch.gov.au

SCAMWATCH

Other very common scams

This list is not exhaustive, but explains some of the main scams Australians are likely to see

- Remote access scams
- Phishing scams
- Online shopping scams

SCAMWATCH

Remote Access scams

Common techniques scammers use

- Remote access scams try to convince you that you have a computer or internet problem.

- The scammer will phone you and pretend to be from a large telecommunications or computer company, such as Telstra, the NBN or Microsoft.

- They'll say there is a problem with your computer or internet, or they'll claim they need your help to catch a scammer.

- The caller will request remote access to your computer to 'find out what the problem is' or to 'help them catch a criminal'.

SCAMWATCH

Remote Access scams

Case study

I was contacted by phone. The caller convinced me that he was working for Telstra and that my internet (IP address) had been compromised. I was to help him by sending money overseas. This trap would catch the 'hackers'. He would deposit money into my savings account. I would then use that money to send overseas via MoneyGram at the local 7-Eleven Store. It was important that I did no internet banking during this time for security reasons. I did this several times until I became suspicious and checked my bank balances. He had been getting cash advances on my credit card and depositing the money into my savings account. I immediately reported to the bank.

Signs this was a scam

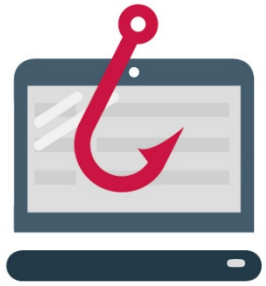
- The victim was phoned out of the blue by a caller claiming to be from a large and trusted organisation.
- The caller claimed the victim's computer was compromised. He also asked for account details and convinced the victim to send money overseas.

Avoid this type of scam

- **Hang up** on the caller.
- **Refuse any request** for remote access.
- **Refuse to provide** personal or bank account information to the caller.
- **Refuse to transfer** money from your account.

SCAMWATCH

Phishing scams



Common techniques scammers use

- You receive an email, text or phone call claiming to be from a bank, telecommunications provider or other business.
- The scammer asks you to update, verify or confirm your details.

Warning signs

- The email or text message does not address you by your proper name.
- It may contain typing errors and grammatical mistakes.
- The website address does not look like the address you usually use and is requesting details the legitimate site does not normally ask for.

SCAMWATCH

Phishing scams (2)

Extortion

- Aug '15 - Emails targeted leaked Ashley Madison customers demanding BTC payment to not notify their spouses.
- Sep '16 - Emails targeted businesses, threatening to perform 'Denial of Service' attacks.
- Dec '18 - Jan '19 - Emails sent out en masse, claiming to be a hitman paid to kill the victim.
- Dec '18 - Emails sent out en masse, claiming to be watching the victim and threatening to detonate a bomb.
- May '19 - Jun '19 - Emails targeted businesses, threatening to leave mass negative reviews.
- Aug '17 - present - Emails sent out en masse, threatening to release compromising adult footage recorded via a hacked webcam.
- Dec '18 - present - Emails sent out en masse, claiming to be a mercenary who would throw acid on the victim.
- Dec ’19 – present – Emails sent out en masse, claiming to have compromising footage of the victim in a hotel room.

SCAMWATCH

Phishing scams (3)

Phorpiex botnet made $115,000 in five months just from mass-spamming sextortion emails

Sextortion emails look silly for the most of us, but there are many users who take them at face value and pay up.

How sextortion emails work

- Spammers will include a victim's previous password.
- They also include the victim's phone numbers in some cases.
- All passwords victims have been quoted were from previous data leaks.
- Phone numbers are from data leaks, or 'consumer leads' lists.
- Can actually see how successful they are paying by looking at the bitcoin wallets on walletexplorer.org

SCAMWATCH

Online shopping scams

Corona Virus

- Expensive ‘medical’ face masks
- Vaccines

Barbeques & Outboard Motors

- Uniquely Australian
- Weberbbqstore.com.au, Bbqdelight.com.au, Weberbbqgrills.com.au.
- Literally dozens of others since 2014.

Online shopping scams (2)

Corona Virus

- Expensive ‘medical’ face masks
- Vaccines

Barbeques & Outboard Motors

- Uniquely Australian
- Literally dozens – getting towards hundreds – of sites since 2014.

Online shopping scams (3)

- airconditionerexperts.com.au
- appliancediscounters.com.au
- appliancespecialists.com.au
- bbqdeals.com.au
- gymsource.com.au
- outboardcentre.com.au
- bbqmaster.com.au
- expertfitness.com.au
- mercurymarineoutboards.com.au
- outboardmarine.net.au
- outboardmarineonline.com.au
- outboardmotors.com.au
- bbqarena.com.au
- gardenoutdoorsales.com.au
- outboardmarineyard.com.au
- suzukioutboardmotors.com.au
- barbecuesales.com.au
- bbqmasters.com.au

- Just one 'batch' of fake online shopping sites targeting Australians from 2017.
- All sites have been removed.

SCAMWATCH

Online shopping scams (4)

What you can do

- Do report to us, but also:
- Report them through your browser to Google and Internet Explorer.
- Report them to Phishtank
- Report them to their domain registrar
- Report them to their hosting provider

- NB: Don’t do this to a legitimate business you are having a dispute with.
- All of these entities will investigate before actioning any change.

SCAMWATCH

Thank you for your time!

Please feel free to ask any questions.