BUSINESS EMAIL COMPROMISE & INVOICE SCAM

Businesses may be targeted by scammers and criminal organisations who enter business systems (through malware or phishing software) to modify or copy genuine invoices. The modified or new invoices are reissued with the scammer's bank details replacing a business's legitimate bank details redirecting payments to the scammer's account.

Be aware that scammers carefully research and monitor their potential victims and will register names, phone numbers and email addresses to closely match the legitimate details.

How to prevent a Business Email Compromise & Invoice Scam:

- Always check the domain name of the business you are receiving emails from – they can easily be disguised or "spoofed" by scammers to look like the real thing.
- Always check payment details directly with a business before paying an emailed invoice, especially if they have changed from previous payments.
- Always contact the business using previously known, or publicly available contact details.
- Never log into a service provider account via a link emailed to you or sent via a text message.

If you have been the victim of business email compromise, follow the steps below as soon as possible:

REPORT TO
Scamwatch.gov.au/report-a-scam
Cyber.gov.au/report

NOTIFY anyone that may be affected, particularly your financial institution.

PROVIDE stakeholders with a warning notice on your website or make personal contact with other potential victims.

Malware or 'phishing software' can be used by scammers to:

- Research or monitor potential individual victims or organisations.
- Record personal information such as your name, phone number, date of birth, email addresses or,
- Record organisational information such as tax file numbers and contact information.

CHECK YOUR INVOICES!

Criminals may be changing your real invoices by modifying payment information.

NSW Police Force

NSW GOVERNMENT

WHAT SHOULD I DO IF I'VE BEEN SCAMMED?

If there is an immediate threat to life or risk of harm please call 000.

NSW Police Force

NSW GOVERNMENT

Has a physical crime been committed?

A physical crime is where a physical item has been stolen, such as your credit or debit card or you have been physically assaulted.

YES

Contact your financial institution to report stolen cards. Then report the incident to your **local Police Station** in person or call the **Police Assistance Line on 131 444.**

NO

Have you suffered a financial loss, or been the victim of online abuse?

A financial loss is where you have had money or assets like cryptocurrency stolen.
Online abuse is behaviour that has threatening, intimidating, harassing, or humiliating effect on a person.

YES

Contact your financial institution immediately. Report the scam in person at your **local Police Station**, over the phone via the **Police Assistance Line (131 444)** or online at **ReportCyber.**
www.cyber.gov.au/report-and-recover/report

NO

Report the scam to ScamWatch.
www.scamwatch.gov.au/

Has your personal information been stolen?

Personal information is anything that can be used to impersonate you.
For example, your name, date of birth, contact details, drivers' licence or other identification credentials that can be used to log into services such as MyGov, email or social media accounts.

YES

Contact ID Support NSW.
www.nsw.gov.au/id-support-nsw

ReportCyber

ScamWatch

ID Support NSW

Triple Zero (000)
For emergencies or life threatening situations.

Police Assistance Line (131 444)
For non emergencies.

Crime Stoppers (1800 333 000)
To provide crime information. It can be in confidence.

HANG UP NOW!

CRYPTO SCAMS

Is someone asking you to send them cryptocurrency?

It's most likely a CRYPTO SCAM

Cryptocurrency ATM's can be used for legitimate reasons, but scammers often use them to steal your money. Once money is converted to cryptocurrency, stolen funds are difficult to recover.

Government organisations or legitimate companies will never ask you to use cryptocurrency ATMs to send money.

Report in person at your local Police Station, over the phone via the Police Assistance Line (131 444) or online at ReportCyber (www.cyber.gov.au/report-and-recover/report)

NSW Police Force

NSW GOVERNMENT

SCAM ALERT

AI DEEPFAKE SCAMS

Artificial intelligence (AI) is the latest technology being used by scammers to deceive individuals into giving away personal information and money.

WHAT ARE DEEPFAKE SCAMS?

Deepfake scams use AI technology to generate videos, voices and images resembling people you may know, prominent international and Australian businesspersons, celebrities, and politicians. The content is used to manipulate people into investing in illegitimate or fake investment platforms, steal personal information or money.

HOW TO SPOT A DEEPFAKE SCAM?

- The origin and/or context of the video are unclear.
- Elements of the video appear to be unnatural such as shadows, lighting, skin tones, mouth movements and facial expressions.
- The video is low resolution.

When watching a video:

- Pay attention to visual and audio inconsistencies – eye movement and mouths.
- Facial expressions look unnatural, mismatched lip-syncing or irregular blinking.

Listening to an audio:

- Pay attention to what they emphasise and when they pause. Often AI voices will emphasise words incorrectly and have inconsistent speeds.
- If you're suspicious of a voice that you know, attempt to get in contact using another method, or ask a personal question that only they would know.

Images:

- Check for distortions around hands and fingers, over blurred or airbrushed faces.

NSW Police Force

NSW GOVERNMENT

PROTECT YOURSELF FROM AI DEEPFAKE INVESTMENT SCAMS:

- Research the legitimacy of an investment firm and/or scheme before engaging with the offer in any way.
- Verify details of the investment with reliable sources before providing any personal information or money.
- Strengthen verification processes – utilise numerous layers e.g. extra ID documents
- Create a family password or PIN - If any family member calls or texts and they're requesting money, requesting you use an unusual app or say they have a new phone number. Ask for the family password or PIN to verify their identity.
- Beware of urgency. Scammers always create a sense of urgency to pressure you into making quick decisions. Take time to validate their details.
- Report any suspicious activity to:
  - » Your local Police
  - » www.cyber.gov.au
  - » www.scamwatch.gov.au
  - » eSafety Commissioner @ https://www.esafety.gov.au

FOR MORE INFORMATION

- Visit the Fraud and Scams - NSW Police Public Site at https://www.police.nsw.gov.au/crime/frauds_and_scams
- Or go to https://www.service.nsw.gov.au/transaction/report-identity-theft-scams-or-cybercrime
- If you believe you have become the victim of a fraud or scam contact your local Police or report at https://www.cyber.gov.au/report-and-recover

NSW Police Force

NSW GOVERNMENT

BUY, SWAP AND SELL SMART

Online marketplaces and social media platforms have become a popular place to buy, sell, share, swap and give away unwanted items. While the vast majority of experiences on these sites are successful and hassle-free, online marketplaces are also popular among thieves and scammers. There are a few tips users should follow to ensure they get the best out of their use of these sites:

- **If it sounds too good to be true, then it probably isn't true,** always use common sense. You should inspect the item carefully in person to ensure it is as described in the ad and any issues are known upfront before you exchange any money.
- **Know who you're dealing with.** If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. It is better to use online sites that you know and trust. Scammers will set up fake online stores or post goods for sale in buyswap-sell groups or online classified sites to trick people into buying items that don't exist.
- For **personal safety** and ease, if possible, you should arrange to meet in a busy public place where there is CCTV. Also, it's a good idea to take a family member or friend with you.
- **Never send money to anyone you don't know.** While online transactions can be simple and convenient, please remember that face to face transactions are the best way to minimise the risk of fraudulent activity.
- When buying or selling an item online, **always transact in person, in public, with cash or through payment methods with buyer protection, such as PayPal or Afterpay.**

A MESSAGE FROM NSW POLICE FORCE

BUY, SWAP AND SELL SMART

PLEASE KEEP THIS IN MIND TO AVOID THE TYPES OF SCAMS LISTED IN BELOW:

- A **scheduled payment receipt** is not a confirmation of money transfer, but a notification of a payment scheduled to be made in the future. This can easily be cancelled by the buyer after goods are exchanged.
- **Oops, I paid you too much!** Buyer's will purposely overpay for an item by cheque and request the overpayment be refunded to them by other means, such as cash. The cheque may appear cleared into your account but can be stopped or refused weeks later. Then you've lost the item, the money from the cheque and the amount you refunded to the scammer. Oops!
- A seller claims that there are **brokerage fees, import duties, or other such fees** required to get an item into the country. Do not pay such fees, as you will most often never get the product and will have lost any money you paid.

OTHER COMMON SCAMS:

Car theft

Be aware when selling a vehicle on online there have been instances where a 'buyer' takes the car on a test drive and never returns or, in an accompanied test drive, forces the owner from the car and steals it.
Always sight buyer's identification and record details before allowing a test drive or access to your vehicle. Have a friend or family member accompany you and the buyer on a test drive. Never leave the buyer alone with access to your car.

Delivery Scam via Whatsapp / SMS

If you receive any Whatsapp or SMS messages from potential buyers offering Gumtree or similar delivery as a service, do NOT click on the link or enter your payment details, this is a scam.

Brand name spoofing / phishing

You get an email/SMS that claims to be from Gumtree, Adevinta, Western Union, or another company and offers buyer protection or an online payment system or perhaps a cash prize. Legitimate companies will never send out such emails. Phishing attempts can also come in the form of emails/SMS messages telling you that your account has been disabled, suspended, locked, or something similar and you are asked to click on a link. Do not click on the link.

SMS Scam

An SMS message from a potential buyer asking you to respond by email is most likely a scam. Legitimate buyers and sellers are unlikely to want to be emailed if they are already texting you.

For more information on how you can protect yourself online, visit the Australian Government's e-safety webiste **https://www.esafety.gov.au/**

or SCAMWATCH online shopping scams **https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams**

NSW Police Force

NSW GOVERNMENT

Triple Zero (000) For emergencies or life threatening situations.

Police Assistance Line (131 444) For non emergencies.

Crime Stoppers (1800 333 000) To provide crime information. It can be in confidence.

Follow us on facebook.com/nswpoliceforce twitter.com/nswpolice youtube.com/thenswpolice **or visit** www.police.nsw.gov.au

REMOTE ACCESS SCAM

NSW Police Force

Scammers impersonate Telecommunication, Computer/Tech, Banking, Investment Companies or Government agencies to gain remote access to your computer via phone, text or email. Genuine companies will never ask for remote access to your online banking.

SCAMMERS MAY USE REASONS SUCH AS:

- Your computer is sending an error message.
- Internet connection problems within your area.
- Your computer has a virus.
- Fraudulent bank account activities have been suspected.

Tricking you into downloading software providing the scammer with full access to your computer and personal information.

PROTECT YOURSELF:

- Never give callers remote access to your computer.
- Never share passwords.
- Never click on unusual links, pop ups or attachments.
- Hang up, call organisations back using trusted numbers from their official website.
- Never provide personal, credit card or online account details over the phone unless you have made the call and it's a trusted source.
- Ensure your computer is protected with anti-virus and anti-spyware software and a firewall. **ONLY** purchase software from trusted sources.

REPORT TO:

Scamwatch **www.scamwatch.gov.au/report-a-scam**

IF SCAMMED:

Contact your bank immediately!

Call Police Assistance Line on **131 444**.

Or report at **www.cyber.gov.au/report-and-recover**

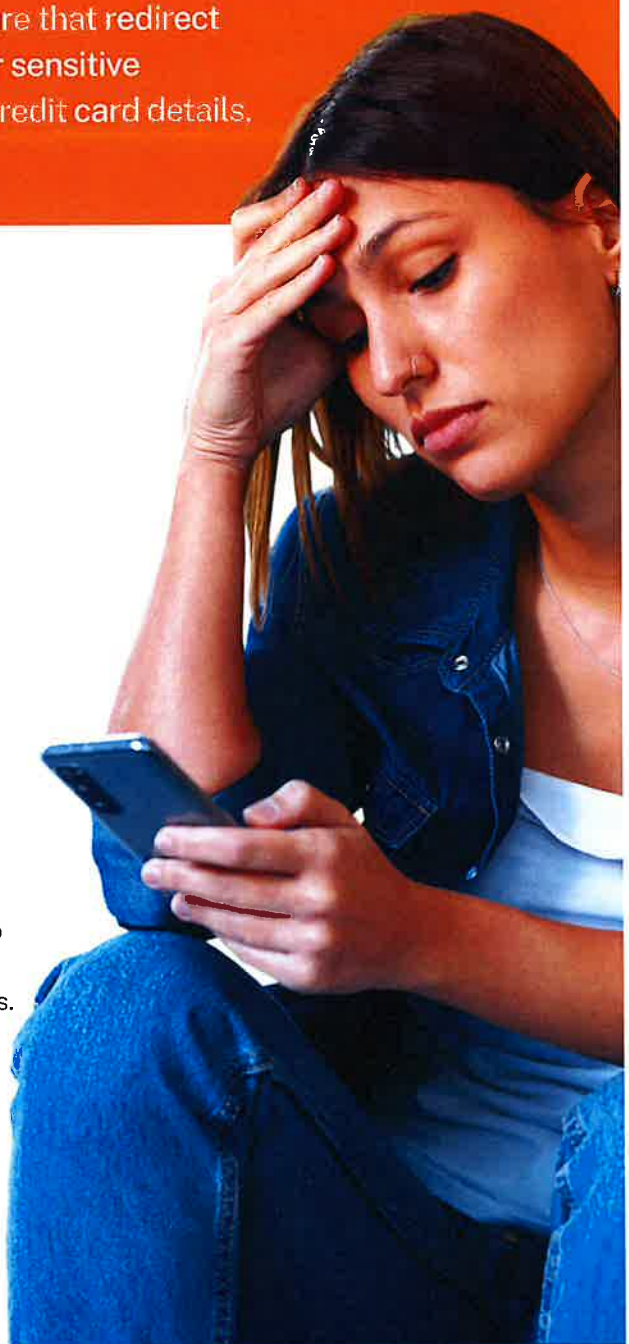
NSW GOVERNMENT

NSWPF/2024/17858

BEWARE of QR CODES

QR codes have become a common place in our lives and unfortunately this has given rise to fake / scam QR codes containing malware and QR enabled '**phishing**' attacks (these attacks are known as 'quishing').

Fake or malicious QR codes may have embedded malware that redirect victims to a 'phishing' (fake) page asking victims to enter sensitive information, such as their name, address, date of birth, credit card details, passwords, photos, and banking/financial details.



Malicious QR codes can also:

- Add an unknown contact to the mobile phone list.
- Connect the victim's device to malicious networks .
- Automatically initiate phone calls, emails and send text messages from your device.
- Reveal the victim's location.
- Enable camera on the device and commence recording.
- Download further viruses and malware to the device which may provide full access to the attacker.

How to safeguard yourself:

- Avoid scanning unnecessary QR codes.
- When scanning a QR code, check the link address to ensure it's a legitimate web page. Scam sites often have hyphens, symbols or misspelt words.
- Be aware of malicious QR codes that might be placed over genuine QR codes in restaurants and public places.
- Be cautious of parking tickets with QR codes which may lead you to fraudulent websites.
- Be cautious of QR codes redirecting you to digital crypto exchanges.
- Think twice before scanning QR codes sent via email, even if they come from organisations and/or people you know.
- Enable multifactor authentication to prevent theft of login credentials.
- Be careful about granting permissions when an app asks as some permissions could be dangerous.
- Install a mobile security app for virus and malware protection to keep your mobile devices safe and secure.

NSW Police Force

NSW GOVERNMENT

What to do if you are a victim:

Report to Police or at **Cyber.gov.au** & **Scamwatch.gov.au**
Contact **esafety.gov.au** for image-based abuse
(sharing or threatening to share intimate images without consent).

Who to contact for help

Bank Orange: 02 6362 4466 **After hours: 1300 705 750**

ID Care – www.idcare.org

MoneySmart – Moneysmart.gov.au

Australian Cyber Security Centre – Cyber.gov.au

ESafety Website – www.esafety.gov.au

ScamWatch – www.scamwatch.gov.au

Lifeline – www.lifeline.org.au

Bank Orange