Advice for Konec customers on phone (call and SMS) scams

Phone scammers cheat tens of thousands of Australians out of millions of dollars every year. The tactics they use are cunning and manipulative and forever evolving. Being aware of how they operate is an important step towards protecting yourself against loss.

Types of scam call fraud risks

Scam callers almost always seek financial gain. Here are some of the methods they use:

- They might try to trick you into making a payment to them or an associate – sometimes under threat of penalty or arrest – or they may be trying to get enough information about you to steal your identity.

- They may try to fool you into giving them remote control of your computer so they can read your emails, banking information or other confidential information. They may install spyware on your computer which gives them access to all that you do on the device, including visibility of logins and passwords.

- If they know enough about you and can pretend to be you, or learn your account passwords, they might steal from your bank account, buy things with your credit card, or obtain new loans and or credit cards in your name.

- A missed call scam is when they scammers ring your phone briefly from a premium rate number – usually masked by a local landline or mobile number – in the hope you'll see a missed call and dial back. When you return the call, the charges for the premium call will be billed to your account. The scammer has arrangements to collect part of those charges at their end.

- Be aware that scammers frequently use technology that masks their own phone number and displays that of a reputable organisation such as a Bank, ATO, Centrelink. This is known as call spoofing and lulls the recipient into a false sense of security. If something seems a bit off, hang up and then call the institution yourself to verify the call/caller.

- Scammers often pretend to be calling from the Australian Taxation Office around tax time seeking information or payment of money, sometimes with the threat of a fine or imprisonment.

- Some scammers resort to threats e.g. they are from a government agency, and you have an overdue fine (that you didn't know about) – and that you'll be jailed if you don't make immediate payment to the account they nominate.

- Recently, scammers have been claiming to be from Customs advising that they are holding a package containing illegal substances that has been addressed to you and that you need to make a payment to release the package and avoid arrest.

- Sadly, scammers impersonate charities and seek donations, especially when a disaster or emergency is in the news.

- Some scammers pretend to be from a parcel delivery company or a well-known online retailer (like Officeworks) and recommend that you click on a link to download certain software to track your parcel deliveries. The software is really giving them access to your computer or phone and can be difficulty to remove.

- Some scammers pretend to be from a parcel delivery company and request payment for a parcel (you didn't order) to be delivered.

- Some scammers call to say you've won a prize and may ask for your account details so they can 'pay' the prize into your account.

- Some scammers work in pairs (or more) – one on the phone/web to your bank or Telco requesting a code to access your account. The other is on the phone to you, claiming to be from your Bank/Telco and requesting the code that's been sent to your mobile so they can discuss a problem with your account. They then steal the money from your bank account or steal your mobile number through a SIM swap.

Fraudsters are always working on new ways to phone scam, so no list is ever complete. But you can keep up to date with the latest scams from official Australian Government resources like:

- www.cyber.gov.au
- www.scamwatch.gov.au. (Subscribe to receive email alerts of scams)
- www.communications.gov.au/what-we-do/phone/unwanted-communications-faqs

The Australian Competition and Consumer Commission's has published 'The Little Black Book of Scams' at www.accc.gov.au/publications/the-little-black-book-of-scams. It's recommended reading.

Blocking suspicious or unwanted calls and SMS

iPhones

- Make sure you've installed the latest version of the iOS operating system and you can 'silence unknown callers' in your phone settings so that any caller that's not in your contacts list will be diverted to voicemail. When this happens, listen to your voicemail and if the call is legitimate, return the call and add the number to your contacts for future calls.

- To block an individual number, go to the recent calls screen and press "i" for a number's "information." There's a block option at the bottom of that screen.

- In the Apple App Store, you'll find several apps that may assist in identifying and blocking scam calls. Use the search term "call blocker" to find some options. Watch for charges and read the reviews before deciding which one to download.

Android phones

- Your recent calls list in the phone app may offer an option to block each number. If you've had calls from a number you don't trust, consider blocking them.

- In the Google Play Store, you'll find several apps that may assist in identifying and blocking scam calls. Use the search term "call blocker" to find some options. Watch for charges and read the reviews before deciding which one to download.

Reducing your risks

Here's how you can protect yourself against SMS and call scams:

Subscribe to the ACCC

- Only share personal information about you with people you trust and be cautious in giving information to strangers.
- Don't share personal information with unknown or unsolicited callers, SMS senders or emailers.
- Your data of birth is a common security question asked of you so be careful who you tell this to. If you tell a scammer, your date of birth, they could answer that security question as if they were you.
- Unless you know who's asking, and why, treat all personal data secret. Personal data includes your name, home address, date of birth, email address, work details, bank details.
- If you think a scammer has taken money from your accounts or is likely to, contact your financial institution immediately so that can block your account or flag it. They may be able to stop a transaction or even reverse it if you act fast. They may be able to temporarily lock a card or account to protect it. Some banks give their customer's the ability to do this via their app or online account.
- You may be able to set up alerts on your bank accounts to notify you of transactions so that you can monitor activity.
- Change default PINs and passwords to personalised ones as soon as you get a new phone or other communications device.
- Choose strong PINS, passcodes and password.
- Whether it's the PIN, passcode or password for your bank account, mobile phone handset, Mobile Phone company, an online store or a health fund, make sure it's not a "weak" one that's easily guessed, associated with you, or worked out by a computer – like "1234" or "0000" or "password", date of birth etc).
- Search the web for "how to choose a strong password" or "how to choose a secure password" for good advice on what makes a secure PIN, passcode or password.
- Change PINs, passcodes and passwords regularly. Don't keep them written down.

- Seriously consider using the "save password" function in web browsers. Whilst this is super convenient, it makes it super easy for a scammer to log into your accounts remotely once they've taken over your device or if they have direct access to it. It's safer, although not as convenient to type your credentials each time you log in.

- Using the same PINs, passcodes and passwords for a long time is a security risk. Sometimes when online stores are hacked, lists of their customer passwords are often sold on the internet. If you changed your password regularly, the password being offered "for sale" may be invalid long before anyone attempts to use it.

- Lock your mobile handset with a secure PIN.

- Set your mobile handset to auto-lock after a brief period of non-use and set it to require a strong PIN to unlock it. Even if your handset also offers face or fingerprint recognition, a weak PIN (like the current year) may open the door for a fraudster.

- Does your mobile phone service or landline offer a "voice mailbox." Voicemail services almost always use a PIN to keep out unauthorised persons, so make sure your PIN is enabled, strong and secure.

- Don't respond to text messages or missed calls from unknown international or Australian numbers, or unknown callers.

- The tricks that scammers play with missed calls are explained above. Text messages asking for a call can be traps in the same way. Don't call back. If the caller is legitimate, they'll leave a message. If you think you know who it may have been, contact them by another means (e.g. email, another phone number on an official website, etc) and check if they called.

- Block suspicious or unknown international or Australian numbers on mobile handsets and use of blocking services or products, where available, on landlines.

- It's explained above how to automatically send calls to voicemail (in some cases). If you can't do that, just don't answer unknown calls. Your own voicemail message might encourage callers to leave a detailed message, so you get enough information about whether to call back.

- If you're not sure about a call you have received, talk about it with someone close to you.

- Don't take computer or phone actions at the request or direction of an unknown caller, unknown emailer or unknown SMS.

- Don't download or install software, visit a web page, click on a link, fill in a web form or open an email at the request of someone on the phone or an SMS unless you're 100% certain of who they are. They could easily be trying to trick you into giving them control of your computer or device or otherwise helping them to scam you.

What to do if you receive scam calls

If you receive a scam call, you should consider taking action:

- by blocking the calling number, as explained above
- by immediately contacting police if you have been threatened or had your property stolen
- by immediately contacting your financial institution, if you believe your account/s have been compromised or you have made a payment to the scammer
- by immediately changing PINs, passcodes or passwords that might be at risk
- by contacting your Telco if you think your number has been ported out or transferred to a SIM card that's not in your possession.
- by reporting the scam call to ScamWatch – an initiative of the Australian Consumer and Competition Commission (ACCC) at www.scamwatch.gov.au

Reporting scam SMS and MMS

You can send SMS and MMS that you think are scams to our network carrier Telstra for review. Their Cyber Security Team will investigate and if it is a scam, they will try to block further messages from that sender entering the network. Here's how you can do this:

From an Android device:

1. Tap and hold on to the message.
2. Tap on the three-dot menu button and hit Forward.
3. Type 7226 (scam) and hit Send SMS

From an iPhone:

1. Touch and hold the message bubble you want to forward, then tap More.
2. Select additional text messages, if desired.
3. Tap Forward and enter 7226 (scam)
4. Tap Send