# Are you a victim of a scam or fraud?

Bank Orange

Signs your account may have been impacted or compromised.

"I am restricted when trying to send or receive funds."

“I have received a message for a One-Time Password that I did not request.’

“I received a message to confirm a transaction I did not do.”

"I've noticed unusual activity."

"There is a problem with my card."

"I can't access my Internet Banking."

## What should I do if I believe I may have been scammed?

If you are concerned your card has been compromised, you can log into your Internet Banking or Mobile App and temporarily lock your cards.

**Contact Team Orange on (02) 6362 2666**

Team Orange may be able to stop a transaction or freeze your account or card while the matter is investigated.

**Contact Vigil Fraud Monitoring on 1300 705 750**

Vigil is our partner in managing Card or New Payments Platform Fraud, including Osko. The team at Vigil monitor transactions to reduce the risk of scams and fraud. If you are having issues with sending/receiving funds, card transactions, or NPP transactions, Vigil will be able to assist. Your transaction history may be reviewed to verify any suspicious activity.

## Have you tried contacting the merchant?

In most cases, the quickest way to get a refund is to contact the merchant and request a full refund, advising that this was an unauthorised transaction on your card or account. Team Orange will assist you with this process.

## Recovering your identity.

If you suspect you are a victim of identity theft, it is important that you act quickly to reduce your risk of financial loss or other damages.

**Contact ID Care on 1800 595 160**

ID Care is a free government service which will work with you to develop a specific response plan to your situation and support you through the process.

## Reporting scams to the authorities.

We encourage you to report scams to the following organisations to help them warn the community and take action to prevent future scams.

**NSW Police** (non-emergency line)
131 444

**Australian Cyber Security Centre**
cyber.gov.au/csc/report

Do not disclose your card details over email or phone. Most places should be able to locate your transaction with just the first and last 4 numbers on your card.

# Bank Orange will do what we can to help, however in most cases recovery is unlikely.

**Counselling and support services are available.**

**National Debt Helpline**
1800 007 007

**Beyond Blue**
1300 224 636

**Equifax (Credit Ban)**
138 332

**National Elder Abuse Hotline**
1800 353 374

**1800RESPECT**
1800 737 732

**Illion**
132 333

**Lifeline**
13 11 14

**Ask Izzy**
askizzy.org.au

**Experian**
1300 783 684

## Tips to protect your account.

### Monitor transactions.

Regularly check your account transactions. This can reduce loss and increase chance of recovery the sooner it is identified and reported. A great way to do this is through our Mobile App. Talk to our team today.

### Do not use common passwords.

Avoid using common dates or phrases such as, your birthday, anniversary, 'password', your city, street or pets' names. Use a combination of letters, numbers and special characters.

### Hang up on unsolicited phone calls.

If a caller claims to be from a company or organisation you have dealings with, call the company on a verified number or go to your local branch/store.

### Do not allow remote access.

This includes all online devices, i.e. computer, tablet, or phone. Never be tricked into installing software that will unknowingly allow them access to 'fix' something on your computer, which they will then use to access your Internet Banking.

### Do not open unknown attachments.

If you receive an unexpected invoice, photos or attachments from an unknown sender, it may contain a virus. Note that these scams often come from users that you do know. Do not forward these emails.

### Do not click on unknown links.

These can be sent by either text or email and may contain a virus. If you know the sender of the link, confirm with them that it is safe to open. If the link is from an unknown number or spam account, block the number from contacting you in the future.

**Do not disclose your password to anyone.**

Bank Orange and service providers such as Australian Government and telecommunications companies will not ask you for your login or password. If you wish to give an additional contact access to your account, contact Team Orange to set a family member to be an authorised account user. This is strongly recommended over sharing your login credentials.