Tips for phone and internet consumers

Telecommunications Industry Ombudsman

Tips to help consumers protect their account from fraudsters

Make your phone or internet account as secure as possible

- **Use strong passwords**. Never use the same password for multiple accounts. Consider using password management software instead of storing them in text.
- **Ask your provider about the availability of extra security.** One example is Multi-Factor Authentication.

Limit the amount of personal information available in the public domain

- **Put your social media on private**, so personal information about you cannot be viewed by the public.
- **Lock your mailbox** to reduce the chances of bills or other letters containing your personal information being stolen.

Make sure you're really speaking with your provider

- **If someone calls you offering you a deal that seems too good to be true**, consider ending the call, looking up your provider's phone number, and calling directly to enquire about the deal.
- **Familiarise yourself with how your provider normally communicates with you**, so you can know what to look out for.
  - Sometimes SMSs and emails from fraudsters may have spelling and grammar errors, unfamiliar links, or strange formatting.
  - Other times, they may look genuine and even include company logos, but may ask for information that the real company would not ask for.
- **If you're unsure whether you are speaking to your provider, hang up and contact your provider directly.** For example, most providers do not call consumers to ask for one-time codes that have been sent to the consumer.

Report any strange activity to your provider immediately

- **If your provider sends you a notification saying you have changed your account details or made a new order, and you did not authorise any changes,** this could mean someone recently attempted to fraudulently access your account.
- Contact your provider as soon as possible.

What to do if you think you've fallen victim to fraudulent account access

- Report the fraud to your local police, IDCare, and your provider.
- If money has been taken from your bank account, contact your bank.
- If products or services have been added to your phone or internet account, contact your provider.
- Further information about hacking, identity theft, phishing, and remote access scams can be found at the ACCC's ScamWatch (www.scamwatch.gov.au).

When you can complain to us

We can handle complaints about your phone or internet provider, where your telco account has been accessed fraudulently and you cannot resolve the issue with your provider.

We cannot handle complaints about fraudsters or scammers and their behaviour. However, you can report their behaviour to ScamWatch or the police.

tio.com.au
1800 062 058 (free call)