

Account Security and Scam Protection Policy

How we protect your account and number, and how to spot a scam.

Effective date: 1 November 2026 · Version 1.0

FlixLink · Flixlink Broadband Pty Ltd, ABN 44 669 575 679 · (02) 9071 2900 · info@flixlink.com.au · flixlink.com.au

This policy explains how FlixLink protects you, your account and your phone number from scammers, including people who pretend to be us and people who try to take over your mobile number or account. It covers how we check your identity before important changes, how we tell you about those changes, how we will and won't contact you, how number transfers work, what to do if your phone is lost or stolen or your number stops working, how we block scam calls and texts, how to report scams, and how Triple Zero (000) works on your mobile.

1. About this policy

This policy is published by Flixlink Broadband Pty Ltd (ABN 44 669 575 679), trading as FlixLink Telecommunications ("FlixLink", "we", "us", "our"). It applies to all our customers and services, including nbn® broadband, mobile, voice and business services.

It explains how we meet these rules:

- Telecommunications Service Provider (Customer Identity Authentication) Determination 2022
- Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
- Industry Code C661:2022 Reducing Scam Calls and Scam SMSs
- Telecommunications (SMS Sender ID Register) Industry Standard 2025
- Telecommunications (Emergency Call Service) Determination 2019.

Please read it with our Customer Terms and Privacy Policy. If you're affected by domestic, family or sexual violence, our Domestic, Family and Sexual Violence Support Policy explains extra ways we can keep you safe. If the two policies differ, the support policy applies.

We'll update this policy when the rules or our processes change.

2. How we check it's really you

Before any high-risk transaction on your account, we use identity authentication processes to confirm that the person asking is you or your authorised representative. This protects you from high-risk transactions you didn't authorise.

2.1 When you sign up

- **Mobile:** you complete our application form, and we check your photo ID on a video call before we activate your service.
- **nbn® broadband ordered online:** you pay by card through our secure Stripe checkout, and we email your order confirmation to you.
- **Business, voice and managed services:** you order through our quote and order form.

2.2 What we treat as high-risk

- swapping your SIM or reissuing your eSIM
- moving (porting) a number to or from FlixLink
- changing your contact details, such as your phone number, email or address
- changing your password or other account security details
- adding or removing an authorised representative
- giving out your personal information or account details, such as your account number
- adding a new ongoing charge, or a large one-off charge, to your account
- anything else that could make you lose access to your service.

2.3 How the check works

1. We ask you to confirm some details about you and your account.
2. We send a one-time code by SMS to the mobile number on your account, or by email to the email address on your account.
3. You give us the code to confirm it's you.

Our message will say that a high-risk transaction has been requested, that you shouldn't share the code with anyone except us when you've contacted us, and what to do if you didn't ask for it.

Only give a code to us, and only if you contacted us or you asked us to move your number. If you get a code you didn't ask for, don't share it with anyone, and call us on (02) 9071 2900.

2.4 If you can't receive the code

If you can't get the code, for example because your phone has been lost or stolen, a trained team member will check your identity another way, such as by checking your identity documents. When we do this, we'll send a notice to your other contact details (for example, your email) to let you know.

If your situation makes the usual checks unsafe or impossible, tell us. This could be because you're affected by domestic or family violence, you've been through an emergency, or you're overseas and have lost your phone. A trained team member can use other ways to confirm it's you.

2.5 If you can't pass the check

We won't go ahead with the transaction. We'll explain what else you can do to confirm who you are. If we think someone is pretending to be you, we'll contact you using the details on your account.

2.6 Identity checks are free

We never charge for identity checks, one-time codes, notices about your account, or the extra fraud protection in section 8.2. We keep records of our identity checks for at least one year, as the rules require.

3. How we tell you about high-risk changes

When a high-risk transaction happens on your account, we'll tell you before or straight after it, by SMS or email to the contact details on your account. If the change was to your contact details, we'll also tell you at your previous contact details. The notice will say what was requested and what to do if it wasn't you.

If you get a notice about something you didn't ask for, call us straight away on (02) 9071 2900. If someone made a change without your permission, we'll reverse it or fix it, tell you what we've done, and explain how to protect your account.

If you're affected by domestic or family violence, you can ask us not to send these notices, for example because someone else can see your messages. If you ask, we won't send them, and we'll agree a safe way to keep you informed instead.

4. How we contact you, and how to check it's really us

We may contact you by phone, email or SMS, using the contact details on your account, about things like your order, a payment, a fault or a change to your service.

4.1 We will

- email you only from addresses ending in **@flixlink.com.au**. Payment receipts may also come from **Stripe**, our payment provider.
- send payment links only from an @flixlink.com.au email address. Our payment pages are hosted by Stripe and show FlixLink's name.
- ask you for a one-time code only if you contacted us, or you asked us to move your number.

4.2 We will never

- ask for your full card number, your passwords or your online banking login, by phone, email or text
- ask you to pay with gift cards or cryptocurrency, or tell you our bank details have changed
- call you out of the blue to say your internet has been hacked, or ask for remote access to your computer or phone.

4.3 How to check a message or call is really from us

1. Don't click links, open attachments or call numbers in a message you're not sure about.
2. Check the sender. Our emails come from @flixlink.com.au. Scammers can make a caller ID, text or email look like it's from us, so a familiar name or number isn't proof.
3. Contact us using the details on our website, not the details in the message: (02) 9071 2900 or info@flixlink.com.au.
4. If a call seems odd, hang up and call us back on (02) 9071 2900.

We've set up email authentication (SPF, DKIM and DMARC) on flixlink.com.au. This helps email providers spot and block fake emails that pretend to come from our address. No system is perfect, so still check before you act.

Card payments are processed by Stripe. We never see or store your full card number.

5. Moving your mobile number (porting)

5.1 Moving your number to FlixLink

An additional identity verification process will be used to verify the identity of the person making a porting request.

Before we move a number to FlixLink, we send a one-time code by SMS to the number being moved. The transfer only goes ahead once you've confirmed you received the code. This shows that the person asking has the phone that uses the number. The SMS is free. If you can't receive the code, we'll check your identity using identity documents instead.

You also give us your authority to transfer the number in your mobile application form.

5.2 Moving your number away from FlixLink

Your new provider must verify your identity before moving your number, usually by sending a code to your phone. If you ask us for details you need for the transfer, such as your account number, we'll check your identity first. When the transfer is complete, your FlixLink service for that number ends (see our Customer Terms).

5.3 Warning signs that someone is taking your number

Scammers try to move your number to a SIM they control, through a fake SIM swap or number transfer. They then get your calls, texts and security codes, including codes from your bank. Watch for:

- your phone suddenly showing **No service** or **SOS only** where it normally works
- a text, email or call about a SIM swap, eSIM, number transfer or code that you didn't ask for
- people telling you they can't reach you
- alerts that the password for your email, bank or another account has changed, or you're suddenly locked out
- someone who says they're from FlixLink or another telco and asks you to read out a code or "confirm" a transfer.

5.4 If you think your number has been taken

If you suspect a fraudulent transfer or SIM swap, act straight away:

1. **Contact us** on (02) 9071 2900 from another phone, or email info@flixlink.com.au.
2. **Contact your bank** and any other financial services providers.
3. **Report it to the police.** You can make an official police report online through ReportCyber, or call the Police Assistance Line on 131 444. In an emergency, call 000.
4. **Get support.** Contact IDCARE on 1800 595 160 for free help with identity theft and scams, and report it to Scamwatch.

If your number was moved or swapped without your permission, we'll work with you, and with the other provider if needed, to get it back to you as quickly as we can.

6. If your phone is lost or stolen, or your number suddenly stops working

6.1 What to do

1. **Contact us straight away.** Call (02) 9071 2900 from another phone, or email info@flixlink.com.au at any time.
2. **We'll suspend your service** so no one else can use it. We'll check it's you first. If you can't receive a code, see section 2.4.
3. **Protect your other accounts.** Change the passwords for your email, banking and other important accounts. If your phone had banking apps, tell your bank. If you can, use your phone maker's device-finding service to lock or erase the phone.

4. **If it was stolen**, report it to the police.

5. **Get a replacement SIM or eSIM** once we've confirmed your identity. We'll then restore your service.

If your number stops working but you still have your phone, it could be SIM-swap or porting fraud. Follow the steps in section 5.4.

6.2 What you pay

- **After you tell us:** you don't pay for calls, texts, data or roaming used on the service after you first contact us, by phone or email, to report it lost or stolen. This applies even if we haven't finished suspending it.
- **Before you tell us:** charges for use of your service are your responsibility, because we can't know your phone is missing until you tell us. That's why it's important to contact us quickly. You don't pay for use caused by our mistake, or by fraud we should reasonably have prevented.
- **Unusual charges:** if someone else ran up unusual charges before you told us (such as extra data, roaming or international calls), tell us. We'll look at what happened with you, and we may reduce or waive those charges.
- **Suspending is free.** Your plan charges continue as normal while your service is suspended, so you keep your number. If you'd rather cancel, see our Customer Terms.
- **Replacement SIM or eSIM:** \$9.24, the same price as a new SIM or eSIM (eSIM is available on 5G plans). It's free if you need the replacement because of our mistake.

If paying is hard, our Financial Hardship Policy can help.

7. Authorised representatives

You can name someone you trust (an authorised representative) to manage your account for you. They can make changes and get information about your account, so choose carefully.

- Adding or removing an authorised representative is a high-risk transaction. We'll check your identity first, and tell you afterwards.
- Your authorised representative must pass the same identity checks as you before we make any high-risk transaction they ask for.
- You can remove an authorised representative at any time.
- If someone has legal authority to act for you but isn't listed on your account (for example, under a power of attorney or a guardianship or financial management order), a trained team member will check their documents before we deal with them. We'll let you know when we do, unless you're affected by domestic or family violence and have asked us not to.

8. Keeping your account and devices safe

8.1 Simple steps that help

- Keep your personal information private. Don't give it to people who contact you unexpectedly.
- Use strong, different passwords or passphrases for your email, banking and other important accounts. Change them if you think someone knows them.
- Turn on two-step verification for your email and banking. Where you can, use an authenticator app rather than text-message codes, so a stolen number can't be used to get into your accounts.
- Lock your phone with a PIN, password, fingerprint or face recognition.

- Set a voicemail PIN and keep it private.
- Change the default PINs and passwords on new equipment, such as modems and phone systems.
- Keep your phone and computer software up to date.
- Keep your contact details up to date with us, so our codes and notices reach you.
- Watch your usage alerts. On mobile plans, we send free alerts when you've used 50%, 85% and 100% of your included data, which can help you spot unusual use.
- **Business phone systems:** change default passwords, turn off features you don't use (such as remote call forwarding), close unused ports, and restrict international calling if you don't need it.

8.2 Extra protection if you're at risk

If you think you're at risk of fraud, ask us for extra protection. For example, your details may have been exposed in a data breach, or someone may have tried to get into your accounts. We can flag your account, add extra checks, pause some high-risk transactions on your account, or send notices to your authorised representative. This is free.

9. What we do about scam calls and texts

We follow the industry code Reducing Scam Calls and Scam SMs (C661:2022). Under the code, telcos, including us and the networks we use, work to identify, trace, block and otherwise disrupt scam calls and texts. This means:

- many scam calls and texts are blocked before they reach you
- we don't let our customers make calls or send texts using a phone number they don't have the right to use
- if we find a FlixLink number is being used to make scam calls or send scam texts, we may block that number or disconnect the service.

No system catches every scam, so some will still get through.

9.1 Common scams

- calls, texts or emails pretending to be from a telco, bank, government agency, delivery company or toll road, asking you to click a link, pay, or give personal details
- calls saying your internet has been hacked, then asking for remote access to your computer
- requests to read out a one-time code
- texts from an unknown number claiming to be a family member with a new phone who needs money
- missed calls from unknown overseas numbers, designed to get you to call back at a high cost.

9.2 Blocking unwanted calls and texts

- Don't call back numbers you don't recognise. Let unknown calls go to voicemail, then decide whether to return them.
- Don't click links or call numbers in suspicious texts.
- Block suspicious numbers on your phone. Most phones can also filter or silence calls and texts from unknown senders. Check your phone's settings.
- If you have a FlixLink home or business phone service and get scam calls, contact us. We'll tell you what call-blocking options are available for your service.

10. Branded texts and the SMS Sender ID Register

Some organisations send texts that show a name (a "sender ID") instead of a phone number, such as a bank's name. Scammers copy these names to make fake texts look real.

The Australian Communications and Media Authority (ACMA) runs the SMS Sender ID Register. Since 1 July 2026:

- **texts with a registered sender ID** are delivered showing the organisation's name
- **texts with a sender ID that isn't registered** are relabelled **Unverified**, and grouped together in an "Unverified" conversation on your phone.

What this means for you:

- Treat any text labelled **Unverified** with extra care. Don't click its links or call its numbers.
- If a text says it's from FlixLink but is labelled Unverified, don't respond. Contact us using the details on our website.
- The register only covers texts that show a name. Scam texts can still come from ordinary phone numbers, and a familiar name is no guarantee. Always check before you click.

We'll also send this information to our mobile customers when they join, and at least once every three months.

11. Reporting scams, spam and fraud

If you suspect fraud on your FlixLink service or account, report it immediately to us and to your bank or other financial services provider.

What happened	Who to contact
You've lost money, or shared your card or bank details	Your bank or card provider, straight away
Someone has used your FlixLink service or account, or pretended to be us	FlixLink: (02) 9071 2900 or info@flixlink.com.au
Your number was moved or swapped without your permission	FlixLink, then the police and IDCARE (see section 5.4)
You've seen or been targeted by a scam	Scamwatch
Cybercrime, such as hacking, online fraud or identity theft	ReportCyber (an official police report), or the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371)
Your identity has been stolen or misused	IDCARE: 1800 595 160 (free)
Spam texts or emails (unwanted marketing)	ACMA: see dealing with spam, or make a spam complaint
You need the police	000 in an emergency, or the Police Assistance Line on 131 444
You're unhappy with your bank's response to a scam	Australian Financial Complaints Authority

What happened	Who to contact
You need someone to talk to	Lifeline: 13 11 14

12. What we may do if we suspect fraud

To protect you and others, we may:

- pause a transaction, such as a SIM swap, eSIM, number transfer or account change, while we check it
- ask for more identity checks
- contact you using the details we had before any recent change
- reverse a change you didn't authorise
- suspend a service, or block a number, to prevent harm, for example if your number appears to have been taken over, or a FlixLink service is being used for scam calls or texts.

We'll tell you before we act, in a way that's safe for you. If we need to act straight away to prevent harm, we'll tell you as soon as we can afterwards. We'll explain why and what you can do. If we got it wrong, we'll restore your service quickly, at no cost to you. We don't charge for these protections.

If you've told us you're affected by domestic, family or sexual violence, we won't restrict, suspend or disconnect your service for 30 days after you first raise a safety concern with us (or a longer period we agree with you), unless you ask us to. See our Domestic, Family and Sexual Violence Support Policy.

13. The Scams Prevention Framework

The Scams Prevention Framework is a law (Part IVF of the Competition and Consumer Act 2010) that sets obligations for businesses in designated sectors to prevent, detect, report, disrupt and respond to scams. Banking, telecommunications and some digital platforms are the first designated sectors. The telecommunications sector was designated in May 2026. The detailed rules for telcos are still being finalised.

We support the Framework. We'll meet its obligations as they apply to us, and update this policy when they do. Until then, we follow the scam protection rules described in this policy.

14. Triple Zero (000) and your mobile

In an emergency, call **Triple Zero (000)**.

- **Before we connect your mobile:** your application form asks for your phone's make and model. We check that your phone can call 000 on the mobile network we use, and on other mobile networks if ours isn't available. If it can't, we'll tell you, we won't connect our service to that phone, and we'll give you information about other phones that can call 000, including low-cost and no-cost options.
- **While you're with us:** if we find your phone can no longer call 000, we'll tell you within 5 business days. We'll send you two more notices. If you're still using that phone, we'll stop supplying our service to it between 28 and 35 days after our first notice. Before we do, we'll give you information about phones that can call 000, including low-cost and no-cost options.
- **If you can't afford a phone:** our Financial Hardship Policy explains at least one way to get a low-cost or no-cost phone that can call 000.

Other emergency numbers:

- **112** works from digital mobile phones, even without a SIM, as long as there's coverage from at least one network. It has no advantage over 000.
- **106** is for people who use a TTY (text telephone).

nbn® and internet phone services, including nbn® Voice, won't work in a power outage unless you have a battery backup. Keep a charged mobile phone for emergencies.

15. Complaints

If you're unhappy with how we've handled a security or scam issue, please tell us. Our Complaint Handling Policy explains how we handle complaints. If you are not satisfied with how we have handled your complaint, you have a right to take it to the Telecommunications Industry Ombudsman, which is a free and independent service. You can contact the TIO on 1800 062 058 or at tio.com.au.

16. Contact us

- Phone: (02) 9071 2900
- Email: info@flixlink.com.au
- Website: flixlink.com.au
- Help: Support and Contact us. Our support hours are 9am to 6pm, Monday to Friday (Sydney time).
- Flixlink Broadband Pty Ltd (ABN 44 669 575 679), trading as FlixLink Telecommunications

nbn® is a trade mark of NBN Co Limited.