# ING's Pocket Guide to Scam Prevention

## Spot scams before they find you.

## Three easy steps to avoid scams

### 1. STOP

**Before sharing any money or personal info, take a breather to assess whether you really know or trust who's asking.**

If it feels off, it probably is. Even if it feels safe, always take a moment to gauge whether a scammer is trying to get in touch. Scammers will offer to help you or ask you to verify who you are. They will pretend to be people or organisations you know and trust, like your bank.

### 2. REFLECT

**Ask yourself, "Could this website, message or call be fake?"**

Check the website address being mindful of lengthy or foreign URLs. Avoid clicking on any links right away or actioning a request over the phone. If in doubt, say no, hang up, or swipe the message away, then contact the business or organisation using the contact information from their official website or through their secure apps.

Signs to watch out for:

- **You feel pressured to act fast.** Scammers don't want you to take your time and think things through. They use techniques designed to catch you off guard and rush you, either saying if you don't act now, you'll miss out, or threatening that something bad will happen.
- **They ask you to pay in unusual ways.** If a person asks you to pay with preloaded debit cards, or iTunes cards, chances are it's a scam. Once this money is spent, you can't get it back.
- **The message contains links or attachments**. Never automatically click a link or attachment you receive via email or text. Scammers try to catch you off guard and send you to scam websites designed to steal your information and money.

### 3. PROTECT

**Don't wait to act if things seem fishy.**

Contact your bank if you notice unusual activity or if a scammer gets your money or information, then report the scam to ReportCyber. Visit the ING security page for more information.

ING is a business name of ING Bank (Australia) Limited ABN 24 000 893 292, AFSL and Australian Credit Licence 229823.