

When it comes to phishing (or fraudulent) emails, you don't want to end up as someone else's "catch of the day".



Email phishing takes place when a fraudster sends an email that looks like it's come from a legitimate business like your bank, eBay or even iinet. By creating a sophisticated email complete with official looking logos, these documents are designed to trick you (or your family) into disclosing account details, passwords and other personal info.

In the real world, any genuine organisation would never expect you to send personal information over an email. Nearly all online shops and services use an email identity check process that doesn't involve passwords - meaning they'll never ask for yours.

To stay one step ahead of information hijackers, run through our tips below to keep your private business, well... private.

Beware of the bait

Most phoney emails contain one (or more) of the following:

- A generic greeting addressed to the "Account Owner".
- A reason. This is where they convince you that you need to share your personal information - it's for your own good.
- A call to take urgent action. It's common to see phishers preying on fear. For example, you'll lose your account or money if you don't do what they say.
- Shoddy looking text. The email might contain tell-tale signs like spelling typos or bad grammar.

Do a little detective work

A classic ploy used by scammers is to scare readers into giving up personal info and passwords. Keep your cool and remember the following:

- Go to the source. Visit the company's official website, rather than following any links in an email. Login as you normally would and suss out any media releases or similar announcements.
- If you're still unsure, ring the organisation or visit your local branch to see if they know what's going on.
- Bookmark the Government's **SCAMwatch** site at www.scamwatch.gov.au. Here you can read up on scams and check what's on the radar.

Phishing in many forms

Phishing isn't always done over email. Some users get caught out clicking through everyday websites like Facebook, or are duped over the phone.

- Remember, organisations like iinet and Microsoft don't make uninvited phone calls offering to fix your computer or to sell you software.
- If you're dubious about a phone call, offer to call the company back. Use their number listed in the phone book, or if it's a bank, use the number listed on the back of your credit card or statement.
- Report the scam to the Australian Communications and Media Authority (ACMA). Email report@submit.spam.acma.gov.au and help others to avoid being conned.

We're only human

Sometimes we make mistakes. If you've accidentally revealed info to someone who you think might not have your best interests at heart, act quickly:

- Change your passwords and pin numbers. Update any accounts that you think might have been compromised.
- Contact your bank directly to place a fraud alert on your credit reports.
- Review your bank and credit card statements for unexplained charges. If there's anything out of the ordinary, report these immediately to your bank
- Be on the look out for anything suspicious over the next 12 months. Missing snail mail, application forms for products or services you haven't asked for, or being refused credit are all signs that you may be a victim.
- Spread the word - share your experience with your family and friends to avoid it happening to them.

Pick up more hints and tips from **iiNet's Online Safety Series** from iinet.net.au/safety.

