# SECURITY GUIDE

With internet use on the rise, cybercrime is big business. Computer savvy hackers and opportunistic spammers are constantly trying to steal or scam money from internet users. PayPal works hard to keep your information secure. We have lots of security measures in place that help protect your personal and financial information.

## Here's how to get a security key

**1.** Log in to your PayPal account at www.paypal.com.au

**2.** Click **Profile** then **My settings**.

**3.** Click **Get started** beside "Security key."

**4.** Click **Get security key** and follow the prompts.

### PayPal security key

This provides extra security when you log in to PayPal and eBay. When you opt for a mobile security key, we'll SMS you a random 6 digit code to enter with your password when you log in to your accounts. You can also buy a credit card sized device that will generate this code. Visit our website and click Security to learn more.

### Website identity verification

If your web browser supports an Extended Validation Certificate, the address bar will turn green when you're on PayPal's site. This means the website is secure. If the address bar of a webpage turns red or yellow, the site is not secure. Check your browser's website to see if an Extended Validation Certificate is supported.

### Dedicated security staff

PayPal has staff dedicated to identifying and stopping unauthorised or suspicious transactions. We also have a team trained to answer your phishing questions and to support government and security agencies in tracking down scammers.

### Encryption

When you communicate with PayPal online or on your mobile, the information you provide is encrypted. This means it can only be read by you. A padlock symbol is displayed on the right side of your web browser to let you know you are viewing a secure web page.

### Automatic timeout period

If you're logged into PayPal and there's been no activity for 15 minutes, we'll log you out to help stop anyone from accessing your information or transferring funds from your accounts.

### Email authentication

PayPal authenticates all its outgoing emails. This allows participating email providers to confirm that an email claiming to be from PayPal is actually from PayPal. While you may not see any difference between a true and fake email, your email providers can spot unauthenticated emails and move them to your spam folder or stop them being delivered to you.

PayPal™

# Common internet annoyances

## If you think you have received a phishing or hoax email or SMS

- Don't respond.
- Don't click on any links.
- Don't open any attachments.
- Don't enter any information.
- Send it to phishing@paypal.com.au
- Delete the email.

## Phishing and scam emails

Phishing emails and SMSs are attempts to fish or "phish" for information so cyber criminals can steal your money or identity.

- They look similar to genuine emails from businesses you're already familiar with.
- They ask you to click on links or attachments to update your personal or financial information or confirm your password.

Visit www.paypal.com.au and click **Security** to learn how to identify phishing emails.

## Computer viruses and Trojans

Links and downloads in phishing emails often contain viruses or Trojans which infect your computer. Trojans are malicious programs attached to software that allow scammers to control your computer by remote access. They can see and record everything you enter.

# Protect yourself when buying and selling online

## Keeping your accounts safer

- Make sure you have a secure password:
  - Use a mix of upper and lower case letters and numbers.
  - Don't use your name, birthday or everyday words.
  - Use a different password for each site you use.
  - Never write your passwords down or share them with anyone else.
  - Don't click on the 'Remember Me?' option in your internet browser. A browser that remembers your password leaves you vulnerable to identity theft and financial fraud.
  - Never enter personal or financial details, including passwords, in response to an unsolicited email, even if it looks legitimate.
- Visit websites by typing the full address into your internet browser's address bar.
- Don't put financial or personal information (e.g. your birthdate) on social networking sites.
- Always log out of sites you have entered personal information into. Closing the browser is not enough.
- Make sure the website you are on is genuine:
  - Does it have the right URL address?
  - Does the business logo look right?
  - Is the spelling and grammar correct?

## Selling

- Ensure there's nothing in the background of your item's photos a scammer could use to identify you.
- Research your buyer's reputation when selling on a marketplace like eBay.
- Check your buyer's address and contact information.
- Consider setting up a second email account to use for customer service enquiries.
- Make sure the funds are in your PayPal account before shipping the item.
- Use a shipping service that tracks the item so you have proof of shipping.

## Buying

- Pay with PayPal or a credit card. Don't pay a seller by bank or instant wire transfer because once the money's gone, it's gone. If the transaction was fraudulent, you won't get the money back. Avoid sellers who demand payment in this way.
- When buying on eBay or other online marketplaces, research your seller's reputation.
- When buying from larger sellers, enter their details into a search engine to see if everything matches up.