




Australian Government

**Department of Communications,
Information Technology and the Arts**

PHISHING—DON'T TAKE THE BAIT!
Avoid being caught by fraudulent emails





As the Internet grows in popularity and convenience it is increasingly being used by people to shop, bank and do business online. The Internet provides access to resources and services that would be far more time-consuming and difficult to reach in person.

The Internet and email are increasingly being used as a medium for fraudulent activities—to trick people into revealing personal information in order to commit a crime.

This brochure contains information about a kind of online fraud called ‘phishing’.

It gives you some pointers on how to avoid being caught out.

What is 'phishing'?

'Phishing' refers to fraudulent email messages used to gain access to personal information for illegal purposes such as transferring funds or purchasing goods.

These fraudulent messages appear to come from legitimate businesses, most commonly financial institutions. They are designed to lure recipients into disclosing personal data such as bank account numbers, passwords and credit card numbers.

How to identify a 'phish'

Phishing messages and emails often look authentic. They pretend to come from a financial institution or other company and have a believable email address. They often copy that institution's logo and message format. It is common for phishing emails to contain links to a website that is a convincing replica of the company's home page.

A phishing email will usually describe a situation that requires immediate attention. It may tell you that your accounts will be terminated unless you verify your account information by reply email or by clicking on a link. This web link then takes you to a screen that asks for personal or financial information such as your Internet banking logon, password, credit card number or PIN.

Phishing emails often try to instil a feeling of urgency by saying things like:

- your account will be closed down unless you log on;
- a recent security upgrade means that you have to log on to be protected; or
- a large sum has been debited to your account and you need to provide your account details to confirm that the charge is incorrect.

Got a phishy email?

Here's how to frustrate the phishers

You can avoid most phishing scams by being alert and employing sound practices for Internet use. If you receive a dubious email, here are some steps you can follow.

Pause and think

Phishing emails may seem plausible when first read. They attempt to force the recipient to urgently reply, or log onto a website, before they have time to think about what they are doing.

If you receive an unexpected email from your financial institution saying that your account will be shut down if you do not confirm your billing information, do not reply or click on any links in the email.

Take your time to think about what you are being asked to do.

Most phishing emails are sent as spam, where the sender has no knowledge of the recipient. But even if you receive a message that is addressed to you alone, read it carefully. If you are suspicious about an email, double-check before responding.

Follow your own path to the site you choose

It is possible for phishing emails to create a link on a web page or in an email and make it look as if it is taking you to a bona fide website when it is actually sending you somewhere else. Your safest course is to check that you have the correct address (URL) and then type it each time into your address bar.

If you want to check the message by telephone, use the contact number that is in the phone book, not a number listed in the email. Often the numbers provided in phishing emails are false or can lead to you incurring costs.

Report it

If you have unwittingly supplied personal or financial information, you should first change your password and then report it as soon as possible to the organisation cited in the email either via telephone (using the telephone number in the phone book) or via a web site address you know to be genuine. You should also report the matter to your local police.

Delete the phishing mail

Some phishing emails include more than fraudulent information—they can also carry viruses. If you identify that an email is 'phishy' delete it immediately and permanently.

Banking online safely: be careful

Whether or not you receive a phishing email, there are some simple steps that you can follow to make your online transactions secure.

Secure your system

Some criminals try to use computer viruses to harvest people's account details, so you should make sure your computer is not an easy target.

- Install and use up-to-date protective software like anti-virus and anti-spyware software or a combination of these.
- Do not run or install programs of unknown origin.
- Use a personal firewall.
- If using a local area network, contact your administrator and seek information on the availability of email gateway filtering for specific file attachments.

Secure your passwords

If you bank online, you have a logon and password or a personal identification number (PIN) so that only you can access your own account. Do not let this personal information fall into other people's hands.

- Do not give your PIN or password to anyone else.
- Change your Internet banking passwords on a regular basis.
- Avoid using your birth date or name as your PIN or password.
- Avoid storing your passwords on your computer.
- Do not set up your computer so it 'autocompletes' or saves your password.

More information

Fighting the phishers

The Australian High Tech Crime Centre (AHTCC), hosted by the Australian Federal Police and the Australian Bankers' Association (ABA) has launched a national education campaign to warn consumers about protecting their personal information online.

- The AHTCC has published a useful fact sheet, *Protecting your information online*. You can find it on their website: www.ahtcc.gov.au > Publications > Protecting your information online
- The ABA is at www.bankers.asn.au. Their media release 'Australian Bankers' Association warns customers of cybercrime' can be found at www.bankers.asn.au > Media Centre > Media Releases 2004.

Australian information on scams

- The Australian Securities and Investment Commission's website www.fido.asic.gov.au has excellent information on fraudulent emails and phishing attacks and on consumer rights and responsibilities.
- The Australian Competition and Consumer Commission's Scamwatch site provides information on all types of scams: www.scamwatch.gov.au

- The Department of Communications, Information Technology, and the Arts has advice on e-security and resources on the *Spam Act 2003* at www.dcita.gov.au/spam
- The Australian Communications and Media Authority enforces the Spam Act. The ACMA website www.acma.gov.au/spam has information about spam and good Internet security practices.

International information

- The United States Federal Trade Commission guide *How not to get hooked by a phishing scam* can be found at www.ftc.gov > For consumers > Commerce and the Internet
- The Federal Trade Commission also has a website www.onguardonline.gov which provides practical advice on protecting personal information and securing personal computers against Internet fraud.
- Canada's Department of Public Safety and Emergency Preparedness and the US Department of Justice have produced a joint special report *Public advisory phishing: an emerging trend in identity theft* at www.psepc.gc.ca > A-Z index > Phishing

DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS
www.dcita.gov.au



Produced by the Department of Communications, Information Technology and the Arts and supported by the Attorney-General's Department, the Australian Communications and Media Authority and the Australian High Tech Crime Centre.

The contribution of the Australian Bankers' Association to the development of this brochure is gratefully acknowledged.

© Commonwealth of Australia 2006

January 2006