

# **Australian Government Department of Communications, Information Technology and the Arts**

## **INFORMATION SHEET:**

### **Phishing – don't take the bait!**

#### **Avoid being caught by fraudulent email**

##### **Introduction**

As the Internet has grown in popularity and convenience it is increasingly being used by people to shop, bank and carry out business online. The Internet provides access to resources and services that would be far more time-consuming and difficult to reach in person. Unfortunately though, there have been cases of the Internet and email being used for fraud – to trick people into revealing personal information in order to commit a crime. This information sheet contains information about a kind of online fraud called “phishing” and will give you some pointers on how to avoid being caught out by it.

---

##### **What is it, and why is it called “phishing”?**

An early form of computer hacking was to gain illicit access to other people's phone accounts and using them for illegal or expensive calls. This was called “phreaking”, using the first two letters of the word “phone”. It became fairly common hacker practice to replace the letter “f” with “ph” when talking about online or phone-based activities.

“Phishing” is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords and credit card numbers. Consumers are lured into providing their account details by deceptive emails that look like they have been sent by a financial institution or other company, but which are in fact clever copies sent by a “phisher” hoping to deceive and defraud.

---

**How to identify  
a Phish**

Phishing 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 .

Phishing emails give themselves away by telling you that there is some reason why you must provide personal details such as your Internet banking logon, password, credit card card number or PIN by reply mail or through a website. Very often phishing emails try to instil a feeling of urgency by saying things like:

- your account will be closed down unless you log on, or
- that a recent security upgrade means that you have to log in to be protected, or
- that 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 what to do:

### Frustrate the phishers

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

---

#### 1. Pause and think

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

When you receive emails asking for personal details , take your time to think about what you are being asked to do:

- Is it a message that you would expect to receive?
- Is it one that you have received from the financial institution or company before?
- Are there related announcements on the financial institution's or company's website?

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 there is the possibility that the message is a suspicious email it isn't going to hurt to double check before responding.

---

#### 2. Follow your own path to the site you choose

It is possible 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. It actually sends you somewhere else. Your safest course is to check that you have the correct address (URL), and then type it each time into your browser's address bar.

If you want to check the message by telephone, use the contact number that is in the phonebook, not a number listed in the email.

---

#### 3. Report it

If you think you've been taken in by a phishing scam, you should report it to the institution concerned as soon as possible. Also report the crime to the police in your state.

---

#### 4. 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' immediately and permanently delete it. .

## Banking online safely

<b>Be careful</b>	Regardless of whether you receive a phishing email or not, there are some simple steps that you can follow to make your online transactions much more secure:
<b>Secure your system</b>	<p>Some criminals try to use computer viruses to harvest people's account details, so you should make sure your computer isn't an easy target:</p> <ul style="list-style-type: none"><li>• Run and maintain an anti-virus product for your operating system</li><li>• Do not run programs of unknown origin</li><li>• Use a personal firewall</li><li>• If using a local area network, contact your administrator and seek information on availability of email gateway filtering for specific file attachments</li></ul>
<b>Secure your passwords</b>	<p>If you bank online, you have a logon and password or a PIN so that only you can access your own account. Don't let this personal information fall into other people's hands.</p> <p>Tips:</p> <ul style="list-style-type: none"><li>• Don't give your PIN or password to anyone else</li><li>• Change your internet banking passwords on a regular basis</li><li>• Avoid using your birth date or name as your PIN or password</li><li>• Avoid storing your passwords on your computer</li><li>• Don't set up your computer so it "autocompletes" your password</li></ul>
<b>Follow your own path to the financial institution</b>	<p>It is possible to create a link on a web page, or in an email, <u>look</u> as if it is going to a bona fide website of a company or financial institution but it actually sends you somewhere else. Your safest course is to check that you have the correct address from your financial institution, and type it into your browser's address bar. If you use the site on a regular basis, you can type in the address, bookmark it and access it from your browser's "favourites" list.</p>
<b>Any doubts? Report it</b>	<p>If you anything stolen, you'd report it as soon as possible. The same principle applies to your account details. If there's a chance that someone could use your account details to illicitly access your money, you should report it immediately instantly to your financial institution and the police in your state.</p>

## More information

### Fighting the phishers

The Australian High Tech Crime Centre (AHTCC) and the Australian Bankers' Association (ABA) are working together to tackle the problem of phishing emails and other bank fraud scams that occur online.

- Australian High Tech Crime Centre: [www.ahfcc.gov.au](http://www.ahfcc.gov.au)
  - Australian Bankers' Association (ABA): [www.bankers.asn.au](http://www.bankers.asn.au)
- 

### Australian information resources

- Australian Securities and Investment Commission's website has excellent information on a variety of scams, and your consumer rights: [www.fido.asic.gov.au/fido/fido.nsf](http://www.fido.asic.gov.au/fido/fido.nsf)
  - [www.consumersonline.gov.au](http://www.consumersonline.gov.au) "Little Black Book of Scams"
  - The Department of Communications, Information Technology, and the Arts has excellent advice on e-security and resources on the Spam Act [www.dcita.gov.au/spam](http://www.dcita.gov.au/spam)
  - The Australian Communications Authority enforces the Spam Act. The ACA website has information about spam and good internet security practices [www.aca.gov.au](http://www.aca.gov.au) click on 'Spam'.
- 

### International information

US Federal Trade Commission guide:  
[www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm](http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm)