Phishing

Phishing is a form of hacking used to gain personal information for the purpose of identity theft using fraudulent emails. The email messages appear to be from a legitimate business but are in fact a form of spam.

These messages are designed to dupe the recipient into divulging personal information, such as passwords and bank account numbers. Phishing emails most commonly pretend to be from banks and other financial institutions and have a functioning email address or website. These fraudulent email messages often ask for sensitive information and can include threatening or provocative instructions, for example:

– *[You must provide this information or your account will be closed down –*

– *A large sum of money has been deposited into you bank account, log on here to confirm the amount is correct.]*

Many phishing attempts can be identified by the wording of messages or the use of logos and icons from well-known businesses. These copies are usually of low quality and can have spelling errors. The Department of Communications, Information Technology and the Arts (DCITA) publishes several consumer guides aimed at helping individuals and businesses ward off phishing attacks.

Strategies to combat phishing suggested by the DCITA include the following:

1. Before responding to any email, ensure the message seems plausible. For example, a message from a bank asking you to go to a website and log on so that the bank can update your details may seem plausible at first. Phishing emails attempt to elicit an urgent response from a victim, hoping that they will act without thinking.
2. Don't use a web page link within an email address. These will often lead to a copycat site that looks like the genuine webpage but is in fact a dummy page set up to capture information, like a person's keystrokes, and therefore their passwords and account numbers. Always navigate to a website by typing the URL into the browser address bar.
3. Look for the person or business's contact details in the message. If there is a phone or fax number, postal address or email, it is safer to use this contact information to make an inquiry before sending any information. Many phishing messages only offer the reply to sender function and do not contain additional contact information.
4. Delete any phishing emails as they often can carry a virus or spyware. Report any phishing email to the police.

More information about phishing and other Internet-based crimes can be found at the Australian High Tech Crime Centre (AHTCC). The AHTCC website releases warnings about current phishing and virus attacks and provides help with detection and prevention. www.ahtcc.gov.au/

Source: *Department of Communications, Information technology and the Arts, 2004, 'Phishing, don't take the bait' www.dcita.gov.au*