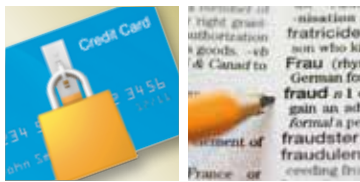


Internet Fraud

The term 'internet fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud may include spam, scams, spyware, identity theft, phishing or internet banking fraud.



Spam

Spam is a generic term used to describe electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

More information about spam is available from the Australian Communications and Media Authority (ACMA) website (www.acma.gov.au).

Scams

The power of the internet and email communication has made it all too easy for email scams to flourish. These schemes often arrive uninvited by email. Many are related to the well documented Nigerian Scam or Lotto Scams and use similar tactics in one form or another.

More information about scams is available from the Australian Competition and Consumer Commission (ACCC) SCAMwatch website (www.scamwatch.gov.au) and the Australian Securities and Investments Commission FIDO website (www.fido.gov.au).

Spyware

Spyware is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth or processing capacity and secretly gives it to someone else. It is recognised as a growing problem.

More information about taking care of spyware is available from the Department of Broadband, Communication, and the Digital Economy (DBCDE) website (<http://www.Dbcde.gov.au>).

Identity theft

A large part of online crime is now centred on identity theft which is part of identity fraud and specifically refers to the theft and use of personal identifying information of an actual person, as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of persons either living or dead.

More information about how to prevent and respond to identity theft is available from the Attorney-General's Department website (www.ag.gov.au).

Phishing

Phishing is a technique used to gain personal information for the purpose of identity theft. Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed the victim downloads a program which captures his or her banking login details and sends them to a third party.

More information about phishing is available from the Australian High Tech Crime Centre (AHTCC) website (www.ahtcc.gov.au).

Internet banking fraud

Internet banking fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as phishing.

More information about internet banking fraud is available from the Australian High Tech Crime Centre (AHTCC) website (www.ahtcc.gov.au).

Suggestions to prevent loss from Online Fraud

- Consideration of using a low-limit separate credit card for online purchases to minimise the potential loss if things go wrong.
- Limiting the amount of personal information you allow to be 'the public domain' i.e.: social networking sites that could be used to assist in identity theft.
- Keeping anti-virus and firewall software up to date.