



Don't share identification numbers and passwords

- Change passwords on a regular basis
- When choosing a password, select a combination of capital letters, lower case and numbers

Internet Transactions

The use of the Internet for buying and selling goods, banking transactions and purchasing digital (non-tangible) products is increasing.

- Always check your bank account transactions and balances and report discrepancies immediately to your financial institution
- Don't automatically check boxes before reading the contents of any statement or agreement
- Consider the use of a third party to hold payment in trust until you receive an item purchased via an online auction site

At home

If you have a computer at home, the same security precautions apply as in the workplace. This includes installing virus software, a firewall and allowing password-only access.

Beware of children accessing adult sites, chatrooms or email from dubious sources.

- Keep your computer in a family room so that you can monitor its use
- Avoid opening unsolicited emails – they may contain viruses! Delete them immediately and do not respond to the inquirer.
- Do not automatically divulge personal information to anyone who has solicited contact with you, without checking their credentials.

Be alert to the methods used by offenders to commit E crime and report any suspicious or fraudulent activity to the police immediately.

Did you know...

...by keeping original, offensive, menacing or harassing emails can help the police track down the offender.

For further information please contact:

Major Fraud Investigation Group
Queensland Police Service
200 Roma Street, Brisbane, Qld 4000

Phone: (07) 3364 6622
Facsimile: (07) 3364 6549
Website: <http://www.police.qld.gov.au/pr/program/fraud/whatis.shtml>
Crime Stoppers 1800 333 000
Crime Stoppers TTY 1800 333 000
Emergency only 000

Cartoons by Rob Wann

Produced with the assistance of the Media & Public Relations Branch
Reproduced from information supplied by the NSW Police Service

Queensland Police Service Vision Statement

We are determined to be a professional police service, dedicated to excellence and committed to working in partnership with the people of Queensland to enhance the safety and security of our community.



Your guide to stopping

E-Crime fraud

'Foiling the fraudsters'

What's Fraud?

Fraud is behaviour that's deceptive, dishonest, corrupt or unethical.

For a fraud to exist there needs to be an offender, a victim and an absence of control or safeguards.

Here in Queensland, the laws on fraud involve dishonesty in any of these situations:

- obtaining property belonging to someone else
- applying someone else's property to one's own use
- causing a detriment to another person or entity
- gaining a benefit or advantage for any person; and
- inducing or causing any person to deliver property to another person

Fraudulent activity in the workplace often results in the loss of revenue and property, while increasing operational costs and service charges. It can also mean obligations to employees, customers, suppliers or contractors can't be met.

The knock-on effect for businesses may:

- damage credibility
- compromise confidentiality
- result in public criticism

Common frauds include using false

- identities
- cheques
- credit and EFTPOS cards

Fraud Risks and Prevention Measures

With the rapid advancements in technology, frauds are becoming more sophisticated, widespread and complex. As a result, stamping out fraudulent practices becomes a huge challenge and requires extra vigilance on the part of businesses and individuals

What's E-Crime?

Electronic or E-Crime involves the use of electronic devices, such as computers.

In line with modern technological advances, E-crime is becoming increasingly sophisticated and complex, with offenders hacking into computer systems or using stolen credit cards to carry out Internet transactions.

Businesses and individuals are equally at risk of E-crime both at home and in the workplace.

The main areas involved in E-crime are:

- breaches of security and privacy

This may include theft of equipment or data, unauthorised use of personal or sensitive information and viruses.

- fraudulent transactions

This may include the use of stolen credit cards or dealing with bogus companies.

Why does it happen?

Breaches in security and a lack of awareness are the fundamental causes of E-crime. Many people unwittingly create opportunities for offenders by not keeping up to date with the ever-changing technology on the marketplace.

Sharing personal information, passwords and other data may also lead to serious lapses in security resulting in fraudulent activity.

What can you do?

Computer security

It's vital to secure your computer and allow password access only. The most important part of the computer is the hard drive, which stores all your data.

It's important to develop and implement appropriate system failure procedures, also known as data

backup. This can be done easily by transferring your data on to a floppy disk, CD Rom, zip drive or the main server if you have one.

Keep the serial numbers of all your computer equipment (separate from the hard drive) in a safe place.

Data Security

More and more businesses and individuals are taking advantage of computer technology as it becomes more widely available and affordable.

This has led to an increase of unauthorised use of data, such as confidential, personal or sensitive information and theft of data for commercial purposes.

It's important to safeguard your data at all times by ensuring:

- a firewall is installed
- a virus protection programme is installed and regularly updated
- data files and listings are secured and shredded when they are no longer required
- security violation reports are reviewed and investigated

Keep reviewing your data security, especially when a staff member leaves or there are staff changes in your organisation. Simple steps you can take include making sure:

- only password access is allowed
- only authorised employees are given access to data
- data access is cancelled promptly when it is no longer required by a staff member or they leave

Passwords

Poor password security is a major cause of computer fraud. Store your passwords and other personal information on a separate storage device rather than on the computer's hard-drive.