Protect Who You Are: Keeping Your Identity Safe Online

With the very extensive use of the Internet today, going online has become a great part of our everyday routine. The internet allows various things to be done in a faster way, and almost every company and organization needs to be accessed through the internet if they want to stay relevant and to keep up with the fast-paced business industry. With this comes the increase in identity theft and online fraud, making it some of the fastest increasing crimes in Australia.

According to the Australian Federal Police, The term ***'online 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.

Proudly brought to you by… Grand Capital FINANCE GROUP

Identity crime causes financial damage to consumers, lending institutions, retail establishments and the economy as a whole. Among its other impacts, identity crime:

- Fuels other criminal activity
- Erodes trust in service providers
- Causes emotional distress for victims
- Increases investment in time and resources by law enforcement
- Increases business investment in methods of securing customers' private information
- Chase's business/individual financial losses that are never recovered
- Can threaten the safety of people who may have data exposed
- Can lead to innocent people being refused employment, denied credit, receiving bills for items not purchased by them or even arrested for crimes they did not commit Identity thieves can use a wide range of methods in the internet:
- **Mail forwarding**—filling out a change of address form to redirect mail to them to gain information.
- **Unsolicited contact**—phone calls claiming to be from banks asking to update personal information, or criminals posing as market researchers.
- **Internet sites**—sharing personal information to gain access to websites and buy goods. Criminals can take the personal information to fraudulently obtain credit. Social networking sites also present opportunities. While people don't present personal information to strangers in the street, they will build online profiles that include detailed personal information such as their birthday and age, residential suburb, relationships and life stories.

- **Phishing**—sending an email to a user that falsely claims to be from an established legitimate business in an attempt to trick them into revealing private information so the criminal can obtain money from accounts.
- **SMiShing**—Phishing via short message service (SMS).
- **Hacking**—unsolicited access into a financial institution's website to obtain e-banking details of customers are using keylogger programs to target online chat rooms and instant messaging systems and gain personal information.
- **Lottery**—a scam where a person is advised that they have won a lottery they have not entered. They are then asked to provide personal information to prove their identity and/or send a fee or bank account details in order to collect the prize.

For additional information on how the Australian Government and Institutions identify and protect us, please visit the following:
Australian Government - Attorney General's Department
http://www.ag.gov.au/identitysecurity
Australian Federal Police

http://www.afp.gov.au/policing/cybercrime/internet-fraud-and-scams.aspx#identity-theft
Australian Crime Commission
http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/identity-crime

Credit Card Fraud

Financial Institutions are actually bound to help you when you experience credit card fraud. It's best to check the rules and guidelines set by your bank, as most banks will give you a refund through their money back guarantee, provided that you complied with their requirements. Knowing this, it is still best to protect yourself from fraud and scams before they happen to you. Some ways you can guard yourself online:

- Regularly check your bank account statements and if there are any purchases you cannot account for, report them to your bank
- Do not give your personal, credit card or online account details to a caller on the phone unless you made the call, or to anyone with an email (even if the caller seems legitimate and has given you most of your account and address details)
- Use the phone book to independently check the contact details of the company calling you before you give them any of your details
- Do not give your PIN to anyone and choose passwords that would be difficult for others to work out
- Never use computers in libraries or internet cafes for your online banking
- Have up-to-date anti-virus software installed on your computer
- Be wary when installing applications onto your phone. Scammers may send you applications designed to

download malicious software and steal bank account details. See the ACCC's SCAMwatch webpage on mobile phone scams.

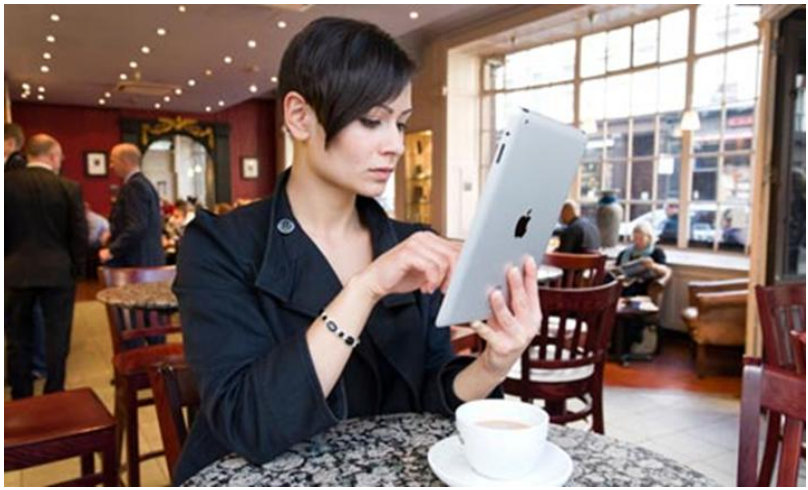
If you have been scammed, make sure to do the following:

- Call your bank to report the scam and ask them to help you get your money back
- File a police report at your local police station
- Get a copy of your credit report from one of these reporting agencies: MyCreditFile.com.au (Veda), CheckYourCredit.com.au (Dun and Bradstreet) and Tasmanian Collection Service (see credit reports and credit repair). This allows you to check that no-one is using your name to borrow money or run up debts.
- Warn your family and friends

How You Can Protect Youself from Online Theft and Identity Fraud

Learn to Identify Phishing and Spear Phishing Attempts

Phishing websites are common nowadays as some legitimate looking website presents itself as legal and asks for important information from you such as your credit card no, bank account no, your social security and more. If you have a question whether the site is a real one for a company, visit the organization's main web page and call their number to ask.



Beware Suspicious Emails and Attachments

Email addresses can easily be faked and made to look authentic. If you have entered your email addresses to some games, websites or freebies online, you might notice getting unsolicited and spam emails on your email. This usually contains links that will instead lead you to harmful websites. If there is a way for you to just copy a link to your browser instead of just clicking a link, it is good to do that. Also, make sure that you are getting a message from your real institution. Double check if the sender and the reply email are the same. If something is almost too good to be true, it almost always is.

Keep Your Anti-Malware Software Up-To-Date

A number of softwares can be automatically installed on your computer and will allow them to enter your system and get your internet activity and other important information you have stored on the internet and your computer. Make sure that you always update your antivirus and anti malware programs to keep your system protected. Some are free and only uses a small amount of your computer's resources so you need not even worry if they will affect your computer's performance.

Use Strong, Secure Passwords, and Different Ones On Different Sites

Because of the various ways to reset and recover passwords nowadays, it is of utmost importance that you keep your passwords secure, unique and use different ones on different sites. Criminals may use to obtain your personal information by logging into your email and other online accounts and glean information from there. That is the reason that it is so important to maintain password security across all of your online accounts. Generating a secure password is the first step to prevent identity theft by keeping your accounts secure, and then Lastpass or Keepass will assist you in remembering them. Make sure your passwords contain a combination of letters, numbers and symbols that you will remember or stored in a very secure place in your computer. The last thing you want is to make it very easy for even your own friends to find out. Make sure that you also use different passwords so if ever one is compromised, the others will still be secure.

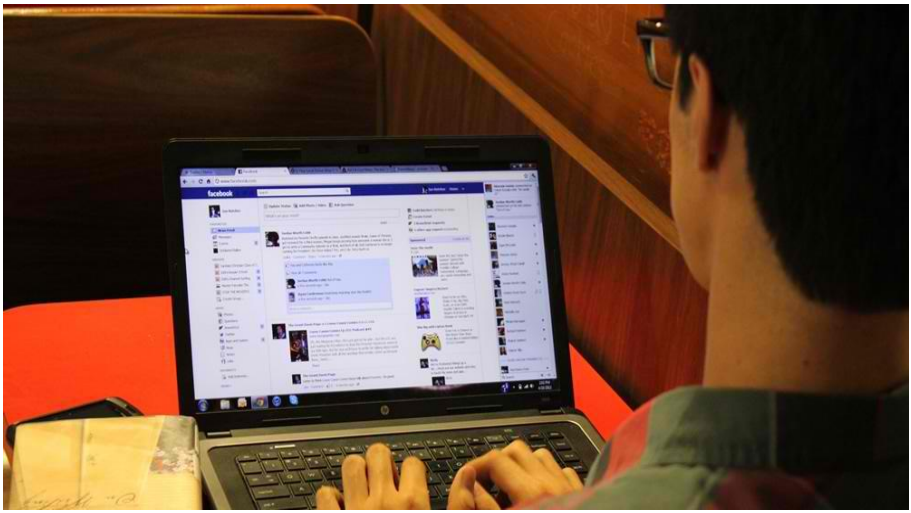
Shop Only at Reputable Websites

It is very convenient to do your shopping online nowadays and it saves you more time to do other important things that you need to be doing. Make sure that you only shop on websites that you trust and be careful in entering your bank or card information.

Don't Divulge Too Much Personal Information via Social Media

Social media is a very effective way to use to communicate and advertise today. But be careful how much information you give out to the general public while sharing what you are, for example, eating. There are people who check into banks occasionally on FourSquare; this is bad because it lets anyone know who you use

for your bank and makes you an easy target for identity theft. The private information listed above should never be divulged on social media sites as well as other information people could use to obtain that private data from you.



Secure HTTPS Before Entering Any Financial Details on a Website

HTTP, the letters you see in the address bar before the name of a particular website stands for Hypertext Transport Protocol, which simply means that this is the language used by your computer to transfer information between web servers and clients. This is the regular but unsecure language and should be looked at properly when using a website that will ask you to enter your credit card no, bank information and other important details about you. For websites that require these numbers, it is important that they start with https, s for secure. This means that your computer is talking to the website in a secure code or language and no one can actually see, monitor or eavesdrop on the information that you will input.

Monitor Your Credit Profile

Part of being vigilant about identity theft is making sure someone doesn't already have your information and is using it – the sooner you catch it the better. Check how you can monitor your credit profile effectively based on your location.

Secure Your Wireless Network

There are a number of reasons to secure your wireless network and one of the main ones is to reduce fraud and identity theft. If you leave your wireless network open (not securing it with WPA encryption) and without a password, not only can an attacker use your network without your knowledge but can also view your website usage. This can allow them to easily build a detailed profile of you (and your family) and the websites you visit. Even if some information is encrypted (your credit card number for example) many sites do not encrypt login information and just the website names alone can help give an attacker information about you. Adding a password to your wireless network protects against this.

Only Download Software from Reputable Sources

Similar to only shopping on reputable sites, you should only run software that comes from known sources. If you download games/screensavers/warez/cracks from disreputable websites they may include backdoor and trojans that your antivirus may or may not catch. The sites mentioned above are a start but always be aware and of course keep your antivirus updated, especially if you frequent those websites. Stored in a very secure place in your computer.

The last thing you want is to make it very easy for even your own friends to find out. Make sure that you also use different passwords so if ever one is compromised, the others will still be secure.

If you require additional information call us on 1300 139 883. Also, like our facebook page to stay up to date on the latest changes in Finance and other related topics at http://www.facebook.com/grandcapitalfinance