

Scams

Increasing levels of technology in day to day life has lead to many benefits, but there are some people, known as scammers, who choose to exploit technology to take advantage of innocent victims. Scammers use technology to illegally make money. Everyone who uses the internet and email needs to be aware of scams and should recognise signs that may indicate a scam.

Scams are designed to fool you into giving away personal details and they do this through a variety of methods. Scams usually involve deals too good to be true often with a time limit so you are forced to act quickly- this is to prevent you from thinking through the situation before making a decision. Scam will often require you to provide personal details under the explanation of 'confirming your identity'. In these instances you will never receive what you are promised and in actual fact you will have inadvertently provide scammers with enough information about yourself that they have been able to deduct money from your bank account, booked purchases up on your credit card, or have stolen your identity.

Some scams are designed to fool you into giving away money not just personal details. A scammer may ask you to send a small amount of money under the explanation of needing 'to finalise legal documents' with the promise of returning a large amount in the long term. Scammers will even tell a story to make you drop your guard. They may tell you they are collecting donations for a charity that helps sick children so you feel more inclined to donate.

A scammer will always pretend to be legitimate and scams are disguised in legitimate looking emails or websites. Scammers expect that when you receive correspondence from a reputable business, that you will assume the correspondence is also reputable. Scammers may portray themselves as banks, big businesses or government agencies. Emails will seem genuine with exact logos and layout, as scammers deliberately design their emails look like original documents. These emails will often ask you to visit their websites, but just because a company has a website doesn't mean it is legitimate. Anyone can put anything on the internet without meeting any standards. If emails ever ask you to "click here to log in" or words to that effect, never click the link. Instead open up the internet and visit the actual website, as links in emails are often the work of scammers. Never click on a link in a scam email, never reply to a scam email and never call a phone number in a scam email.

Just because a website has features normally associated with 'safe' websites, such as showing a padlock, starting with https://, featuring VeriSign, Comodo or Secure Socket Layer (SSL) Certificates this does not necessarily mean the website is legitimate. A knowledgeable scammer can easily set up a secure looking website to trick people into believing it's legitimate and safe. The best way to identify a legitimate website is to research the company online by typing the business name into a Google search along with the word 'scam'. When the search results appear you will be able to see if they have a long history associated with scams or whether they are in fact a legitimate business with a very limited history featuring the word scam.

Even with junk mail filtering settings every email address inbox will receive junk email at some stage. Before opening each email in your inbox ask yourself "Do I know this person?" If the name is unfamiliar, if the address is unfamiliar or if the topic is strange, you should delete these messages immediately. In many instances people open emails without thinking and this allows scammers access to the computer and to all of the details stored in the computer. Never reply to junk emails.

You may receive emails from a familiar person's name, yet the actual address will not be the normal one that your friend uses. This could be a sign that your friend has signed up for a scam on the internet which has then been distributed through their address book. The email you receive will often suggest that you sign up for a free gift. If you reply, what you are actually doing is confirming your identity to a scammer who will then sell your details to spammers, so you will be bombarded with huge numbers of spam emails.

Real banks will never contact clients via email and no email should ever ask you to confirm passwords. If either of these things happens you will immediately know you are dealing with a scam and that you should delete it.

One way of identifying whether you are a victim of a scam is to always check your bank statements and ensure you can account for each transaction. If some stand out, such as transactions made in Europe when you have never left Australia, then follow these up immediately with your bank. Some banks offer a service where they contact you when an unusual new charge is made to your credit card. Even with these types of legitimate sounding courtesy calls, still ensure you never give any details to the person on the phone as it could potentially be a very sneaky scammer. Instead follow it up by going into your bank's nearest branch or calling the bank back.

The best way to avoid a scam is by being smart and accepting there are no get-rich-quick schemes. If something seems too good to be true then it's a scam. If someone contacts you about a long lost relative who has left you money, chances are it's a scam so be sceptical. It is by being naive and hoping for the best that many people become the victims of scams. Legitimate companies making genuine offers will not mind if you take time to think things through and to conduct research to ensure the offer is real. It is only scam operators that will put you under pressure to make an instant decision.

The best way to protect yourself from web based scams is to research different types of scams and to stay up to date with current scams as they continue to evolve with improving technology. You can download "The Little Black Book of Scams" from <http://www.scamwatch.gov.au>. It outlines many different scams including ones not based on the internet or email. Copies of 'The Little Black Book of Scams' are also available from the Grenfell Internet Centre in Main Street.

If you are looking for a new or used computer drop into the Grenfell Internet Centre on Main Street. We currently have access to special deals for Centrelink concession cardholders, individuals who can verify low income status, schools and not for profit organisations where second hand computers are available from \$290. Call Josh on 6343 1720 to find out more.