COTA

FACTSHEET

Internet safety: be confident online

TIPS FOR USING THE INTERNET SAFELY

The following table shows some of the common challenges associated with internet use. For each of the challenges we've included a series of safety tips that you can follow to minimise the risks associated with using the internet.

Challenges	Safety tips
Maximising the security of your internet	• Install and update security software e.g. anti-virus, anti-spyware, firewall. • Set your security software to scan regularly. • Turn on automatic updates for all of your security software. • Ensure the time you choose for the automatic update to take place is a time that your computer will be turned on. • Optional: set updates to occur when you first open up the internet.
Limiting external or remote access to your computer	• Only allow remote access to your computer if you have paid for remote support. Ask the caller a few questions about their company and your account so you can verify they are who they say they are. • If you have not requested or paid for remote access support, ignore requests by phone or email requesting remote access.
Protecting your identity online	• Use strong passwords and change them regularly. • Protect your personal, credit card or online account information. Only enter a website if you are certain it is a genuine site. • Be cautious if you receive a request by email or on websites to update, validate or confirm your personal information. Contact the organisation by phone or go to their website and ask them if they have requested the information or sent the email. • When using social media, read and use the privacy settings to control the amount of information you want to share.
Protecting your financial information online	• When visiting a financial institution's website, like a bank, type the full website address into the internet address bar (found at the top left hand corner of the internet page). Hyperlinks in emails and webpages may disguise where you are really going. • Sending financial information by email is as risky as keeping your credit card password with the card. Never do it. • When shopping online, use a secure payment method such as PayPal or BPAY. Major online shopping sites use secure payment methods but if you want to know more about payment options you can give them a call.

Challenges	Safety tips
Recognising spam (electronic junk mail)	• Internet providers can help with spam filtering. Speak to your provider about your options. • Only open or forward emails where you know the sender. • Only give your email address away when you are confident the recipient is a trusted party.
Avoiding viruses	• Scan email attachments with security software before opening them. • Only open emails or attachments if you're expecting them or you know the sender. • Look closely at the name of the email sender, as the name can look like someone you know but there may be slight difference.
Outsmarting scammers	• Ignore suspicious emails, letters, or phone calls. • Any email containing an offer that sounds too good to be true should be treated with distrust. Never respond to emails where an unknown sender asks for money or financial information.
Creating strong passwords	• Generally, a strong password has all of the following attributes: • A minimum length of eight (8) characters, although 12–14 is better. • A mix of upper and lower case letters. • At least one numeral. • At least one non-alphanumeric character eg (@#%^). • Does not include a dictionary word in any language.
Remembering your password	• The password does not literally have to be a single word. To make a password easy to remember, think of a pass phrase and then change some of the characters to make it a strong password: June School Holidays can be modified to: 7un3Schoo1Ho!id@ys Be good, be wise can be modified to: B3g00db3wi5e$ • Note: don't use the examples above as your passwords.

Note: some of the information in this fact sheet has been taken from Factsheets on Stay Smart Online www.staysmartonline.gov.au/factsheets

Every care has been taken in the preparation of this document such that the information it contains is believed to be accurate. It contains guidelines only in relation to its subject matter. COTA NSW suggests that professional advice be sought wherever necessary.

STAY SMART ONLINE

COTA

Australian Government
Department of Communications