Scams and Online Safety

Have you ever experienced……

- An email or text
    - asking you to update your personal information
    - that you were not expecting with an attachment
    - stating your account is about to expire
    - finally locating you as the long lost relative and you have inherited money
    - wanting payment on your account
- Shopping sites that sound too good to be true
- Phone calls saying there is a virus on your computer

Beware of Scams

Where someone tries to trick you into giving them your money or personal information. They often:

- Look real
- Catch you by surprise
- Come with believable stories
- Play on your emotions

Top 10 scams by losses

- Investment scams
- Dating & romance scams
- False billing
- Hacking
- Online Shopping Scams
- Remote Access Scams
- Identity theft
- Threats to life, arrest or other
- Classified scams
- Inheritance scams

5 Key Items to look out for:

1. You cannot confirm who the email is from
2. It has spelling and grammatical errors
3. It has a request for you to do something
4. It has a malicious link
5. There is a sense of urgency

E: enquiries@stayintouch.net.au | P: 03 9596 4547
PO BOX 8100, North Road LPO, 609 Hawthorn Road, Brighton East VIC 3187

Avoid SPAM, Scams and Fraud!

- Never respond to requests for personal information in an unexpected email
- Be skeptical if you receive a request to update, validate or confirm your personal information
- Do not provide email addresses unless needed
- Create separate email accounts
- Never send money or provide credit card, account or personal details to unsolicited offers, emails or calls
- Don't let scammers push your buttons and resist the personal touch
- Banks will never send unsolicited emails
- If in doubt contact the organisation by phone with the phone number in the book

What to do?

- Do not reply
- Do not agree to anything
- Call someone else
- Call the organisation back with the number you know it to be
- Open your internet browser and type in the website address and log in to check your account
- Go to scamwatch.gov.au and see what scams there are

What to do if scammed

- Contact your bank first
- Don't give up or feel ashamed
- Report the scam with www.scamwatch.gov.au/report-a-scam
- Scan your devices and run a security check

Secure Your Devices

- Install security software and update it regularly
- Turn on automatic updates on all of your software
- Set strong passwords and change them regularly
- Use administrator and standard user accounts
- Secure your internet, internet browser and wireless network
- Control the access to your device
- Monitor your programs and apps
- Back up your information

Stay Informed!

- **www.cyber.gov.au**
- **www.scamwatch.gov.au**
- **www.esafety.gov.au**
- **www.stayintouch.net.au**

Book a 1-on-1 appointment

If you require 1-on-1 **tutoring**, **technical support** or **security check** performed on your devices, please call our office on 03 9596 4547 or email bookings@stayintouch.net.au to book an in-home or remote appointment with one of our friendly staff.

Stay informed and keep learning

www.stayintouch.net.au
Sign up for our newsletters to receive top tips and upcoming events!
Keep an eye on our Events page for upcoming sessions

www.beconnected.esafety.gov.au
Create a Free account with this government program to keep learning.
Your Support Centre is Stay In Touch Pty Ltd

Share Tech Tip Tuesdays with friends

If you would like to invite your friends and family to join our Tech Tip Tuesday sessions each week from 12.30-1.00pm, please ask them to register with this link.
https://www.eventbrite.com.au/e/102000702848