QUICK ONLINE SECURITY TIPS...

Stay Safe Always.

lions australia

Whilst technology can be a great tool for all of us, it is important to be aware of the many scams that can be found online. These emails are indiscriminate and are becoming increasingly clever and sophisticated. We've collated some tips and tricks to keep yourself safe online and help you identify some of the common scams.

Online Safety Tips

- Protect your computer by purchasing and installing a good quality malware/virus protection program.
- Use complex passwords to make it difficult for hackers to guess. Make sure you don't use the same password for everything, instead write them down on a piece of paper and keep it somewhere safe. Alternatively, use a reputable password manager application. Some tips on creating a strong password can be found here: **https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases**
- Never provide personal information via email (address, passwords, date of birth, etc.). With hacking being so prevalent, it's impossible to know where this information could end up. If you receive an email requesting these details and it is a business/someone that you know, give them a call and provide the information over the phone, instead. If you don't recognise the sender, delete the email immediately.
- Do not open any attachments or links unless you know who is sending it and you are expecting it. This is one of the most common ways that viruses can infect your computer. Hackers are very clever and can replicate email addresses, meaning that a virus may be enclosed in an attachment that looks like it is coming from a family member. Consider every link in an e-mail as potentially risky. For example, if you receive an e-mail from your bank asking you to click a link, go to your bank website instead, and find that link.
- Be alert to unusual e-mails. Think about what you know about the sender, is the e-mail unusual or unexpected? If you're unsure about it, don't reply. Give them a call or open 'new message' and send an email to the sender using a known email address.
- Do not pay any bills that you cannot independently verify as legitimate, or if you don't remember receiving the service. Do not email/phone the provider using the information provided in the suspect email, as it may be fake. Instead, find the correct contact details online to verify the bill.
- Never make bank transfers, particularly for large amounts, based on account numbers and BSB numbers sent by e-mail. E-mails can be forged. Always verify the account details over the phone.
- Learn to check e-mail addresses for hidden code. Remember the name you read may not be the destination of the e-mail.
- If you get an e-mail from someone you know requesting money, ring the sender, or their friends and family, to independently verify their status before sending any money.

Always.

lions australia

75 years and counting

Common Scams

https://www.scamwatch.gov.au/types-of-scams

- **Attempts to gain your personal information**
  - Scammers are clever and use sneaky tactics, such as hacking or phishing, to get your personal details which they can then use to commit fraudulent activities or identity theft.
- **Dating and Romance**
  - Scammers create a fake online dating profile and convince vulnerable people to send them money.
- **Remote access scams**
  - Scammers will pose as IT specialists and convince you that there's an error with your computer. They will attempt to gain remote access to your computer in order to "fix the problem" and steal your credit card details. Never give an unsolicited caller remote access to your device.
- **Unexpected prize and lottery scams**
  - If you receive an email or text advising you you've won a large amount of money that sounds too good to be true, it almost certainly is. Scammers attempt to convince you to give them money or personal information in order to receive a prize that doesn't exist.
- **Sick friend scam**
  - Scammers pose as a sick friend of yours and send you an email requesting financial assistance.
- **Missed Delivery scam**
  - Scammers contact you via text/email advising you that you've missed a delivery. They will ask you to click on a link to organize an alternate delivery time. Clicking on this link will download malicious software to your phone.
- **False billing**
  - You receive an email with a bill that looks legitimate. The account will have false payment details or are for services that you have not received.

Hackers and scammers are increasingly becoming more clever and diverse with their scams. If you believe you have been scammed, lodge a report with the ACCC (Australian Competition and Consumer Commission), here.

Stay suspicious and keep yourself informed https://www.scamwatch.gov.au/.

Always.
lions australia
75 years and counting