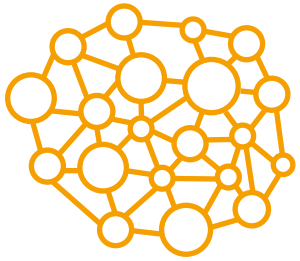
Staying Safe Online

Cyber Safety Guide for New Zealand Shoppers

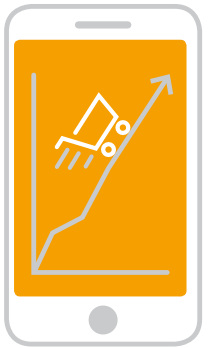
mastercard

CIS
Centre for Internet Safety



23 billion connected devices globally

3 out of 5 New Zealanders shop online



Online spending is growing faster than traditional payments

Why Shop Online?

The internet has revolutionised the way we shop, providing numerous benefits over the conventional way of going to a store. It provides the convenience of being able to purchase 24/7 from any location. Online shopping can provide more variety and the ability to buy global brands that may not be available at your local store.

Most internet businesses accept online payments, making the experience quick, safe and hassle free. Staying safe when making online transactions isn't complex or hard.

Tips

- Check that you are dealing with a trusted and reliable business by confirming their company details and researching online feedback and complaints.
- Only enter your payment details into a secure web page. A secure web page has 'https://' at the beginning of the address bar and a picture of a locked padlock in the browser.
- Never send your bank or credit card details via email.
- Be wary of websites making offers that seem too good to be true.

CASE STUDY

Julie received an email from a stranger offering her cheap tickets to an upcoming concert. The email contained details on how to purchase, and Julie clicked on the link provided. This action resulted in a new internet window opening on her computer – loading a professional-looking website where she entered her name, address and credit card information. Julie never received the tickets and was later informed by her bank that her credit card has been used to make several unauthorised overseas transactions.

Protecting Your Information

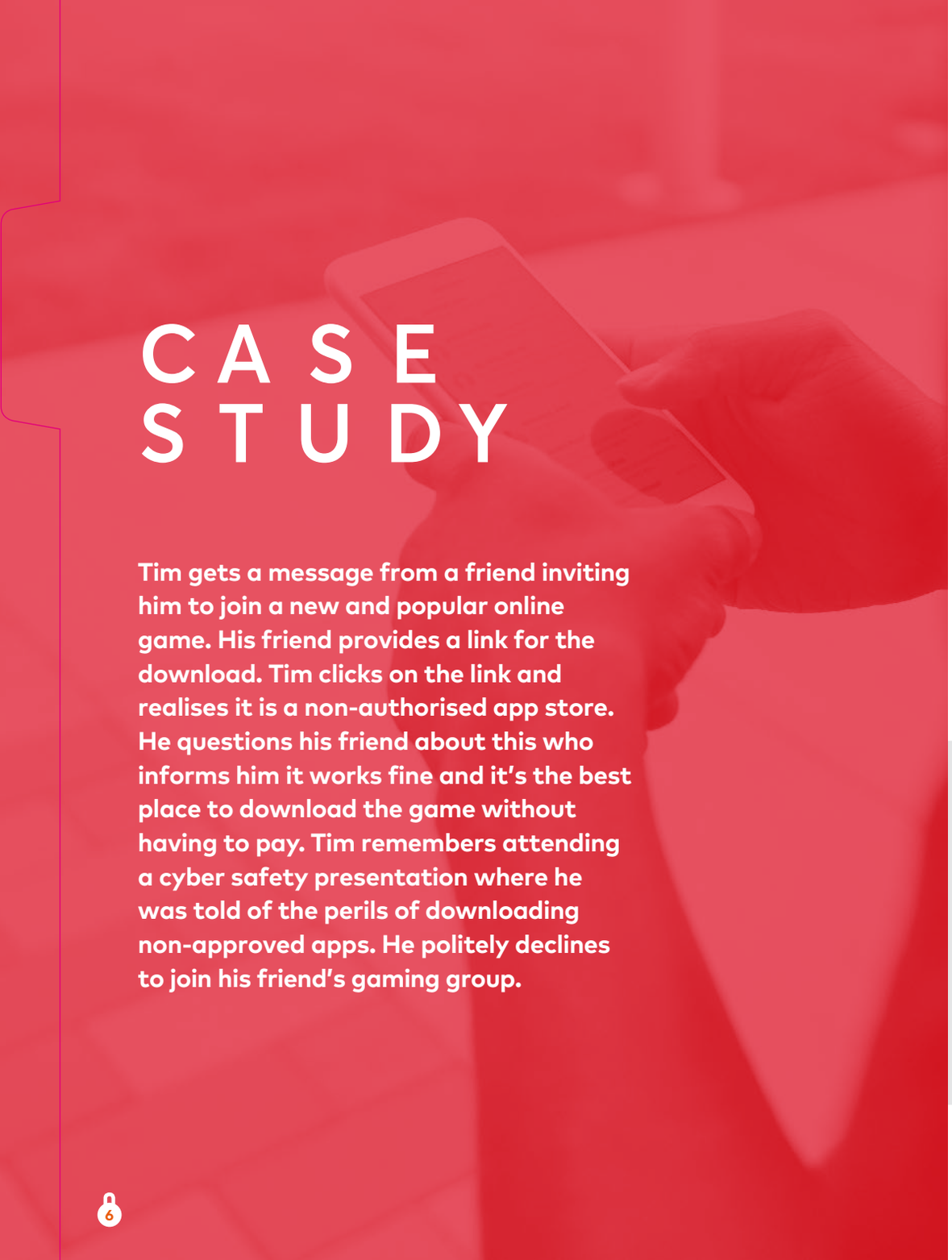
As we spend more and more time online, it becomes increasingly important to understand how to protect our personal information. Personal information includes names, addresses, phone numbers and bank details.

Many online merchants ask you to provide some personal information to use their service. They may be seeking to verify your identity to process payment or for the delivery of goods. You should look for online merchants that promote their trust and safety credentials.

Unfortunately, there are online criminals seeking to scam you, conduct identity theft or commit some other fraudulent activity. By stealing your identity, a criminal may access your bank account, obtain credit cards or loans in your name, and potentially ruin your credit rating and reputation.

Tips

- Install security software on your device and ensure it is up to date to protect against the latest threats.
- Use strong passwords and update them regularly.
- Do not store your password or PIN on your computer.
- Don't do your online banking or purchasing on a public wi-fi network.
- Backup your computer and mobile devices regularly.



CASE STUDY

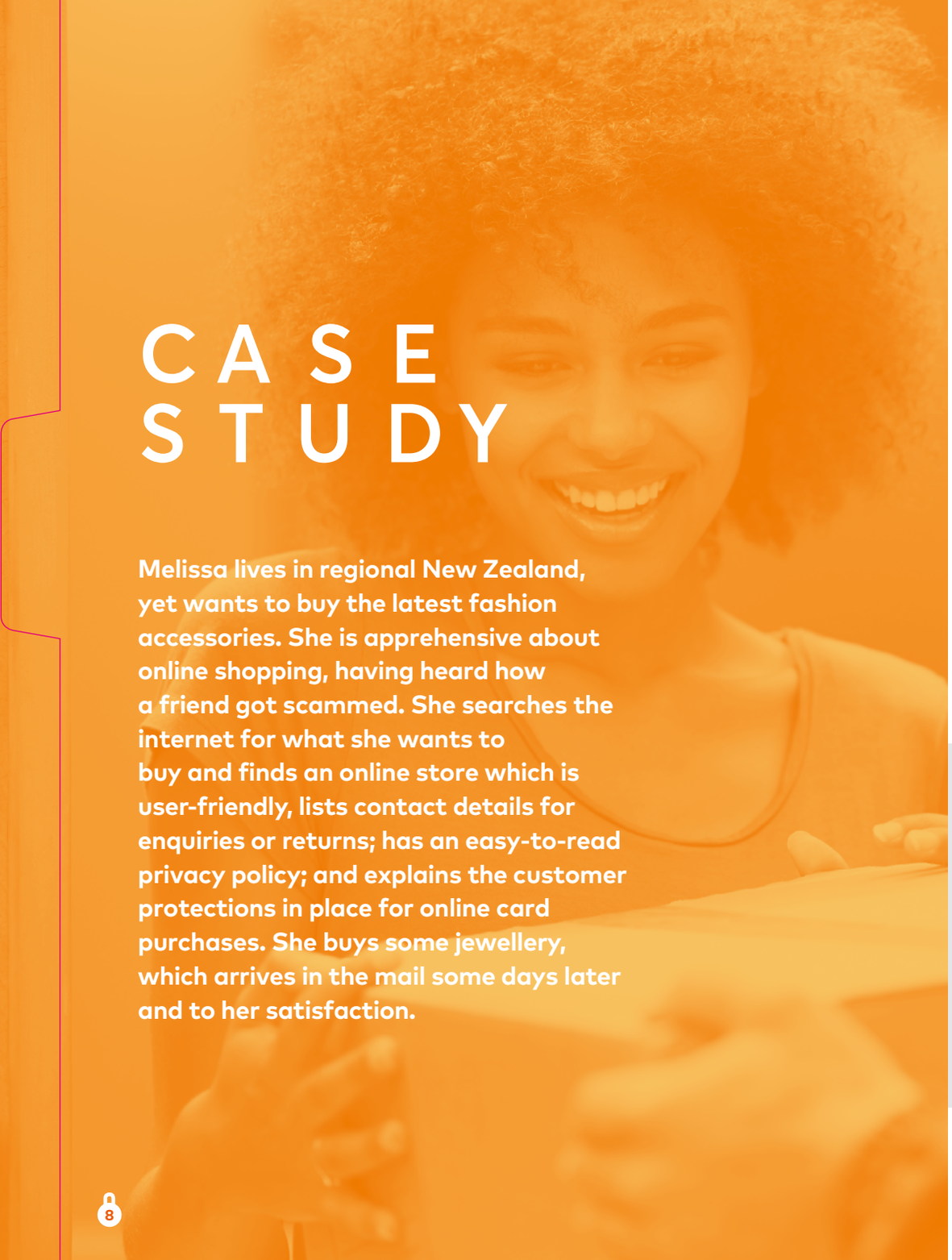
Tim gets a message from a friend inviting him to join a new and popular online game. His friend provides a link for the download. Tim clicks on the link and realises it is a non-authorised app store. He questions his friend about this who informs him it works fine and it's the best place to download the game without having to pay. Tim remembers attending a cyber safety presentation where he was told of the perils of downloading non-approved apps. He politely declines to join his friend's gaming group.

Protecting Your Device

Many of us use mobile smart devices to access the internet for social media use, web surfing and online shopping. This offers great convenience, however it can open us up to a number of risks. It is important to protect your device and the information on it.

Tips

- Set a password, PIN or passcode.
- Use your device's automatic update feature to install new application and operating system updates as soon as they are available.
- Ensure your device does not automatically connect to new networks without your confirmation.
- Check the privacy permissions carefully when installing new apps on your device and only install apps from reputable vendors.



CASE STUDY

Melissa lives in regional New Zealand, yet wants to buy the latest fashion accessories. She is apprehensive about online shopping, having heard how a friend got scammed. She searches the internet for what she wants to buy and finds an online store which is user-friendly, lists contact details for enquiries or returns; has an easy-to-read privacy policy; and explains the customer protections in place for online card purchases. She buys some jewellery, which arrives in the mail some days later and to her satisfaction.

Personal Responsibility

Online shopping is great, but you don't want to become complacent with security. While banks and payment technology companies devote a lot of effort to protecting consumers, it is important that you keep vigilant when shopping online.

Tips

- Use strong, unique passwords for each online account.
- Check your privacy and security settings on your social networking profile and never give away your account details.
- Don't use public computers or wi-fi networks to access your personal information.
- Check your account statements – including credit cards, bank statements, telephone and internet bills – for possible fraudulent activity.

THE ROLE OF MERCHANTS

Merchants are the first line of defence and can help customers have a safe and secure online experience. They play an important role by protecting their own computers; being vigilant to online scams and fraud; and by providing a safe and secure shopping experience.

Payment technology companies like Mastercard help merchants by providing them with an authenticated payment system to improve online transaction security and encourage the growth of e-commerce payments.

How is Industry Helping?

Masterpass

Masterpass is a digital wallet service that makes online shopping easy, secure, and convenient. A digital wallet stores all your payment and shipping information in one central and secure location.

Masterpass eliminates the need to enter financial and shipping information at every new merchant site, or the need to store personal information across a number of apps – better safeguarding your personal information.

3DS

Each time you make a purchase with a participating merchant you will be prompted by your bank to checkout using Mastercard SecureCode™. You will be asked to give a private one-time code provided by your bank, such as an SMS to confirm your payment. This code will never be shared with the merchant and can only be used for that one transaction.

Zero Liability

Mastercard Zero Liability card protection means you won't be held responsible for unauthorised transactions on your card.

Tips

- Contact your bank to discuss access to Masterpass and 3DS
- Further information can be obtained at www.mastercard.com.au

WHERE TO GO FOR HELP

- **CERT NZ** – CERT NZ works alongside government agencies and organisations to help New Zealand better understand and stay resilient to cyber security threats. CERT NZ is your first point of call when you need to report a cyber security problem. https://www.cert.govt.nz/
- **Netsafe** – Netsafe is New Zealand's independent, non-profit online safety organisation that provides practical tools, support and advice for managing online challenges including scams and security concerns. https://www.netsafe.org.nz
- **Connect Smart** – Connect Smart is a partnership that promotes ways for individuals and businesses to protect themselves online. Connect Smart is led by the Government's National Cyber Police Office (NCPO), as part of the Prime Minister and Cabinet, in partnership with Government agencies, NGOs and the private sector. https://www.connectsmart.govt.nz
- **Scamwatch** – The Scamwatch website is run by the Ministry of Business, Employment and Innovation (MBIE) and has information to assist New Zealanders about scams, including how to work out if you are being scammed, what to do and where to report it. https://www.consumerprotection.govt.nz/general-help/scamwatch/identify-a-scam/is-this-a-scam/
- **Office of the Privacy Commissioner** – The Office of the Privacy Commissioner investigates possible breaches of the Privacy Act, and provides education about the privacy rights of all New Zealanders. https://www.privacy.org.nz/about-us/introduction/
- **Crime Stoppers** – Operating throughout New Zealand, Crime Stoppers is an independent charity that helps New Zealanders fight crime by providing an anonymous and simple way to pass on information to authorities. https://www.crimestoppers-nz.org/
- **Banking Ombudsman Scheme** – the Banking Ombudsman Scheme is a free and independent dispute resolution service that looks into complaints by customers about their banks. https://bankomb.org.nz/about-us/
- **Your financial institution** – Contact your bank or financial institution when you think your account may have been compromised and money withdrawn without your authorisation.

ABOUT MASTERCARD

Mastercard is a technology company in the global payments industry that connects consumers, financial institutions, merchants, governments and businesses worldwide, enabling them to use electronic forms of payment instead of cash and cheques.

As the operator of what we believe is the world's fastest payments network, we facilitate the processing of payment transactions, including authorisation, clearing and settlement, and deliver related products and services. We make payments easier and more efficient by creating a wide range of payment solutions and services. We do business in more than 210 countries and territories and work with over 150 currencies.

Our network is designed to ensure safety and security for the global payments system.

ABOUT CIS

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

Notes