Staying Safe Online

A Guide for Older People

mastercard

Staying Safe Online

Many of us are used to paying in cash or in person. However, sometimes this an option is not available, as shown during the social restrictions for COVID-19.

While making payments online might seem daunting if you have never tried it, shopping, paying bills and banking online is convenient, easy and safe if you know what to look out for.

This guide will help you understand how to shop online safely and how to protect your personal information when browsing, shopping and socialising online.

Taking just a few simple precautions can make all the difference and ensure your online experience is smooth and safe.

Mastercard does not contact cardholders to request personal information, including credit or debit card account information. If you receive an unsolicited phone call, email, text message or social media request from someone claiming to be from Mastercard, DO NOT RESPOND.

Be cautious and never respond to suspicious emails or other inquiries with sensitive information.

If you think you may have been a victim of a scam and have inadvertently disclosed your account information, contact your bank or financial institution to report the incident immediately.

Online Shopping

Shopping online allows for easy price comparisons and often saves a lot of time and effort. You can shop anytime from a variety of retailers and businesses at any time of the day.

A few easy precautions make shopping online very safe:

- Legitimate businesses generally accept electronic card payments and don't require money transfers. Not accepting payments by card is suspicious.
- Check you are dealing with a trusted and reliable business by confirming their company details and researching online feedback and complaints.
- Only enter your bank account or card payment details into a secure web page. A secure web page will have https:// at the beginning of the address bar and a picture of a locked padlock in the browser.
- Never send your bank account or payment card details via email, SMS or instant message.
- Don't overshare personal information with an online seller.

CASE STUDIES

Paul is apprehensive about online shopping after hearing that people have been scammed.

For his camera purchase from an online store, he checked whether the retailer lists contact details for enquiries and returns, has an easyto-read privacy policy and explains customer protections in place for online card purchases.

He bought a new camera which arrived in the mail a few days later. He was delighted with his purchase.

Anna bought cheap flights on the website of a travel company she had never heard of. She did not research the company further. She paid for the tickets via a money transfer because the travel company did not accept card payments. The tickets she bought turned out to be fake as the travel company was the front for a scam.

Protecting Your Information

When you are online, whether you are shopping, paying bills or just browsing the news, it is vital to take active steps to protect your personal information.

There are online fraudsters looking for people to scam out of their personal and financial data. Identity theft is very serious – a criminal can access your bank account, obtain credit cards or loans in your name and harm your credit rating and reputation.

Scammers can set up sites that may look legitimate but have been set up to trick people into disclosing their personal details and passwords.

If you are not certain about a site, don't enter your details. That includes names, addresses, phone numbers and bank details.

- You can check whether a business is legitimate by doing some online research or calling them on the phone.
- Make sure a website is secure. Look for the picture of a padlock and https:// at the address bar.
- Don't share information that could be used to guess your passwords and steal your identity. For example, don't use your birthday as a password.
- Make sure you have malware protection and anti-virus software installed on all personal devices, including your laptop, tablet and phone. Ensure you keep it up to date.
- Never send your bank or credit card details via email.

CASE STUDIES

Joanne gets a message from a friend inviting her to join a new communication app. Her friend provides a link to a non-authorised app store, telling Joanne it's the best way to download the app without having to pay. To keep her personal information safe, Joanne downloads the communication app from the authorised app store.

Margaret receives a phone call claiming to be from her Internet Service Provider. The caller tells her a virus has been detected on her computer and sends her an email with an anti-virus software download. Margaret opened it, which allowed the scammers to access her computer and steal her personal financial details. Her bank's security team was unable to contact Margaret about unusual activity on her account as she was on the phone to the fake Internet Service Provider.

- **If you receive a call from someone claiming to be a service provider, take their details and call your provider back on their public phone number, which is usually listed on a bill or their website, to double check whether it was a legitimate call.**
- **If you receive a call with an automated or pre-recorded message asking for your personal information, such as bank details or passwords, hang up immediately.**

Protecting Your Device

Protecting your personal devices in paramount to staying safe online.

- Always set a password, PIN or passcode to stop others using your devices.
- Make sure you install application and operating system updates as soon as they are available. You can use your device's automatic update feature for that purpose.
- Ensure your device does not automatically connect to new wifi networks without your express permission.
- Avoid entering any confidential or sensitive information, such as usernames, passwords, card details, while connected to unknown or public wifi networks.
- Only install apps from reputable vendors.
- For passwords, use a combination of uppercase, lowercase, numbers and symbols. Long passwords are strong, think passphrases rather than passwords. Don't reuse passwords across different accounts.

CASE STUDIES

James received an email from what he thought was his energy company, asking him to immediately pay a bill or risk disconnection. James clicked on the link and entered his credit card details to pay the bill. The email and website were fakes, designed to trick unwary customers into disclosing their credit card details. Scammers made large purchases on James' credit card.

- **Always check what follows the @ symbol in the e-mail – if it's a legitimate email, it will always replicate the company's public website address.**
- **If you are unsure about an email or a text message you received, contact the company, agency or person directly to confirm it is legitimate.**
- **Don't respond to any messages asking you to disclose your personal or financial information. Legitimate businesses do not ask for such information.**
- **Ensure you have anti-virus software on your devices and keep it up-to-date.**

Sam received a text message saying he has an unclaimed package to collect. The message asks him to click on a link to pay the delivery fee. Even though Sam doesn't remember buying anything, he clicks on the link and enters his credit card information. Unfortunately, the message was sent by scammers, who then make large purchases on Sam's credit card.

- **Be alert – if you haven't ordered any goods, you don't have to pay a delivery fee. You cannot be charged a delivery fee for something you haven't purchased.**
- **If you receive a text message like this, delete it and lock the number it came from or follow up with the official postal service.**
- **Never share your card details for transactions you have not initiatied. Ensure you have anti-virus software on your devices and keep it up-to-date.**

Scams and Phishing

Being aware of the potential for scams means you are already minimising the risk to yourself.

Scams

Being aware of the potential for scams means you are already minimising the risk to yourself.

Phishing

Phishing targets internet users via email, telephone or text message. Phishers pose as a legitimate business or institution (bank or a government agency) or as a friend or relative, to trick people into disclosing financial or personal data such as bank account or credit card details and passwords.

Tips

- Do not open suspicious pop-up windows or click on links or attachments in emails or text messages from people you don't know.
- Don't respond to phone calls asking for remote access to your computer – hang up straight away.
- Be wary of any unusual request to pay for goods or services you don't recall purchasing.
- You may be liable if you provide your payment details to a source which is fradulent – always check that the payee is legitimate.
- Don't open emails from people you don't know. Check emails purporting to be from friends or family by ensuring the email address is correct.

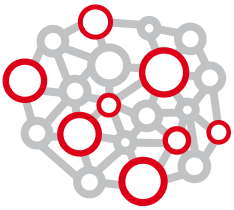
CASE STUDIES

Charles meets Marie through an online dating website. Marie tells him she is in the armed forces and on overseas duty, but has leave coming up. After emailing for a few months, Marie asks Charles to pay for flights and some medical treatment so that they can finally meet. Charles transfers money to her. Unfortunately, Marie never turns up, because she was the invention of a scammer, using someone else's name and picture to entice men on dating sites to send her money.

- **Don't send money to people you've never met in person.**
- **Romance scams are very common. Signs that someone you meet on a dating site may be a scammer:**
  - **Early professions of love and offers of marriage.**
  - **You cannot meet in person because the person claims to be working interstate or overseas.**
  - **The person is reluctant to talk on the phone.**
  - **Meeting in person requires you to send money to pay for travel or to resolve some other financial issue for the person. Ensure you have anti-virus software on your devices and keep it up-to-date.**

Peter uses social media to keep in contact with family and friends. Recently, he received a direct message on Facebook from one of his friends who he knew was travelling. In the message, the friend stated she had lost her phone, wallet and passport and asked Peter to send $100 to help her out financially. Peter thought this was odd and contacted his friend by email and text. He realised the friend's Facebook account had been hacked by scammers.

- **If you receive a request like this on social media, contact your friend directly to check it is legitimate.**



Social Media

Social media, like Facebook, Instagram and Twitter, is a great way to keep in touch with friends and family, especially with grandchildren who may be more active online.

- Privacy and security settings should enable you to control who sees what you post.
- Keep personal details such as your address, email address, phone number and birthdate, private.
- Be careful who you become friends with online, especially if you don't know them in real life. Be wary about what you share with them.
- Always look at the username of the person adding you. The use of different names to their display name, or inclusion of long strings of numbers are often telltale signs of fake accounts.

Tips

Safe Travelling

Many older people enjoy travelling. Whether interstate or overseas, a few precautions will go a long way toward protecting your digital privacy and security while you are away from home.

Tips

- Check the expiry date on your credit card to make sure it won't expire while you're travelling.
- Tell your bank your travel dates and where you are going, so it won't lock your card for suspicious payments from unusual locations.
- Many banks enable you to lock your card when not in use, set daily spending limits or prevent ATM withdrawals, which gives you extra protection if your card is stolen.
- When overseas, you may be able to pay in either Australian dollars or local currency. It often costs less to pay in the local (foreign) currency because overseas merchants can add extra charges or use a less favourable exchange rate if you pay in your home currency.
- Don't do your internet banking or make payments on public computers in hotels. Your passwords and account numbers could be captured by criminals over public networks.
- If possible, keep your phone and laptop in a safe in your accommodation when not in use.
- Make a backup of any essential data before travelling, in case your device is lost or stolen.

Online businesses are working to protect you

Online shops and businesses like banks and energy companies play an important role in keeping us all safe online by protecting their own computers, being aware of online scams and fraud, and by adopting the latest technologies to keep your personal data safe.

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

How Mastercard Helps You Stay Safe Online

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 in an SMS or email to confirm your payment. This code will never be shared with the merchant and can only be used for that one transaction.

Zero liability

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.

- You have used reasonable care in protecting your card from loss or theft; and
- You promptly reported loss or theft to your financial institution.

If you believe there has been unauthorised use of your account and you have taken these steps, rest easy knowing you have the protection of Mastercard's Zero Liability promise.

- If you lose your card or it's stolen, contact your bank immediately and suspend or cancel your card.
- Review your bank and card statement regularly and report any suspicious transactions.
- Contact your bank to discuss how you can benefit from

  3DS. For more information, go to www.mastercard.com

Where To Go For Help

In Australia

If you see any unusual or suspicious transactions in your bank statement, contact your bank immediately.

Report cybercrime or suspected cybercrime to the Australian Cyber Security Centre for investigation:
https://www.cyber.gov.au

Report suspected scams to the Australian Competition and Consumer Commission's (ACCC) ScamWatch:
https://www.scamwatch.gov.au/report-a-scam

In New Zealand

If you see any unusual or suspicious transactions in your bank statement, contact your bank immediately.

Report cyber security problems to CERT NZ:
https://www.cert.govt.nz/

Learn more about scams and how to protect yourself at Scamwatch, run by the Ministry of Business, Innovation and Employment (MBIE):
https://www.consumerprotection.govt.nz/general-help/scamwatch/identify-a-scam/is-this-a-scam/

About Mastercard

Mastercard is a global technology company in the payments industry. Our mission is to connect and power an inclusive, digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible.

Using secure data and networks, partnerships and passion, our innovations and solutions help individuals, financial institutions, governments and businesses realize their greatest potential.

Our decency quotient, or DQ, drives our culture and everything we do inside and outside of our company.

With connections across more than 210 countries and territories, we are building a sustainable world that unlocks priceless possibilities for all.

www.mastercard.com

mastercard