Staying Safe Online
Cyber Safety Guide for Small Merchants
23 billion connected devices globally

7 out of every 10 adult Australians shop online

Online spending is growing 5x faster than traditional payments

Small business accounts for 23% of online spend
Why Accept Online Payments?

These days, many people prefer the ease and convenience of electronic payments. And more and more people are paying for their goods and services online.

Accepting online payments is easy. If your business has a website for advertising products or services, then accepting online payments could be a great way to increase your business revenue. An online payment gateway makes selling and purchasing faster, easier and hassle-free.

By accepting online payments, businesses get instant payment with the added benefit of security and credibility. Since online transactions are quick and easy, online payments may influence customers to purchase on the spot.

Staying safe online for small business isn’t complex or expensive, and by following some simple tips you can greatly reduce your risk of online fraud and compromise.

- Research the various online payment options and work out which one is best for you, based on cost, convenience and safety.
- Research the various payment methods such as website, mobile and virtual terminal.
- Discuss online payment options and security with your bank.
CASE STUDY

(Fraud)

Mark owns a small online business selling hoses. Mark receives a phone order for a significant amount of stock to be shipped overseas. Mark is suspicious as the same hoses can be bought overseas, however he continues with the order. Mark is provided with two credit cards by the caller and asked to split the transaction between the two cards, which he does, and ships the stock. Later, Mark is informed by his bank that the credit cards used to pay for the goods were stolen.
Preventing Fraud

With the growth of online services, online shopping and payments, there are also increased opportunities for criminals to commit scams and fraud. Criminals rely on the anonymous nature of the internet and unsuspecting nature of small business owners and their employees. Awareness and following a few simple tips can greatly reduce this risk.

- Be cautious of suspicious orders, such as unusually large orders or those requiring urgent delivery.
- Be cautious of dispatching goods to a freight forwarding company for new clients.
- Never take payments on behalf of any other person or business.
- Ensure the billing and delivery postal codes match.
- Use tracking numbers and delivery receipts.
- Consider the use of fraud detection software.
- Talk to your bank about online authentication methods such as Mastercard SecureCode.
- Consider using a fully hosted payment gateway provider to collect payment on your behalf.
81% of hacking related breaches leveraged either stolen or weak passwords

66% of malware was installed via malicious email attachments

73% of breaches were financially motivated

Source: Verizon: 2017 Data Breach Investigation Report
Hackers seek to access networks that are not properly secured and configured, just like a burglar may break into an unsecured office. Think carefully about where you store data and how you secure it physically and electronically. Internal threats are more difficult to anticipate, but can be equally devastating to your business. Staff may remove data inadvertently or on purpose for financial gain or revenge. Promoting your trust and safety credentials to current and future customers is good for business.

- Install security software and ensure it is up to date to protect against the latest threats.
- Perform a complete virus scan on your computer at least once a week.
- Install security patches for all operating system software and application software and set them to update automatically.
- Only provide access to your computer network and data to those that need it to do their job.
- Use strong passwords and update them regularly.
- Be suspicious of unsolicited emails, messages or phone calls requesting personal or business financial information.
- Back up your data to a removable storage device such as a hard drive.
(Ransomware)

Mary receives an email with an attachment from an unknown address. Mary opens the attachment and unknowingly downloads malicious software that gives the cyber criminal the ability to take over and control her computer. The cyber criminal has locked Mary’s business files and client details, demanding payment before she can gain access to her computer and files.
Personal Accountability

The customer is an important part of the online payments ecosystem. While banks and card schemes devote a lot of effort and resources to protecting end-users, there still needs to be a degree of personal and business accountability.

As a merchant, you are the first line of defence and can help customers have a safe and secure online experience.

- Use strong passwords and don’t share them with anyone.
- Keep your computer up to date with antivirus, anti-spyware and firewall software and set them to update automatically.
- Be aware of suspicious or unusual transactions.
- Don’t provide personal or banking details to anyone over the phone.
- Don’t open emails or attachments from suspicious senders.
Phishing

Malware

Spam

DDoS

Trojan horse

Ransomware

Social engineering (impersonation)
Scams

Scams targeting small businesses come in various forms – from invoices for advertising or directory listings that were never requested to dubious office supplies that were never ordered. Small business scams are becoming increasingly sophisticated and scammers will go to great lengths to convince you that the documents they send you or the offers they make are legitimate.

Scams include false billing, overpayment, ransomware, phishing and investment scams.

Tips

☀️ Keep your office networks, computers, and mobile devices secure. Update your security software, change passwords and back up your data regularly. Store your backups offsite and offline.

☀️ Limit how many people have authority to buy or order something on behalf of your business.

☀️ If you notice a supplier’s usual bank account details have changed, call them to confirm the new details.

☀️ Don’t open an email or attachment if you’re not expecting an email or you’re unsure of who sent the email.
WHERE TO GO FOR HELP

- **Australian Cybercrime Online Reporting Network** – ACORN is a national policing initiative of the Commonwealth, State and Territory governments. It allows the public to securely report instances of cybercrime. [https://www.acorn.gov.au](https://www.acorn.gov.au)

- **Scamwatch** – A website run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams. [https://www.scamwatch.gov.au](https://www.scamwatch.gov.au)

- **Office of the Australian Information Commissioner** – The OAIC investigates possible breaches of the Privacy Act, including data breaches. Data breaches can be caused or exacerbated by a variety of factors. [https://www.oaic.gov.au](https://www.oaic.gov.au)

- **Crime Stoppers** – Operating throughout Australia, Crime Stoppers is an integral part of community safety with the information gathered and supplied by the community essential to assisting our police agencies with crime solving and prevention. [https://www.crimestoppers.com.au](https://www.crimestoppers.com.au)

- **Your financial institution** – Contact your bank or financial institution when you think your account may have been compromised and money withdrawn without your authorisation.

- **www.mastercardmerchant.com** – Supports your business by providing advice on growing your business and keeping it safe and secure.
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.

Statement of Confidentiality and Disclaimer

©2015 MasterCard. All third-party product names and trademarks belong to their respective owners. The information provided herein is strictly confidential. The information contained is MasterCard’s view only. It is intended to be used internally within your organization and cannot be distributed nor shared with any other third party, without MasterCard’s prior approval. This presentation is intended solely to facilitate discussion between the parties. MasterCard will not be responsible for any action you take as a result of this presentation, or for any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.