



DIGITAL  
MAIN ST.

tabia  
Toronto Association of  
Business Improvement Areas

# Cybersecurity: How to protect your business in 2022

Presented by DMS, TABIA and Mastercard

OCTOBER 2022



# Presenters

**DIGITAL  
MAIN ST.**



**Darryl Julott**

Managing Lead,  
Digital Main Street



**Nishant Raina**

Director, Product Management,  
Small Business at Mastercard



**Aviva Kline**

VP, Digital Payments  
& Cybersecurity Solutions  
at Mastercard



**Gina Ganahl**

VP, Product Management,  
Cyber & Intelligence  
Solutions at Mastercard



# Mastercard small business solutions overview





# The Canadian small business market remains a key economic driver



As e-commerce growth has exploded due to consumer shifts, it's become more important than ever for small businesses to move towards digitally enabled payments.



## Key economic growth

# 37.8%

Total GDP contribution<sup>1</sup>

- 81% of all small businesses are willing to integrate new technologies into their operations.<sup>4</sup>
- 61% would be willing to move away from cash, if they had other options.
- 67% of small businesses are willing to move away from cheques, if they had other options.<sup>5</sup>



## Digital is the path forward

# 10.4%

Projected increase in e-commerce sales in 2022 YoY<sup>3</sup>

- 90% of small business owners moved a portion of their operations online.<sup>4</sup>
- 40% of small businesses accelerated technology investments (sales and customer service).<sup>4</sup>
- 81% are planning to offer contactless service.<sup>4</sup>
- 51% of small businesses are looking to secure digital payments.

### Sources:

1. Government of Canada-Key Small Business Statistics (Innovation, Science, and Economic Development Canada).
2. Salesforce, How Do Small Businesses Earn Customer Loyalty 2020.
3. eMarketer 2021.
4. Small Business Trends-Salesforce 2021.
5. 2018 Payments Canada-Payments Pulse: SMB Survey Edition.



# Small businesses are critical to the Canadian economy

- **98.1% of businesses** in Canada are small businesses
- Small business owners employ **almost 63.8% of Canadians**
- **95% of consumers say trust** is why they are more likely to be loyal to a small business<sup>1</sup>

**1.2M**

**Small businesses in Canada.<sup>2</sup>**



Sources:

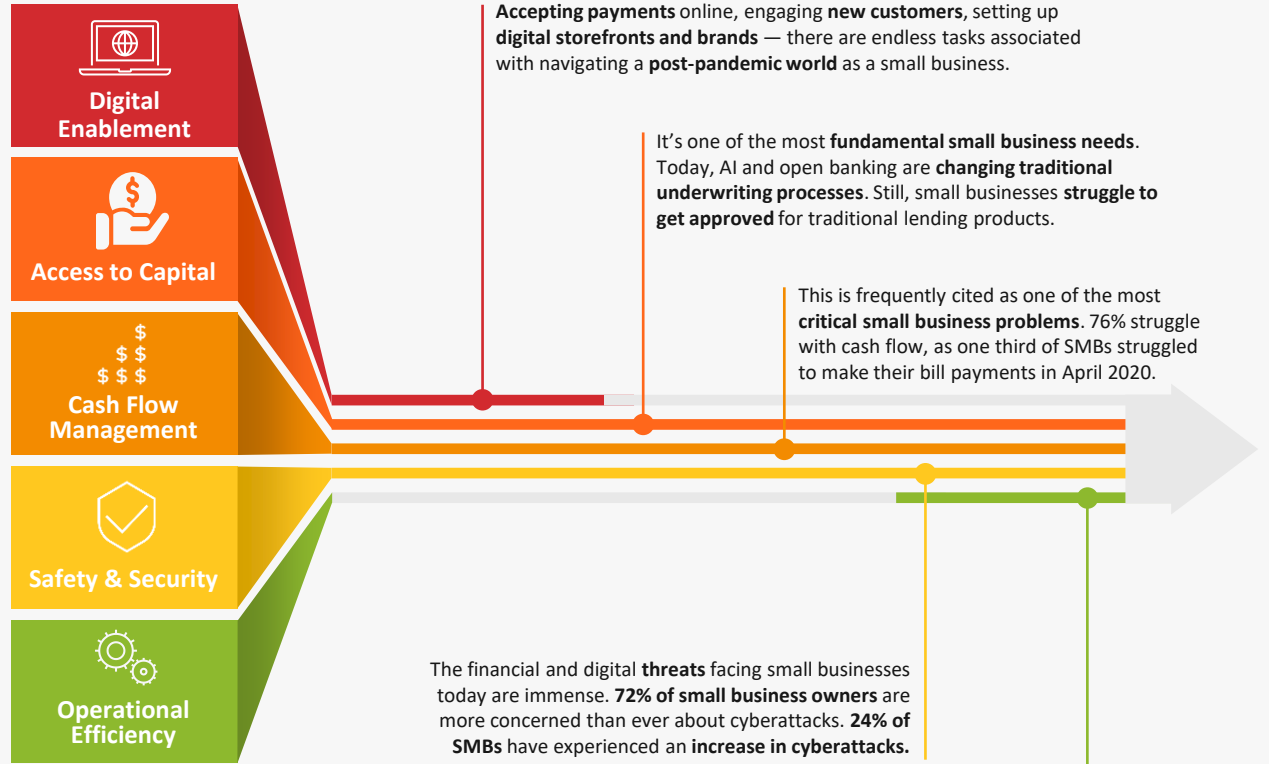
1. Government of Canada-Key Small Business Statistics (Innovation, Science, and Economic Development Canada).
2. Statistics Canada. "Analysis on small businesses in Canada, first quarter of 2022", March 2022



# The small business journey

In a post-pandemic world that's undergone **rapid technological change**, small businesses face a complex set of problems. Many predate the pandemic, like **managing cash flow**, while others are new, like **accessing new payment networks, fighting ransomware, and utilizing open banking data** for better, more consistent access to lending products.

This journey explores some of these challenges and how Mastercard is **helping small businesses solve them**.



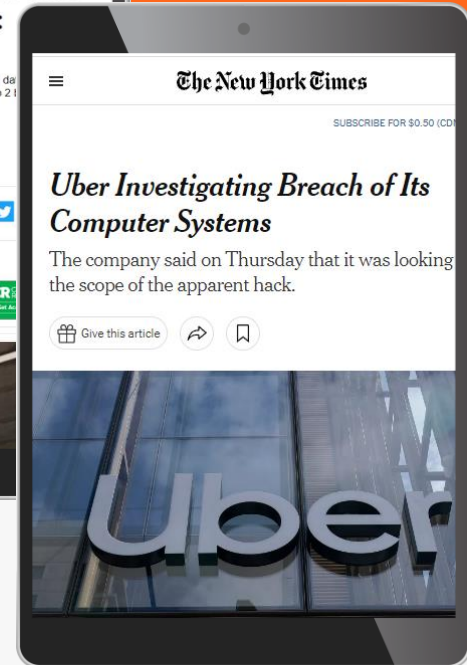
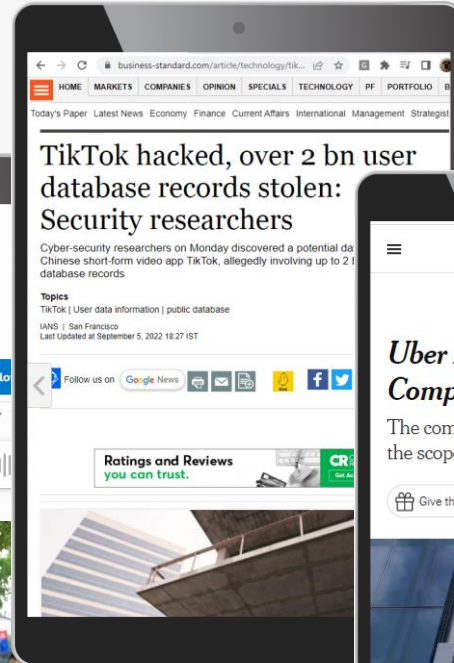
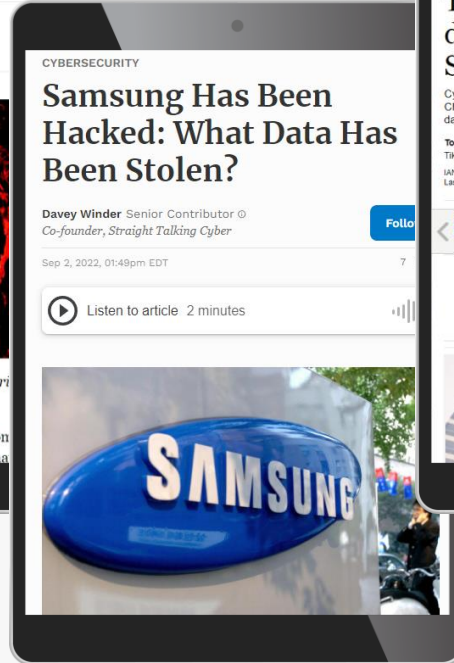
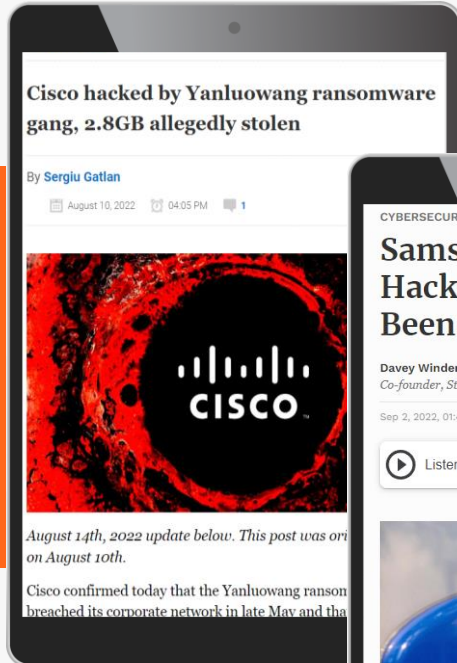
# Cybersecurity for small business

Trends, threats,  
best practices and  
free resources





# The headlines can be scary!





Cyberattacks have negative long-term implications for a company's reputation and relationship with customers

#1

Security and privacy safeguards are the most important factor for consumers when deciding to do business with a company

60%

of consumers are unlikely to shop with companies that have a significant data breach

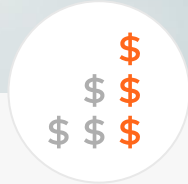
88%

of customers won't use a brand they don't trust with data<sup>1</sup>

Sources:  
The Great Data Exchange, Become 2020.  
1. <https://techwireasia.com/2021/02/customers-are-losing-patience-with-data-security-issues/>



# Cyberattacks lead to significant financial costs for Canadian businesses



**\$6.75M**

average cost<sup>1</sup> of a data breach in Canada per incident in 2021, a 20% increase since 2020



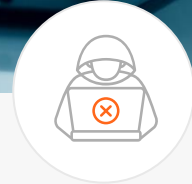
**60%**

of all data breaches happen via third-party vendors<sup>3</sup>



**87.5%**

of Canadian organizations experienced at least one cyberattack within a 12-month period in 2021<sup>1</sup>



**\$3.12B**

Canadian losses<sup>4</sup> to cybercrime every year, which is 0.17% of GDP

Sources:  
1, 2. IBM Security Report  
3. Reciprocity  
4. Intel Security, Net Losses – Estimating the Global Cost of Cybercrime



Mastercard is committed to helping small businesses mitigate cyber risk



The consequences of failing to take proactive cybersecurity actions can be disastrous.

*“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”*

**Stephane Nappo**  
Global Head Information Security,  
Société Générale International Banking



# Focus on seven key issues for culture change



**Authentication**



**Data Backup and Recovery**



**Software Updates**



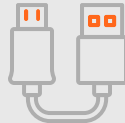
**Social Engineering**



**Phishing**



**Ransomware**



**USBs**





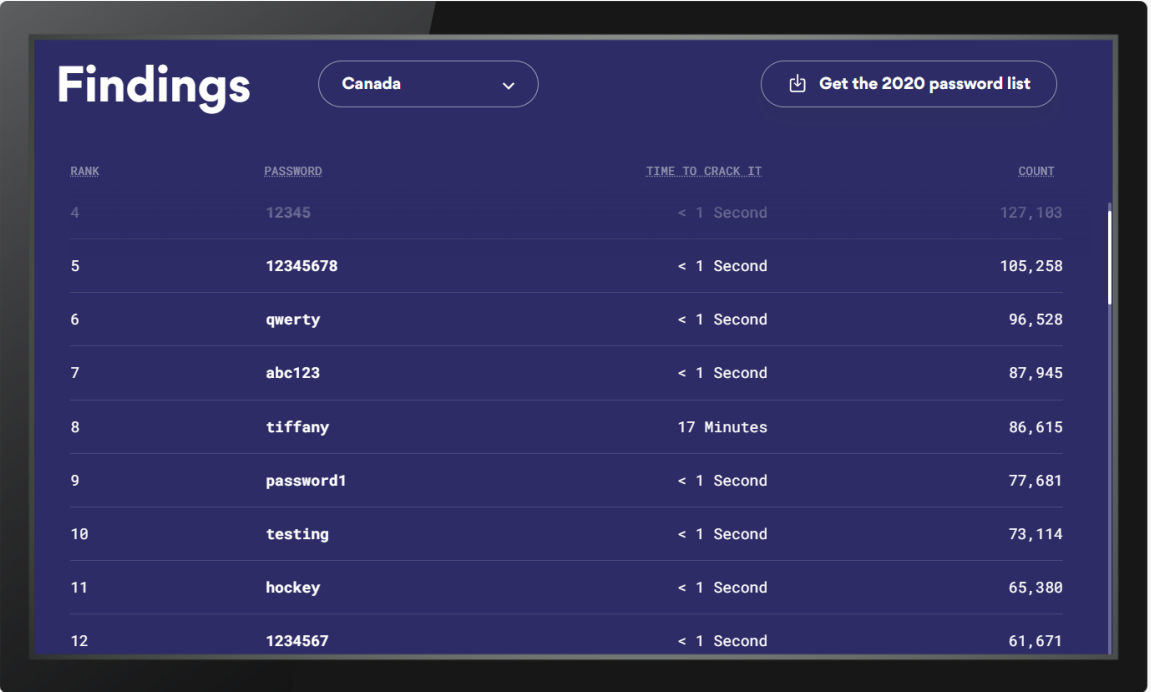
# Authentication

# 63%

of data breaches result from weak or stolen passwords<sup>1</sup>

# 570,000

Canadian passwords are 123456. This takes less than a second to crack<sup>2</sup>



RANK	PASSWORD	TIME_TO_CRACK_IT	COUNT
4	12345	< 1 Second	127,103
5	12345678	< 1 Second	105,258
6	qwerty	< 1 Second	96,528
7	abc123	< 1 Second	87,945
8	tiffany	17 Minutes	86,615
9	password1	< 1 Second	77,681
10	testing	< 1 Second	73,114
11	hockey	< 1 Second	65,380
12	1234567	< 1 Second	61,671



# Authentication: Solutions



Strengthen your passwords by using a “passphrase”:  
A combination of words with letters that only you know  
(e.g., a line from your favourite TV show, movie or song).



Use a unique password for each account:  
**Don't reuse passwords!**



Enable two-factor authentication:

- Two-factor requires you to input a unique code that is sent to your mobile device for each new login.
- Two-factor authentication creates an important security link between the password and the person.



# Software updates

# 77%

of attacks in 2017 exploited gaps in software already on computers<sup>1</sup>

A patch is a set of changes to an operating system, program, app or its supporting data designed to update, fix or improve it. This includes fixing security vulnerabilities and other bugs.

Failure to patch systems in a timely fashion can leave your operations vulnerable and exposed.



# Software updates: Solutions



When you receive a notification to update to the latest software version, it's best to update right away

- Turn on the auto updates whenever it is offered
- A best practice is to assign one person to manage updates for all company computers

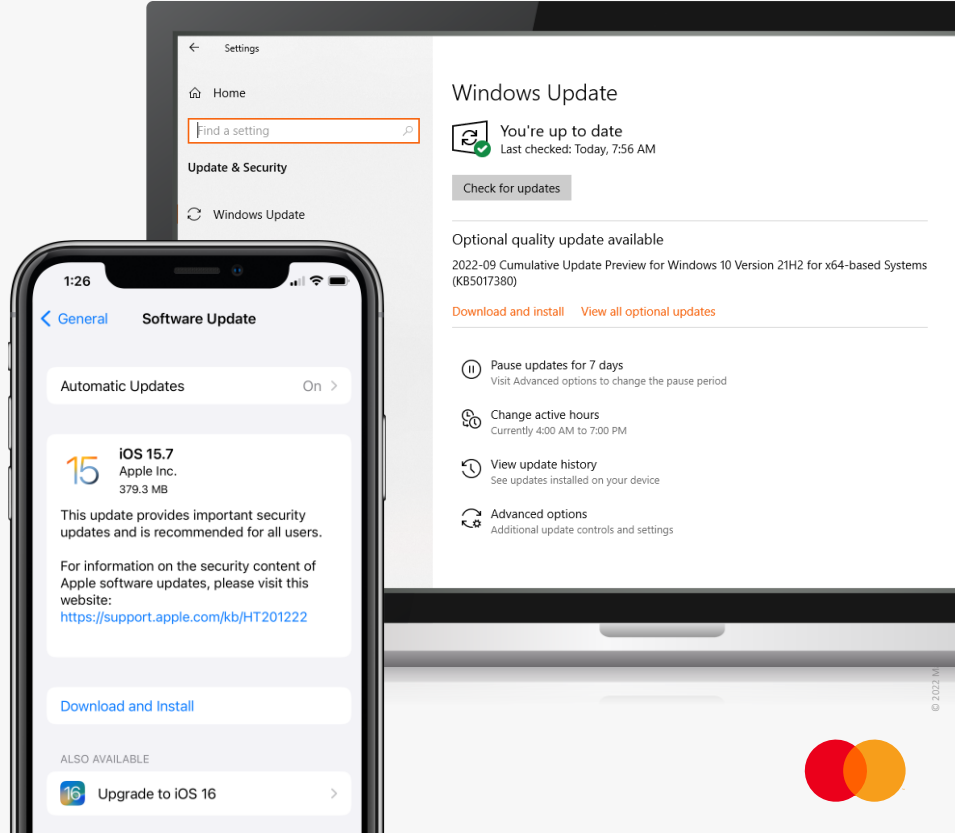


Updates are issued often for programs like Microsoft Word and Excel, as well as your computer operating system like Windows or MacOS



Update all software and apps

- Both those issued by the company and those downloaded by employee
- These updates often include security patches



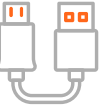


# USBs and removable media



# 27%

of malware infections originate from infected USBs<sup>1</sup>

USB drives can be useful for sharing files between computers, but they can also be used to deliver viruses and malware. There's no way to tell where the drive has been or who may have compromised it.



## Solutions

-  Introduce easy-to-use alternatives to USB drives, such as cloud-based file-sharing services so that USB drives are less necessary.
-  Use good judgment: If you don't know where the drive came from, don't plug it in.





# Data backup and recovery

# 21%

of ransomware attacks are backup systems targeted until they were unusable<sup>1</sup>

Data backup and recovery is the process of creating and storing backup copies of data to safeguard businesses from data loss due to breaches, external attacks, software crashes and hardware failures.<sup>2</sup>



## Solutions

- ✓ Separate the backup infrastructure from the active directory
- ✓ Since ransomware attacks often propagate on the same operating system, it may be worthwhile to adopt a different operating system for the backup infrastructure
- ✓ To further reduce the risk of an administration account being compromised, backup administration access should also be strengthened, for example with multi-factor authentication (MFA).





# Phishing

# 91%

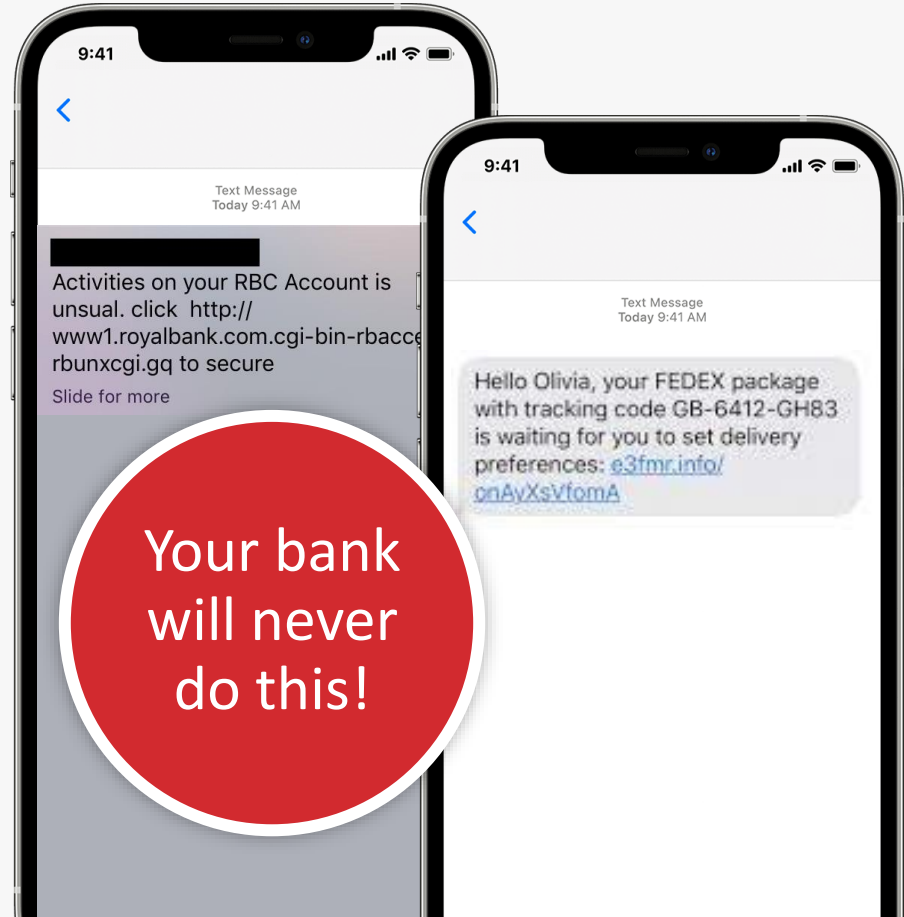
of all cyberattacks start with a phishing email<sup>1</sup>

A phishing email may look like a real message. But opening it may result in downloading software viruses or giving attackers access to your data.

- Everyone receives phishing emails.
- Awareness is the best defense against phishing

Once you have been caught in a phishing net, your systems may become infected with ransomware.

Ransomware is a type of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.



Your bank will never do this!



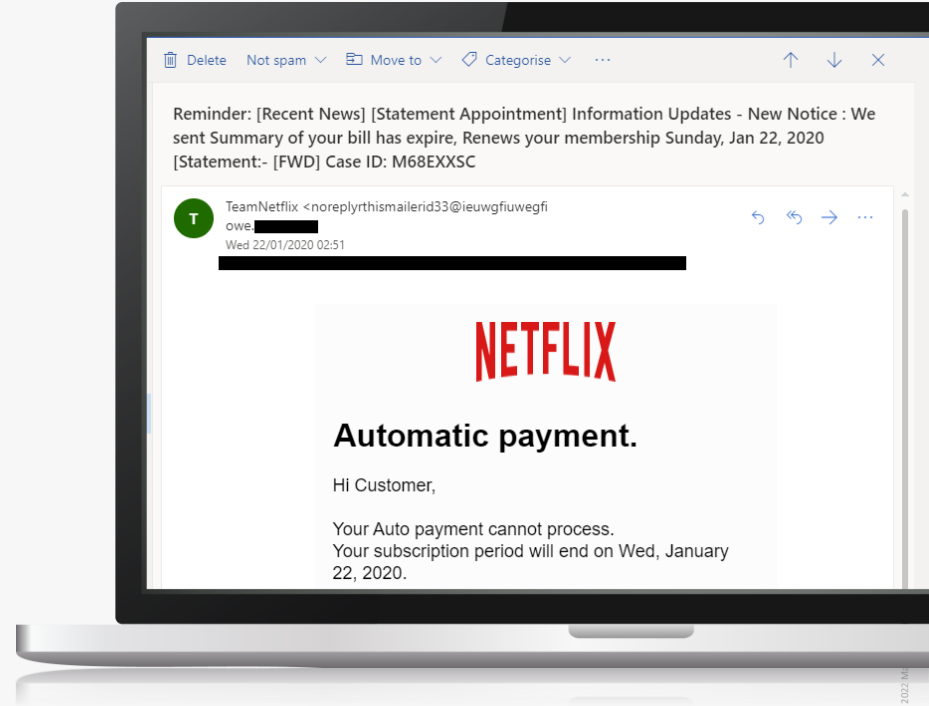


# Phishing: Solutions

- ✓ Check the sender's email address and any other identifying information (e.g., company logo, address and contact details) for any inconsistencies or signs it may be fake.
  - Details may often look similar but be slightly off.
- ✓ If you are not familiar with the email sender, do not click any links or download any attachments in the email.
- ✓ Delete any suspicious emails and immediately empty your trash.
- ✓ Back up data often in case your data is taken hostage.

**NO MORE RANSOM!**

<https://www.nomoreransom.org/en/index.html>





# Social engineering




The practice of obtaining confidential information by manipulation of legitimate users is called social engineering.<sup>1</sup>

## Common patterns:

<b>Fear as motivator</b>	<b>Urgent requests</b>	<b>Irresistible opportunities</b>
--------------------------	------------------------	-----------------------------------



## Solutions

-  Slow down and don't let messages of urgency influence you. Always take the time to review the details carefully and research the facts before you take any action.
-  Be wary of downloading free apps, files, programs, software or screensavers.
-  Install antivirus, antispyware and firewalls purchased from trusted retailers or suppliers.



Sources:  
1. <https://www.getcybersafe.gc.ca/en/blogs/understanding-how-social-engineering-works-cyber-scams-three-tactics-watch-out#defn-social-engineering>



# Ransomware

- Ransomware is a form of malware that infects your computer or device.
- When ransomware takes control of your computer or device, it locks you out of that computer, device or certain files entirely.
- Now bad actors will ask a hefty amount from organizations to get their critical assets and information back.

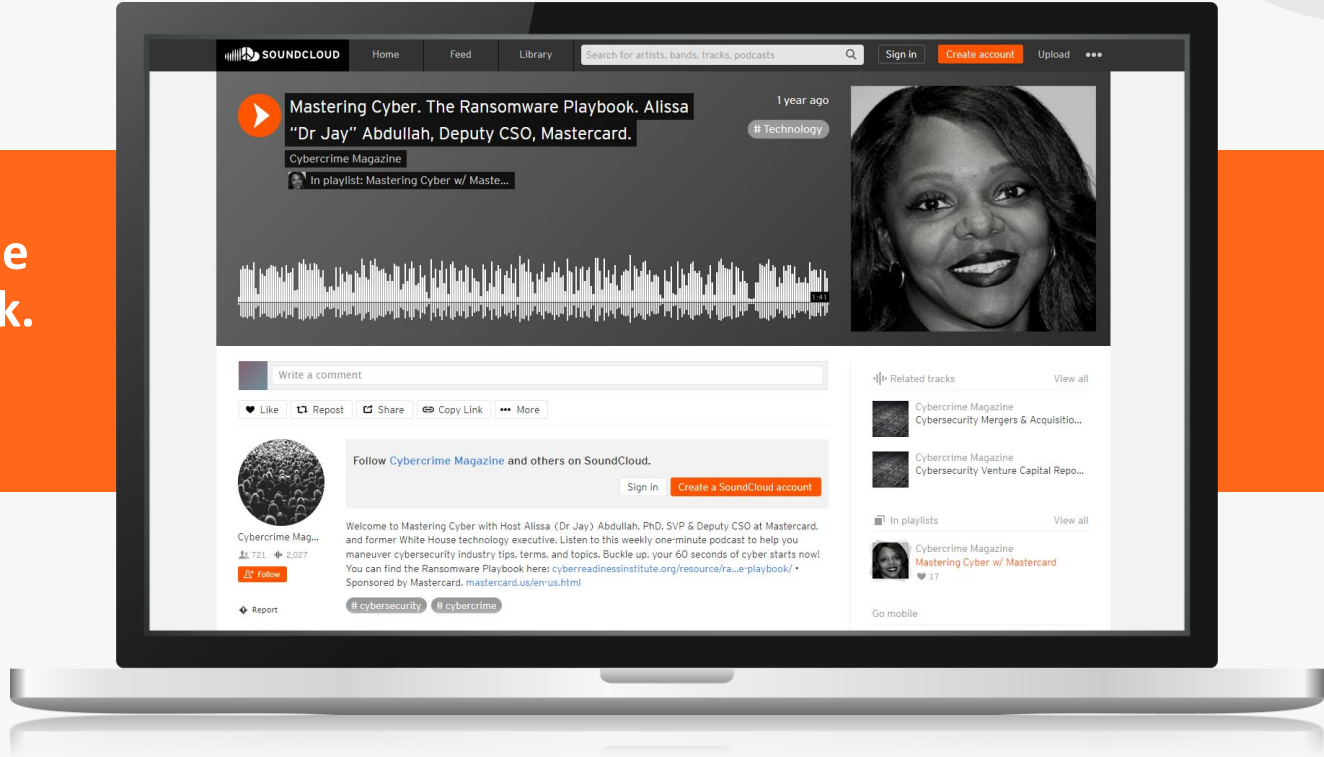
## Solutions

- ✓ Avoid suspicious downloads, as cyber criminals commonly spread ransomware through email attachments, infected programs and compromised websites.
- ✓ Regularly back up your files.
- ✓ Keep your operating system updated.



# Thoughts on ransomware by Alissa “Dr. Jay” Abdullah, Deputy CSO, Mastercard

**Dr. Jay’s insights on the  
Ransomware Playbook.**  
[Click here to review.](#)



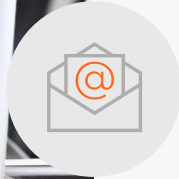
# Best practices and tips



- ✓ Use two-factor authentication whenever available
- ✓ Don't reuse the same passwords across multiple sites
- ✓ Use strong passwords



- ✓ Keep software up to date with the latest patches
- ✓ Consider automatic updates when available
- ✓ Back your data up regularly
- ✓ Share data in the cloud rather than USBs to enhance security



- ✓ Avoid clicking on links and attachments in emails
- ✓ If you weren't expecting the email, verify using a trusted phone number
- ✓ Don't be rushed by a sense of urgency in the message
- ✓ Listen to your gut: If something feels off, delete the message





95%

of cyber breaches are  
caused by human  
error<sup>1</sup>





# Mastercard Trust Centre

Offers centralized access to free education, resources and tools, plus low-cost products designed to help small businesses secure their cyber ecosystems.

## Our mission

To bring the Mastercard Trust Centre to every small business, everywhere, enabling them to feel more secure and better equipped to thrive against uncertainties.



Free cybersecurity education, resources and tools to fit every level of expertise



### LEARN THE BASICS

"I'm a beginner who's feeling overwhelmed."



### EXPAND YOUR KNOWLEDGE

"I'm fairly experienced but want to learn more."



### MASTER YOUR SECURITY

"I'm an expert looking to keep a step ahead."

Each Learning Journey Includes

**Cybersecurity core concepts. Cyberattack methods. Protect your business.**

**Mastercard Trust Centre in English**

[Click here](#)

**Mastercard Trust Centre in French**

[Click here](#)



# Mastercard Trust Centre Resources and tools

We make the learning journey simple by providing information, research and solutions in multiple formats to best help users learn about and implement each topic.



Podcasts



Videos



Whitepapers



Articles



Infographics



Toolkits

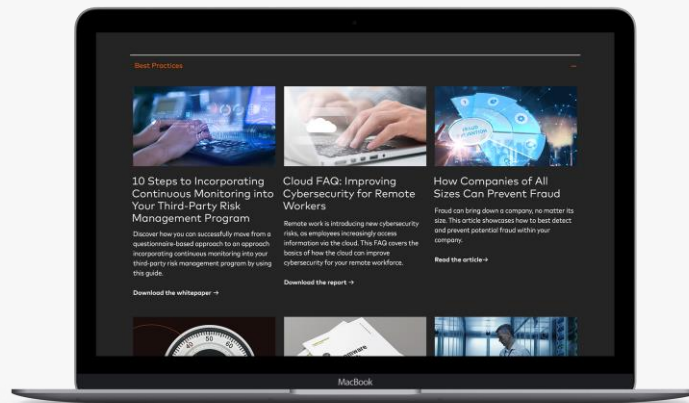
Content from Mastercard and trusted sources

**CYBER READINESS**  
INSTITUTE



**NATIONAL  
CYBERSECURITY  
ALLIANCE**

Plus, many additional trusted sources



# CYBER READINESS

## INSTITUTE

The Cyber Readiness Institute focuses on four core issues for culture change to improve your business's cybersecurity



Authentication



Phishing



Patching



USB Use

## Free Cyber Readiness Institute resources

### Starter Kit:

<https://cyberreadinessinstitute.org/starter-kit/>

### Cyber Readiness Program:

<https://cyberreadinessinstitute.org/the-program/>

### Cyber Leader Certification Program:

<https://programs.cyberreadinessinstitute.org/courses/cyber-leader-program>

### Ransomware Playbook:

<https://cyberreadinessinstitute.org/quick-facts-from-the-ransomware-playbook/>

Visit **BeCyberReady.com** for even more resources, preventative measures and a practical incident response plan.





Practical free tools and resources designed to help small businesses improve cybersecurity, all in one place



Learning portal



Handbook



Community forum

Addresses the most common cyber risks affecting small businesses and allows you to focus on your core business objectives.

Visit: <https://gcatoolkit.org/smallbusiness>

Visit: [Cyber Basics for Small Business Training](#)

Failure to perform basic cybersecurity best practices plays a part in a high proportion of ransomware attacks.



Join us for a free webinar

## Selling Online: How to improve online experience and security

Learn how to protect your small business from the most common cyber risks, and challenges that small businesses face with Mastercard Canada.

When: Tuesday, October 18, 2022

Time: 1:00pm to 2:15pm EDT





# Questions



# Appendix



# Fundamentals of cybersecurity:

## CIA triad

### Confidentiality

Confidentiality is an organization's efforts to keep data secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data — whether intentional or accidental.

### How to maintain confidentiality

- Only authorized personnel have access to data based on the principle of least privilege
- Classify and label restricted data
- Enable access control policies
- Encrypt data both at rest and in transit
- Use multi-factor authentication (MFA) systems



# Fundamentals of cybersecurity:

## CIA triad

### Integrity

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate and reliable.

An attacker may bypass an intrusion detection system (IDS), change file configurations to allow unauthorized access or alter the logs kept by the system to hide the attack.

### How to maintain integrity

- Use intrusion detection systems (IDS) to prevent unauthorized access to data
- Use hashing algorithms such as SHA-1, SHA-2
- Use digital certificates or digital signatures
- Encrypt data both at rest and in transit
- For websites, employ trustworthy certificate authorities (CAs)



# Fundamentals of cybersecurity:

## CIA triad

### Availability

Availability involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate and reliable.

An attacker may bypass an intrusion detection system (IDS), change file configurations to allow unauthorized access or alter the logs kept by the system to hide the attack.

### How to maintain availability

- Use intrusion detection systems (IDS) to prevent unauthorized access to data
- Use hashing algorithms such as SHA-1, SHA-2
- Use digital certificates or digital signatures
- Encrypt data both at rest and in transit
- For websites, employ trustworthy certificate authorities (CAs)

