CAPITAL
THAT
WORKS

Fraud and Cyber Security Insights: Keeping Your Organization Safe

OCTOBER 2021

™ Trademark of The Bank of Nova Scotia

Scotiabank®

Agenda

01 Cybercrime Landscape

02 Why does someone commit fraud?

03 Common Types of Fraud

04 Fraud & COVID-19

05 Best Practices

06 What You Can Do

07 Additional Resources

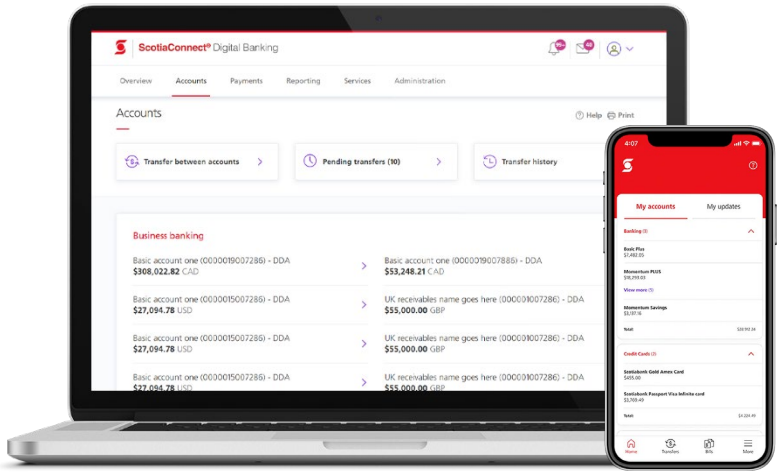
01

Cybercrime Landscape

Cybersecurity Landscape

THE CYBERSECURITY LANDSCAPE REMAINS EXTREMELY FLUID WITH NEW PLAYERS, NEW TECHNOLOGIES AND NEW ATTACKS.

- A **new virus** is created every 5 seconds.
- **Only 10%** of cybercrimes are reported.
- The average cost of a data breach in 2020 exceeded **$150 million.**
- Cybercrime will cause **$6 trillion** in damages by 2021.
- The cybersecurity market will be worth **$300 billion** by 2024.



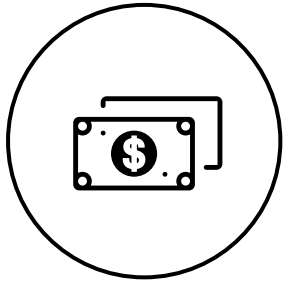
We protect **$1.2 trillion** in assets, and information for over **25 million customers** around the world.

Source: Herjavec 2019 Attack Surface Summary

Fraud is Profitable

CYBERCRIME IS EVEN MORE LUCRATIVE THAN THE COMBINED REVENUES OF APPLE, AMAZON, FACEBOOK, TESLA & MICROSOFT IN 2019 ($761 BILLION).

CRIME	ANNUAL REVENUE
Illegal Online Markets	$860 billion
Trade secret/IP Theft	$500 billion
Data Trading	$160 billion
Crime-ware/CaaS	$1.6 billion
Ransomware	$1 billion



= $1.5 trillion

Source: https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/

The Evolving Landscape

THERE ARE MORE POTENTIAL TARGETS FOR HACKERS THAN EVER BEFORE

- By 2022, there will be a predicted **6 Billion Internet users**
- Data volumes online were **50 times greater** in 2020 than in 2016.
- The amount of data stored in the cloud will be **100 times greater** this year than 2020.

THE VOLUME, COMPLEXITY AND FREQUENCY OF ATTACKS CONTINUES TO GROW

- More than **half a billion** wearable devices will be sold worldwide this year (2021). Wearables include smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.
- Over **20 million connected cars** with built-in software-based security technology were shipped by 2020.

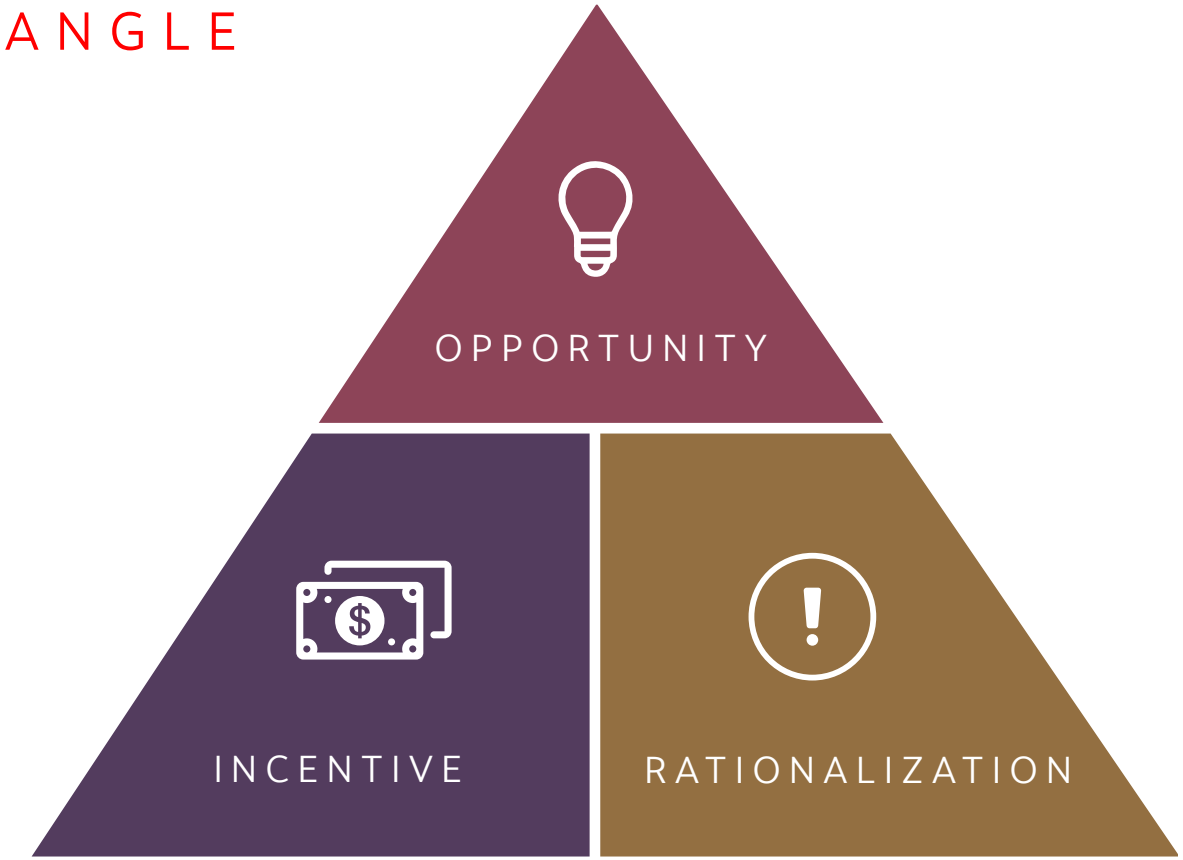
Source: Herjavec 2019 Attack Surface Summary

02

Why does someone commit fraud?

Why does someone commit fraud?

THE FRAUD TRIANGLE



03

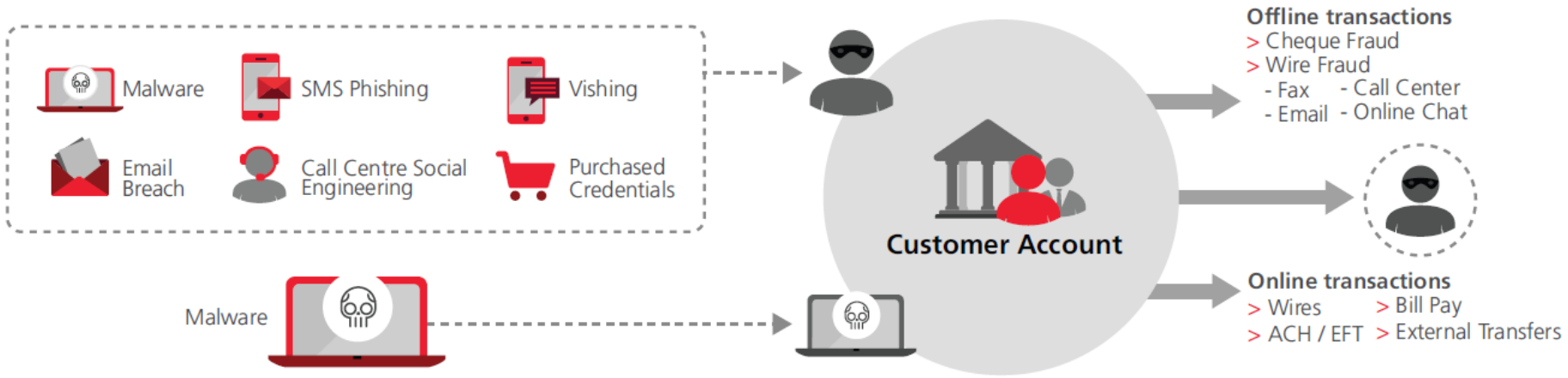
Common Types of Fraud

Fraud Awareness

Prevalent online threats that can impact your business include: Phishing, Malware and Business Email Compromise.

- Looking to protect your business from online threats?
- Keep this step-by-step guide nearby to help remember best practices:

COMMON FRAUD EXPLOIT PATHS



PREVENT IT!

- > **Call a known contact** within the firm
- > **Confirm change** of bank account
- > **Check invoices** for irregularities
- > Have a **payment approval process**
- > Look out for **different contact information**
- > Designate a **single point of contact**

RED FLAGS

- > **Variations of email address** and domain identifiers
- > **Requests to contact suppliers** via the information on received correspondence
- > Requests for immediate, urgent **payment changes**
- > **Urgent and highly confidential** requests of fund transfers
- > **First time payment** to a new beneficiary
- > **The timing** of the fraudulent instructions is often late afternoon on a Friday

Common Types of Fraud

- Business Email Compromise
- Ransomware
- Phishing
- Cheque Fraud
- Malware
- Credit Card

Business Email Compromise

Business Email Compromise (BEC) scams are a type of **payment fraud** that involves the compromise of legitimate business email accounts for the purpose of conducting an unauthorized wire transfer.

Business Email Compromise

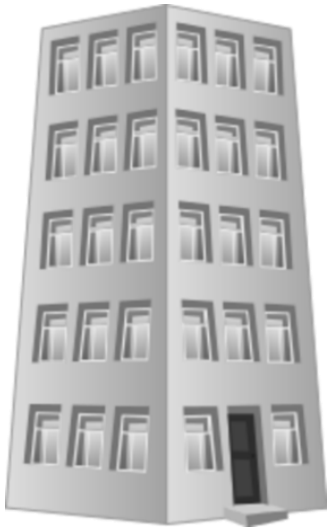
HOW IT WORKS

- Your vendors' or your own **executive's email is hacked** to request the wire payment.
- Your **employee initiates a wire payment through ScotiaConnect** believing they are paying a legitimate vendor or other entity (Lawyer, M&A payee).
- Your **employee does not verify the legitimacy of the email** instructions with the vendor before sending the wire payment.
- **You do not detect that the email instructions are fraudulent** until after large or multiple payments have been sent.

Basic Transaction Flow

Requestor:
i.e. Vendor or Executive

Customer:
i.e. YOU



Scotiabank

Beneficiary Bank

Types of Business Email Compromise

VENDOR/BENEFICIARY CHANGE

"Send payment to our new account"

You get an email that looks like it's from your supplier – but it's actually from a fraudster. They tell you their banking information has changed and ask you to send payments to a different account.

jsmith@vendorInc.com	*instead of*	jsmith@vendorinc.com
jsmith@vend0rinc.com	*instead of*	jsmith@vendorinc.com

CEO SCAM

"Wire funds to me right away"

Scammers email you posing as the CEO or other senior-level executive.

They claim to need money for a business opportunity, emergency, or another urgent matter.

They ask you to wire funds immediately to an unfamiliar account.

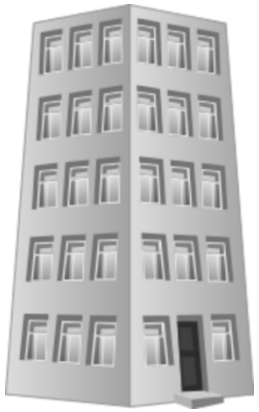
Vendor/Beneficiary Change

Requestor:
i.e. Vendor

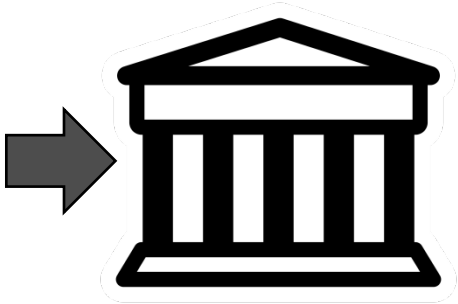
jsmith@vendorinc.com

jsmith@vend0rinc.com

Customer:
i.e. YOU



Scotiabank

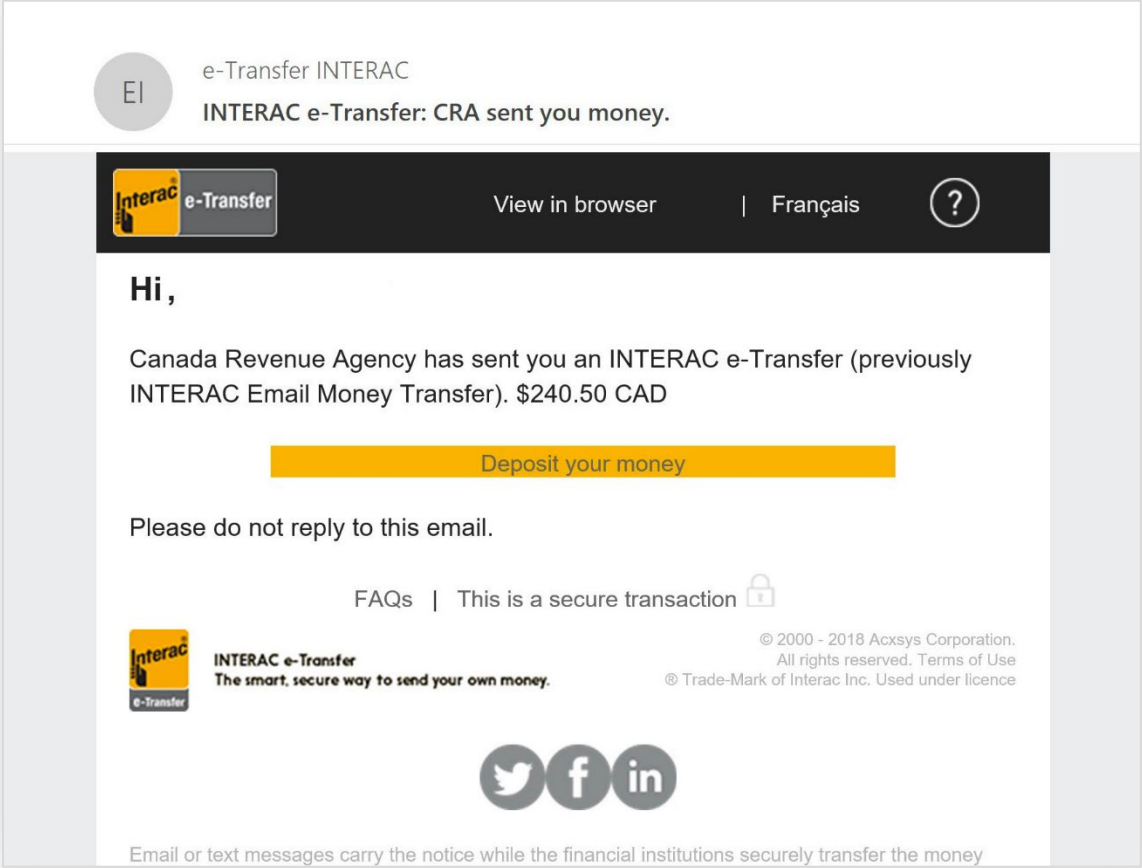


Beneficiary Bank

Types of Business Email Compromise

SPOOFED EMAIL ACCOUNTS

- The email header is disguised so it looks like the email is coming from a legitimate account.
- Only when you hit ‘Reply’ can you see it is a completely different email address.



Examples of Business Email Compromise

PAYROLL

- A hacker emailed the payroll department advising them of a change in banking information.
- The payroll employee believed the hacker was a real employee, changed the beneficiary banking information and the payment was made.
- Fraud was identified and the funds were lost ($18k).

VENDOR

- A vendor email was hacked and a fraudulent email was sent to a bank customer.
- The customer unsuspectingly updated the vendor payee information and made payments.
- Fraud was caught by the receiving bank and funds were recovered ($63k).

WIRE TRANSFERS

- The CEO's email was hacked and a fraudulent email request for urgent wire transfer was sent to AP Department.
- An entry-level AP clerk took the email as credible and processed payment.
- Fraud was caught by the bank fraud team funds were recovered ($1 MM).

Phishing

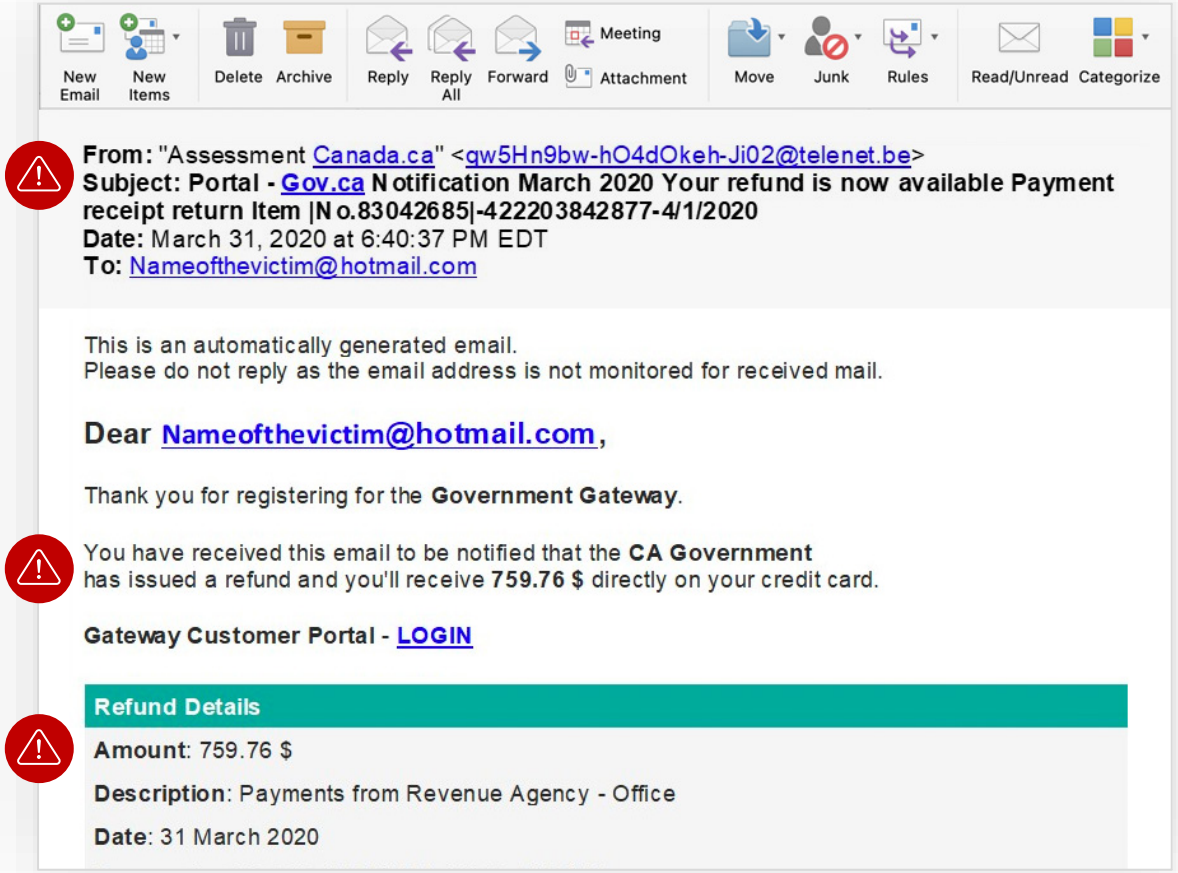
Phishing is the **fraudulent practice of sending emails** claiming to be from reputable companies in order to obtain sensitive information like **usernames, passwords, and credit card numbers** from unsuspecting individuals.

Criminals can carry out Phishing by phone (vishing), SMS texting (smishing) and email hacks.

Example of Phishing

RED FLAGS TO LOOK FOR

- **Check the "From" address.** By hovering your mouse over the name, you can see the actual email address.
- Be skeptical of **suspicious subject lines**
- Take notice of **incorrect abbreviations, grammar and spelling errors**
  - "CA Government" would be spelled as "Canadian Government"
  - Dollar sign is *after* the dollar amount on an English-written email)



Malware

This is a type of cyber attack in which malware or **malicious software** performs activities on the victim's computer system, usually without his/her knowledge.

Ransomware

This is a type of **malicious software** designed to block access to a computer system until a sum of money is paid. Although ransomware is usually aimed at individuals, we are starting to see businesses targeted as well.

Common Red Flags

SOMETHING DOESN'T LOOK RIGHT

YOU MAY NOTICE:

- **Minor changes** in the email address or domain name.
- **Differences** in the invoice, letterhead, fax, or email template.
- **Poor grammar** or spelling.
- **An unfamiliar supplier** or vendor.
- **Altered** beneficiary and transaction information.

SOMETHING DOESN'T SOUND RIGHT

BE WARY IF YOU DETECT:

- A strong sense of urgency, **"You must act immediately."**
- The demand for secrecy, **"Keep the payment details confidential."**
- Communication challenges, **"I can't talk, I can only email."**
- Contact information that is different than what you have on file.
- A desire to skip regular approval processes.

Cheque Fraud

Fraudsters continue to target new technologies but cheque fraud is still on the rise.

Cheque Fraud

CHEQUE FRAUD OCCURS WHEN:

- An **unauthorized cheque** is paid against an issuer's bank account
- An individual uses a cheque to **get funds they're not entitled to**
- A cheque is negotiated **without the knowledge or authorization** of the account holder

THE MAIN TYPES:

1. Counterfeit
2. Altered
3. Forged
4. Duplicate Presentment
5. Forged Endorsement/Intended Payee not Paid

Common Types of Cheque Fraud

CHEQUE TYPE	DEFINITION	PAYMENTS CANADA RETURN TIME FRAME
Counterfeit Cheque	Counterfeit cheques generally have slight differences compared to legitimate cheques. The color, logo, font, security features may vary.	24 hours
Altered Cheque	Materially altered cheques are valid and authorized items but contain changes to the payee's name; date; amount (figure/words); time of payment.	90 days
Forged Signature	Signature on the face of a cheque that is not the signature of the authorized signatory or signature that is written on or applied to an item without the drawer's authority.	24 hours
Forged Endorsement	The cheque is endorsed and cashed by an unauthorized individual, other than the intended payee.	6 years
Intended Payee not Paid	A cheque can be returned with the reason 'Intended Payee Not Paid' when the cheque is negotiated by an unauthorized party, other than the intended payee.	6 years
Duplicate Presentment	The type of fraud is made possible through new digital deposit channels such as Mobile and Online Business platforms. An individual or entity deposits an image through the digital channel one or more times, after which the item is presented through an alternate channel in paper form such as an ABM, Branch or Night Deposit.	90 days

* Timeframe starts from when cheque was negotiated and has cleared the account.

Cheque Fraud

RED FLAGS

1. The writing and spacing on the cheque looks different
2. The cheque is made out to an unfamiliar vendor or employee
3. The cheque is for an unexpected amount

RECOMMENDED CLIENT PREVENTATIVE MEASURES

- Use cheque fraud detection services: **Subscribe to services** such as Positive Pay with Payee Match.
- Sign up for electronic payments: **Set up and use ScotiaConnect** for online bill payments, Electronic Funds Transfers (EFTs) or wire payments.
- Reconcile records frequently: **Daily reviews (if possible)** of bank account balances, issued and paid cheques and account transactions.

Positive Pay and Positive Pay with Payee Match

CHEQUE FRAUD

- **Positive Pay** enables customers to stay on top of their cheque processing, with scheduled Paid Cheque and Outstanding Issued file transmissions, and online cheque image, search and reporting features. With our “Negative Pay” feature, customers can conveniently return cheques online.
- The **benefits of this Positive Pay** are realized by every market segment - the larger the market segment, the greater the time savings, making it ideal for businesses with 250 or more cheques per month and/or an in-house cheque-based payroll.
- **Positive Pay Service with Payee Match** is a comprehensive fraud detection service that provides customers with all of the fraud protection features of **Positive Pay** (serial number, amount, and issued versus clearing date verification) and the added protection of Payee Match, which includes the ability to detect alterations to the payee information of a clearing cheque.

Credit Card

Anytime your credit card or number is used without permission – it's **card fraud**. From small business to large enterprises, companies of all sizes can become victims of card fraud.

Credit Cards

HOW YOU CAN MINIMIZE FRAUD RISK

- **Give cards only to the employees** who need them.
- Ensure **HR informs the card administrator** of departing employees and recovers the cards.
- Set transaction and **monthly dollar limits** for cardholders.
- Implement **Merchant Category Code (MCC) restrictions**.
- Establish **authorization controls** and trending analysis.
- **Monitor cardholder spending**.

04

Fraud & COVID-19

Pandemic Cyber Threats

Canadians lost over **$7.2 million** to COVID-19 online scams.[1]

PHISHING SCAMS

Cybercriminals are tricking people into revealing personal information and clicking on malicious links using emails that impersonate the World Health Organization and other public health agencies.[2]

FAKE SHOPS & SITES

UK authorities shut down 2,000+ COVID-19 online scams including fake online shops, malware distribution sites, phishing sites and advance-fee frauds.[3]

CERB FRAUD

Cybercriminals are sending fraudulent texts and emails to trick Canadians into believing they received the Canada Emergency Response Benefit (CERB) and need to provide personal information or click on a malicious link.[4]

GOVERNMENT ACCOUNTS HACKED

The Government of Canada reported 9,000+ accounts compromised due to a weakness in their systems. Cybercriminals used **credential stuffing**, where they run stolen usernames and password from previous attacks.[5]

1. Canadian Anti-Fraud Centre (March 2021), cbc.ca 2. Canadian Bankers Association, cba.ca 3. ZDNet (April 21, 2020), zdnet.com 4. Canadian Bankers Association, cba.ca 5. Government of Canada (Aug. 15, 2020), canada.ca

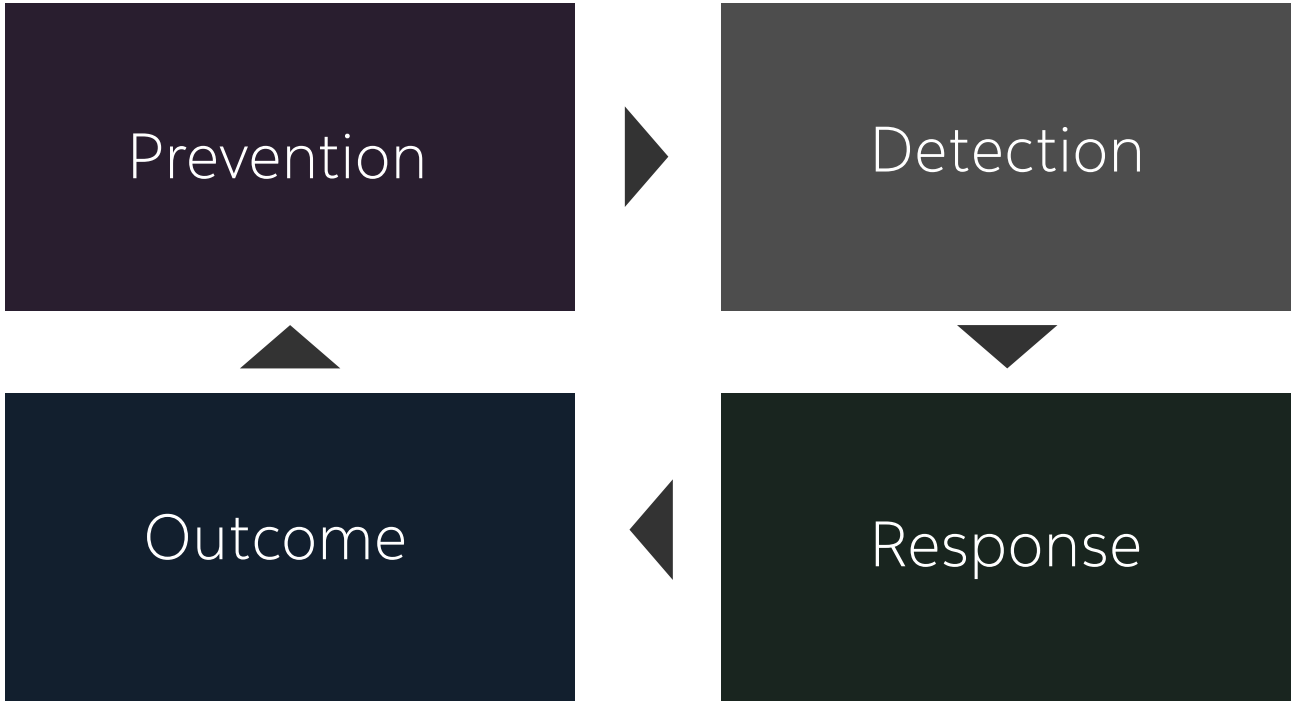
05

Best Practices

Most Important Factor in Successful Recovery of Funds

Incident Management – Fraud Lifecycle

Fraud Management ♦ Corporate Banking ♦ Corporate Security



♦ Global Transaction Banking ♦

♦ Money Transfer Operations

Enterprise Security Services ♦ Business Service Centres ♦ Legal ♦

Remember the 3 Rs

RECOGNIZE fraud by knowing the most common scams.

REJECT fraud by being aware of preventive tips.

REPORT Fraud by immediately notifying Scotiabank.

Best Practices for Fraud Prevention

EDUCATION: Be FRAUD AWARE and educate your staff.

RECONCILIATION: Review and reconcile accounts daily.

ELIMINATION OF CHEQUES (AS MUCH AS POSSIBLE) BY USING:

- Online Bill Payments & Tax Payments.
- Credit cards for small dollar vendor payments.
- Payroll.
- Pre-Authorized Debits.

SEGREGATION OF DUTIES: Ensure different people are responsible for payment issuance, execution and reconciliation.

SPECIAL ACCOUNTS: Open separate accounts to separate functions such as incoming wires and high-volume small-dollar cheques.

AUDITS AND INSURANCE: Conduct security audits and obtain Cybercrime Insurance.

Best Practices for Fraud Prevention

CYBER INSURANCE: WHAT DOES IT ENTAIL AND IS IT WORTH IT?

- Do an impact assessment to understand what a cyber breach would cost your organization.
- Get an understanding of the possible sizeable fines and additional costs associated to remediate against an attack.
- Based on this, set your organization's **risk limits** and **appetite for losses** to determine if there is a need for insurance.

IT SPEND: HOW MUCH SHOULD YOU BE SPENDING ON CYBERSECURITY?

Need to think about how important is the information you have, and what would the business impact be if it were lost. The stats and numbers vary from organization to organization and there is not set % of budget.

TOOLS TO EDUCATE EMPLOYEES AND TEST AWARENESS

KnowBe4, Cofense, and Beauceron (Canadian Company). However, the bank is not in a position to make specific recommendations.

06

What You Can Do

Protect Yourself

1. **Consider purchasing anti-virus software** for your devices.
2. Regularly **update your software** and operating systems
3. Use strong, **unique passwords**
4. Only access sensitive information when you are connected to a **trusted network**, like a home network, or mobile carrier.
5. **Think before you click!**
6. Continue to **use common sense** and nurture your inner skeptic.
7. **Pay close attention to privacy policies** of social media sites, and applications.
8. Strengthen your **Fraud Awareness**.
9. Establish a process to **immediately initiate** a recall message.

Reporting Fraud

THINK YOUR COMPANY HAS BECOME A VICTIM? HERE'S WHAT TO DO.

- **Gather** as much information as possible
- **Engage** IT team/support
- **Inform** your Bank relationship team & review bank accounts for any unusual activity
- **Report** to Canadian Anti Fraud Centre
- **Contact** the RCMP / Regional Police to report the fraud

WIRE TRANSFERS AND EFT

- Call the **ScotiaConnect Helpdesk** and initiate a recall online
- Once recalled on line, **full details need to be provided** to Relationship Manager to provide to respective stakeholders.

Key Takeaways

EVERYONE NEEDS TO BE FRAUD AWARE.

1. **Education** is key.
2. **Review internal processes** and controls.
3. **Speak to your banker** as they can provide a wealth of information.
4. Banks use **best effort**s to recover funds
5. **Prevention** is a shared responsibility between the Bank and the Customer.
6. Be aware that the **Bank will never call, text or email** and request security or personal information.

07

Additional Resources

Additional Resources

Canadian Bankers Association
https://cba.ca/protecting-your-business-from-business-email-compromise-fraud

Stay Safe From Scams
https://gtb.scotiabank.com/content/dam/gtb/documents/commonScam_QuickGuide_March2018.pdf

Get Cyber Safe
https://www.getcybersafe.gc.ca/en/home

Canadian Anti-Fraud Centre (CAFC)
http://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Scotiabank.com
https://www.scotiabank.com/ca/en/about/contact-us/security.html