



# How to Prepare for the Most Common Cyber Threats Facing SMBs

NPC Safe Computing Webinar Series

---

November 15<sup>th</sup>, 2022

---

Larry Keating, President  
Darren Mar, National Sales Manager

# Presenters



**Larry Keating**  
President

30+ years' experience with information technology, remote communications and data security.



**Darren Mar**  
National Sales Manager

More than 10 years in SMB technology products and services, with emphasis on financial services small office security.

# Thank You!



# Agenda

- Most Common Cyber Threats for SMBs
- What to Do
- Q&A





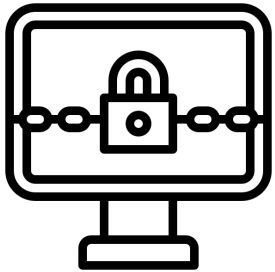
**What's the Issue?**

# Overview

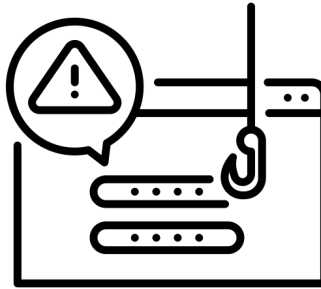
- Attacks and their impacts are increasing with little end in sight
- Smaller businesses are the target, and are more severely impacted
- Damage is increased due to a lack of investment in preventative measures and technology, and poor incident preparation

# Most Common SMB Cyberthreats

---



**Ransomware  
Attacks**



**Phishing**



**Compromised  
Accounts**

# Definitions

## **Ransomware**

Malicious software that encrypts your data until a ransom is paid to cyber criminals. Otherwise, it may be kept locked or published online.

## **Phishing Attack**

A wide range of techniques used to try and trick you to visit, click, download, or share something in an email that you should not.

## **Compromised Accounts / Credentials**

When a threat actor gains access to an account (usually by obtaining your username and password) to perform actions or transfer funds on your behalf.



# Increase in Tactics to Coerce Payment

## - Ransomware -

### **Doxing:**

- Publish stolen data if ransom to unlock not paid
  - May cause violation of contract terms, non-disclosure agreements, privacy laws, securities laws, loss of intellectual property, or intellectual property protection

### **Shaming:**

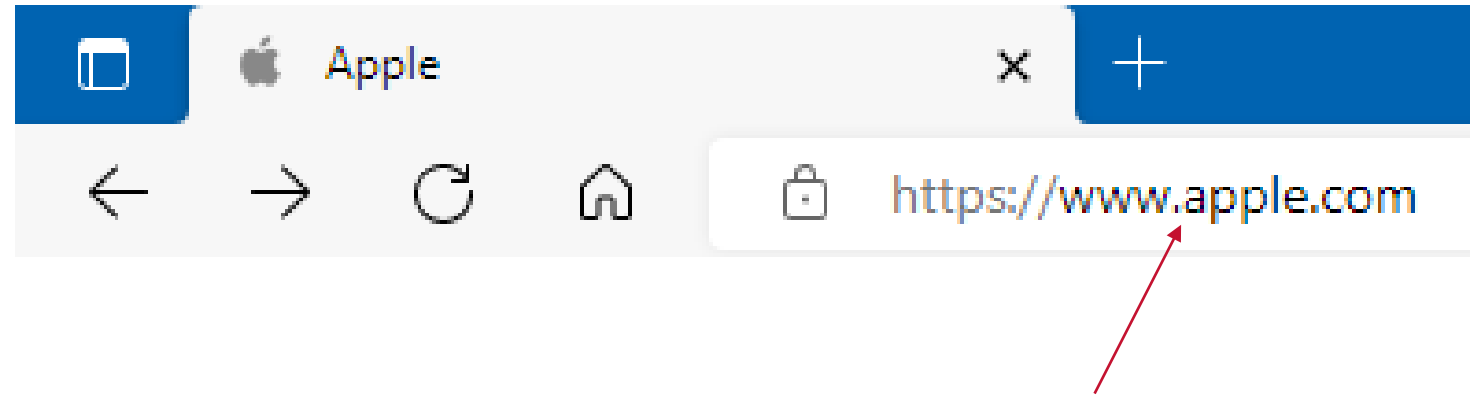
- If ransom still not paid, advise victim's clients, suppliers, partners, etc., of the breach via victim's social media and stolen email lists

### **Double-Encrypting:**

- A second layer of encryption requiring a different key, or two or more segments of data have different keys


## Increase in Tactics to Fool You

### - Look-a-like Domains -



- This “a” character replaced with a “Cyrillic” character
- Site then re-directs to the bad guys, or is used to create a spoof email that looks like the email comes from a legitimate email account

# Spoof Banking Website

**RBC Royal Bank®**

[RBCRoyalBank.com](#) | [Customer Service](#) | [Francais](#)

Aug 20, 2019

### How Can We Help?

- ▶ [Get Sign In Help](#)
- ▶ [View System Requirements](#)
- ▶ [Bookmark This Page](#)
- ▶ [Contact Us](#)
- ▶ [Sign Up For Training](#)

### RBC Express Highlights

- ▶ [Fact Sheet](#)
- ▶ [Interactive Demo](#)
- ▶ [RBC Express Mobile](#)

## Sign In to RBC Express Online Banking

**Sign In ID:**


☐ Remember my Sign In ID  
▶ [Learn More](#)

**Password:**

▶ [Forgot Password](#)

**Token Number:**  **Sign In**

▶ [Help with Token](#) (if required) ▶ [First Time Sign In?](#)




**RBC Commercial Cards Program.**  
Gain control over company expenses and insights on spending.


[Learn More >](#)

## Deposit your cheques faster with Cheque-Pro™

The new electronic cheque depositing solution

[Learn More >](#)



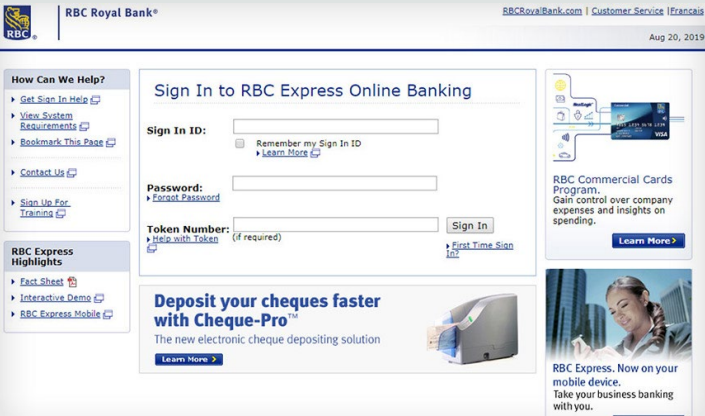
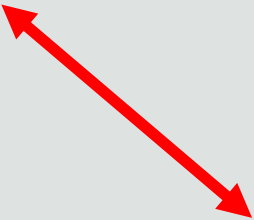
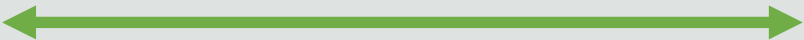


**RBC Express. Now on your mobile device.**  
Take your business banking with you.

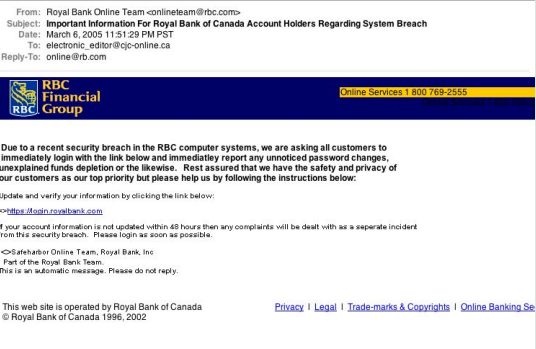
# Man-in-The-Middle Attack



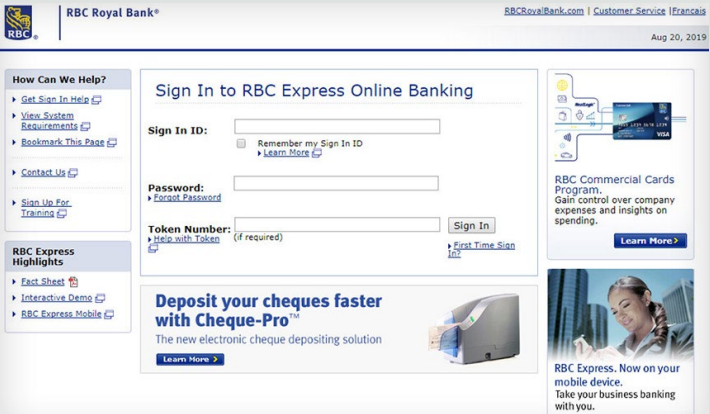
You!



Legitimate Site



Phishing Email



Fake Site

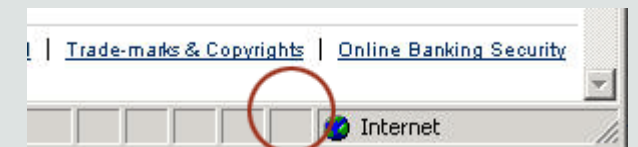
# The Bank's Advice



*Review the URL*



*Check the Security Cert of the Site*





# Compromised Email Account



## So, what is this all leading to...

- Regulators establishing minimum defense requirements, incident reporting, penalties
- Partners, suppliers, clients demanding increased vigilance
- Insurers denying coverage, increasing premiums, and rejecting claims
- Civil exposure

***Dramatically increased threat to every business***



**What to Do?**

# Minimizing Risk the Ultimate Goal

## Drivers Minimizing Risk

Cisco  
Connect



### Executive Leadership

Executive leadership must own and publicly evangelize security as a high priority.



### Policy

Regularly review security practices, and control access points to networks systems, applications, functions, and data.



### Protocols

Regularly, formally and strategically review and improve both security practices and connection activity on the network.



### Tools

Put tools in place to enable users to review and provide feedback on security, and empower them to increase security controls on high-value assets.



### Detect

To alert your organization to security weaknesses before they become full-blown incidents, implement a system for categorizing incident-related information.



### Prevent

To minimize impact of breaches, encourage employees to report failures and problems, and clearly communicate security processes and procedures.



### Mitigate

Implement and document exact procedures for incident response and tracking. Inform and educate all parties on precise, step-by-step crisis management response protocol.

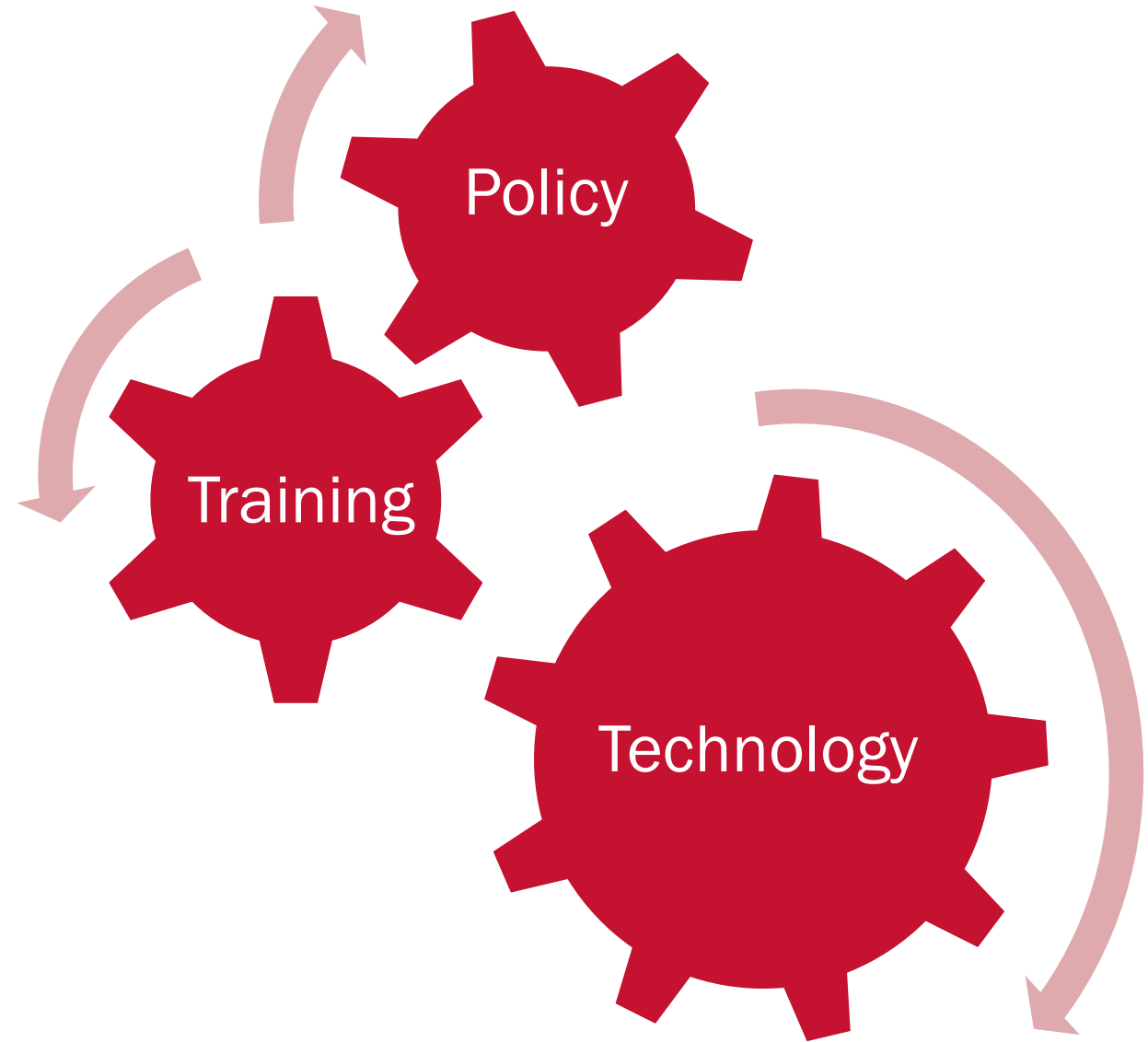


Minimized  
Risk





# The Three Pillars of Risk Governance







# Policies and Plans

# Policies and Plans: Top 5 Picks

---

## Risk Management Program



1. Incident Response Plan (IRP)
2. Business Continuity Plan (BCP)
3. Information Security Plan
4. Asset Management Plan
5. Vendor Risk Assessment

1. Privacy Policy
2. Computer, Mobile, and USB Device Policy
3. Password Policy
4. Data Encryption and Backup
5. Email Use / Social Engineering Awareness

# Plan 1: Incident Response Plan

---

## The plan I would do first if I had no other plan or policy in place:

- ☐ What are your particular risks, what type of incident would have the most impact
- ☐ Have an Incident Response Team organized and at the ready
- ☐ Ensure a lawyer, your insurance agency, and your compliance professional are part of the team, and are immediately contacted in the plan
- ☐ Map out how you will communicate within the team
- ☐ Know your regulator or professional association reporting requirements and timelines
- ☐ If you do business internationally or extra-provincially, know your responsibilities in those territories
- ☐ Map out how you will mitigate damage, quell the attack
- ☐ Ensure you are using professional technical services immediately to minimize damage, preserve evidence
- ☐ Perform a post-mortem, and extensive post-event technical testing
- ☐ Test and revisit the plan at least annually

# NPC IRP Template

Table of Contents	
Overview and Purpose of Plan.....	1
Purpose.....	1
Scope of this Plan.....	1
What is an Incident? .....	1
Incident Levels .....	2
Level 1 Incident .....	2
Level 2 Incident .....	2
Level 3 Incident .....	2
Our Priorities in the Event of an Incident.....	2
Initial Actions to Respond to an Incident.....	2
Our Incident Response Team .....	3
Preparation .....	4
Communications Plan .....	4
Location of Information .....	4
List of Assets and Systems.....	5
Incident Detection.....	6
Threat Containment.....	7
Threat Eradication.....	7
Recovery .....	7
Activities Schedules .....	8
Document Review .....	8
Document Revision .....	8
War Game Schedule.....	8
Appendices .....	9
Breach Notification Letter Sample .....	9
Internal Communication Sample .....	9
Issue These Instructions to Staff that are Not a Part of the IRT.....	9
Event Log.....	9
IRT Team Briefing Information.....	10
Critical Practices to Avoid Security Incidents .....	10
Incident Response Team Responsibilities .....	10

Strictly Company Confidential  
Do Not Copy or Distribute Outside of Company

## Overview and Purpose of Plan

### Purpose

This plan is to ensure that in case of an actual or suspected information security incident that threatens the security of the information of our clients or our company, our response is executed in an organized and effective way. It ensures the appropriate leadership and technical resources quickly assess any violation of the integrity, control, or accessibility of our systems, identify any damage to or theft of information, minimize the impact of the incident, and restore impacted operations.

### Scope of this Plan

All company and client information other than published sales and marketing material is considered company confidential, proprietary, and sensitive, and falls within the scope of the policy. This policy applies to all our systems, services, and information for which we are responsible or store or have processed by another company. It applies to any computing or communications device we own. It also applies to any other computing or communications device regardless of ownership, which is used to store confidential data for which we are responsible, that if lost, stolen or compromised, could lead to the unauthorized disclosure of our client or company confidential information.

### What is an Incident?

[Place here examples of types of breaches applicable to your business. Define what your incident severity levels are.]

An incident would be any unauthorized access, locking, deletion, transfer or modification of our systems or information, destruction of our computing or our communications equipment, the disabling or destruction of any computer network or system resource, or the theft of credentials or unauthorized access to our financial systems or accounts, or that of our clients. Examples:

- Ransomware attack
- Report of stolen funds or information from fraudulent email attack - Business Email Compromise (BEC)
- Loss of login credentials or unauthorized access to systems
- Loss of a device – laptop, desktop, smartphone, USB storage device containing confidential data or system login capabilities or credentials
- Physical break-in or insider theft of paper records
- Inadvertent transfer or transmission of client information to an incorrect client or other location

## Review your Computing and Information Security Policies and Plans

- ☐ Check to ensure you have appropriate cyber protection and information security policies and plans in place
- ☐ Check to ensure the plans you have are up to date
- ☐ Ensure staff are revisiting the plans at least bi-annually
- ☐ Keep plans and policies as simple as they can be, but meet effectiveness requirements





# Training

# Train, Train, Train

- ❑ Communicate your policies for computer use, passwords, information handling, etc.
- ❑ Teach users how to recognize suspicious communications
- ❑ Teach don't click what you don't know, open nothing that is unexpected:
  - ❑ Links or attachments in unexpected emails
  - ❑ Websites you are uncertain of
- ❑ Observe computer error and warning messages
- ❑ Observe email addresses
- ❑ Establish email source and address verification process

**Make it OK to halt the business process to check**

# Email Attack Clues

Report: Quarantine Notification - Message (HTML)

File

Message

Help

Tell me what you want to do

Ignore

Junk

Delete

Archive

Reply

Reply All

Forward

More

Meeting

Phishing Attacks

File In

QuickPick

PERM Delete

NEWS

Reply & NEWS

Create New

Move

Rules

OneNote

Actions

Mark Unread

Cate

Tag

Delete

Respond

SimplyFile

Quick Steps

Move

Tag

IS

Mon 10/8/2018 2:15 PM

IT Support <cap@gsnmed.com>

Report: Quarantine Notification

To

Dear

You have 20 new messages as of October 08, 2018, which are listed below along with the actions that can be taken:

Release to I

https://u8455767.ct.sendgrid.net/wf/click?upn=tk980v06-2bdsaptv1tjios4rzeum3tkga30sivmta  
hszy-2b48aokig2afytthscpo\_pzd9s6qiqomsizuev2fug  
m6wd8hdzqmk4bgr-2fjwid7h1ih8wc2quc1ppjq-2fm  
yujv-2fefnncjqrhzpm70eodqfz2xu-2boil62kjl9tqoovj  
ivn9n2tmcbcpiy-2fs1bdwuihsmwbdaxmc-2fut1o2zv  
5zdexsrmw2lsiyysae1gehjvlsczy3x7betdhhbtehndchdfl  
qwauhkuztrfbieprhxbi8kp-2bj-2bct9hltxkfh5o-3d

Quarantine

Click or tap to follow link.

and change your quarantine settings.

© 2018 Microsoft Corporation. All rights reserved. | Acceptable Use Policy | Privacy Notice

Suspect Email Address

Inserted Salutation

Typographical Errors

Suspect URL Destination

No Links

# Spoof Email

## Notification



BMO Harris <info@greenpia-yame.com>

To

↩ Reply

↩ Reply All

→ Forward



Wed 2022-01-19 5:34 PM

[EXTERNAL - Use caution when opening attachments or links.]

**BMO**  **Bank of Montreal**

Dear Customer,

Your password has been disabled due to multiple use of incorrect login details. For your security, we have disabled your Online banking.

To restore your account and continue the use of online banking and stop further disabling of your bank account.

[Click here to restore and protect your accounts online.](#)

If you have any questions, we are available 24 hours a day, 7 days a week ,

Please do not reply to this email.

Sincerely,

You will find a confirmation of this message in your Messages & Alerts inbox.

Bank of Montreal Online Customer Service

# Train for Identity Protection

- According to CrowdStrike, 80% of all breaches use compromised identities
- For small business professionals, personal and business identities are closely intertwined
- Many small business professionals are owner, officer, director and key executive, with personal guarantees, or even personal accounts, to run the business



# Multi-Factor Authentication

## Definition:

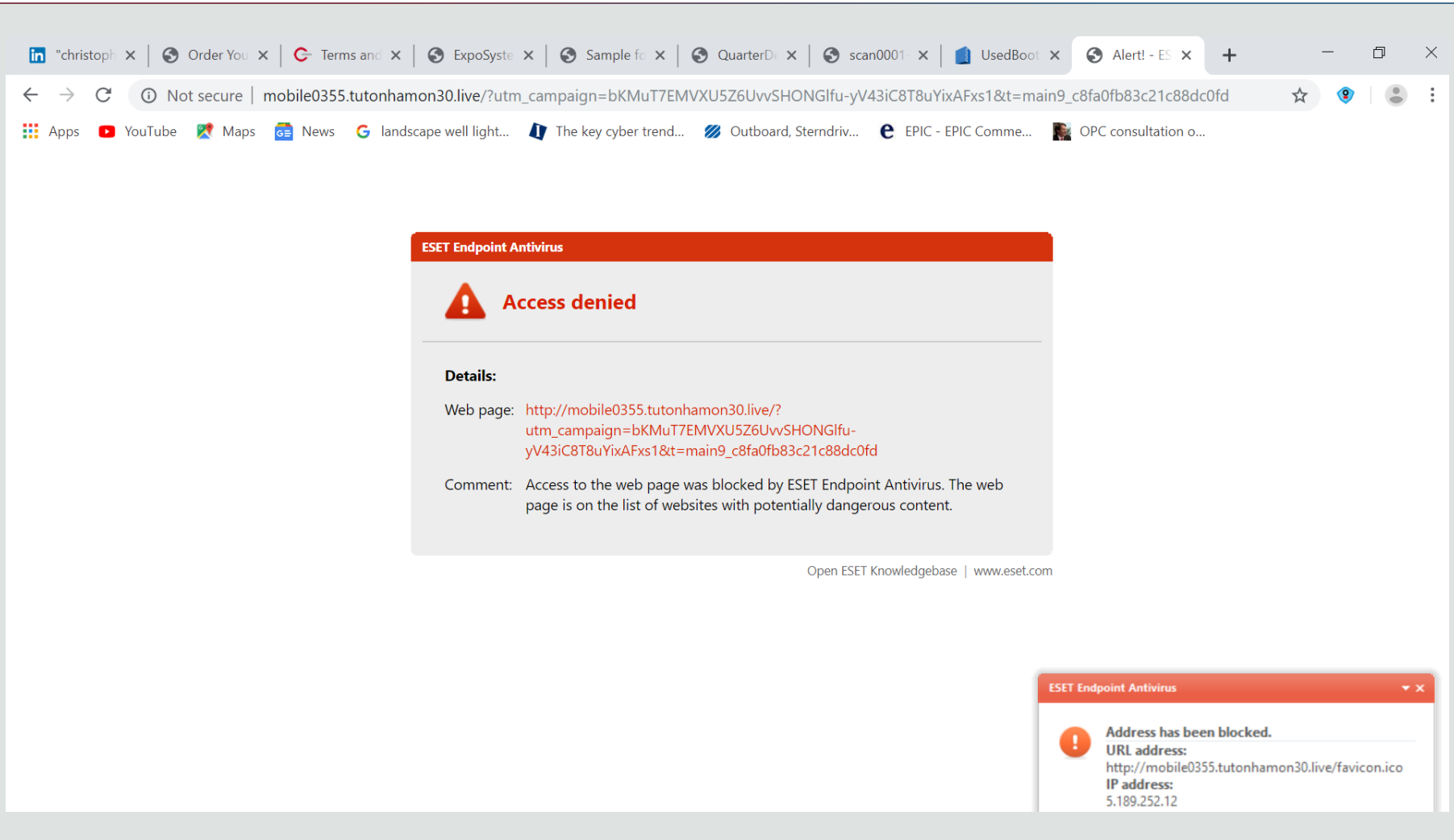
A method of allowing access to applications, websites, systems or devices, only after the user presents two or more pieces of authentication evidence.





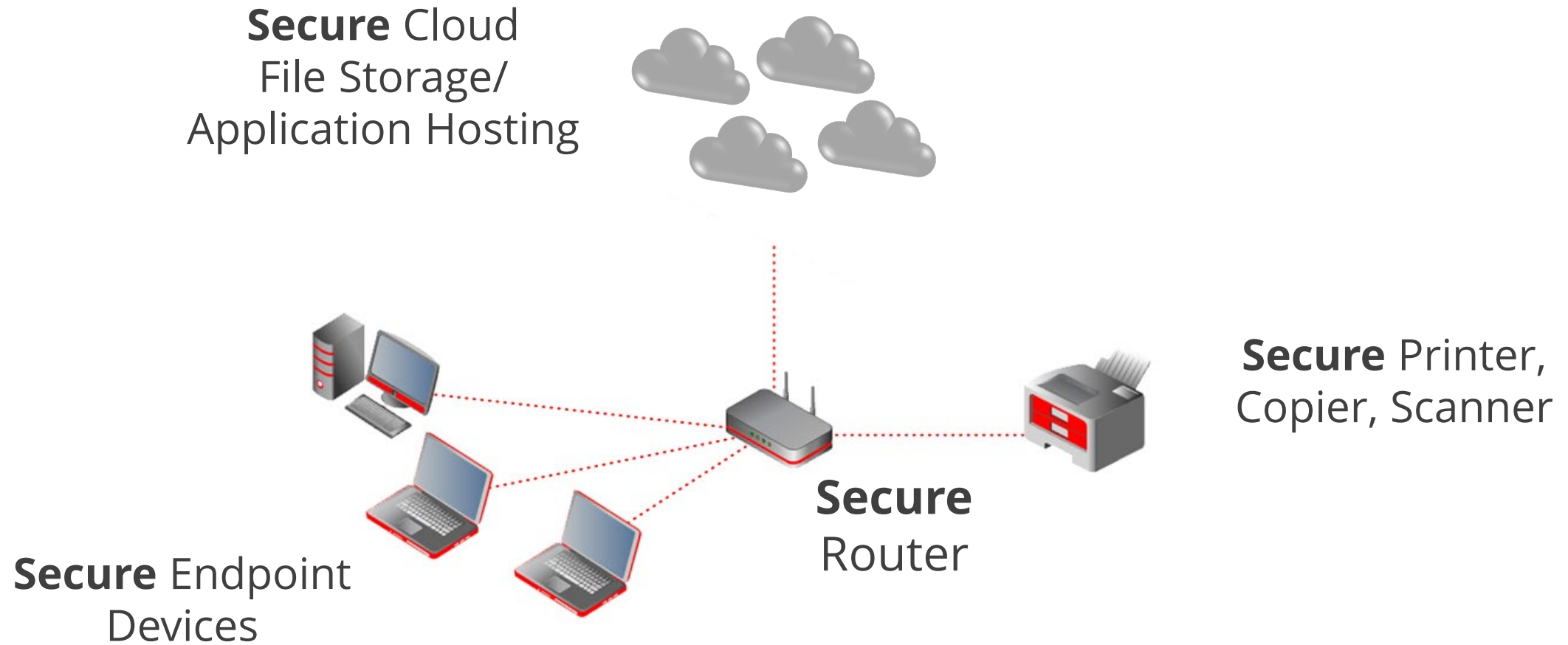
Technology

# Drive-by Attack Blocked

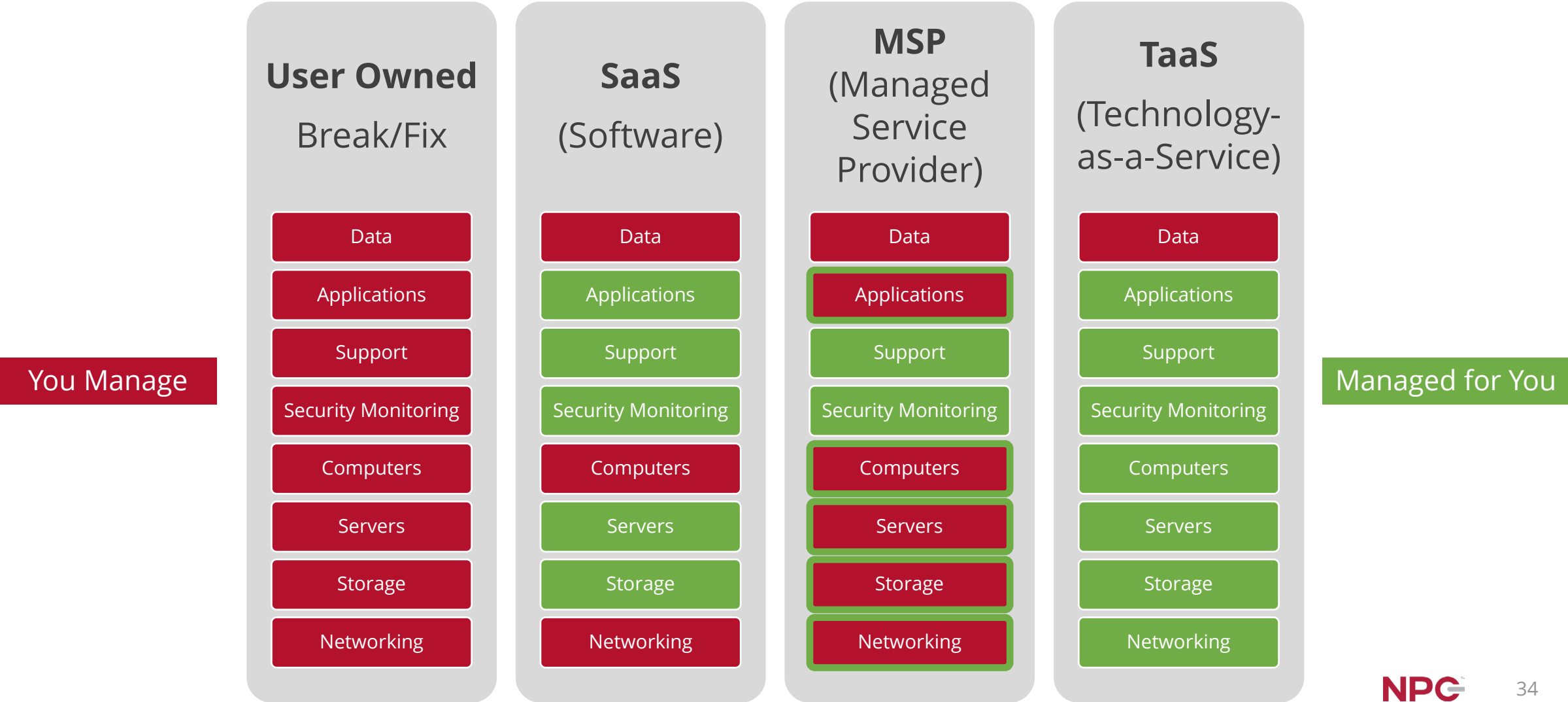


# Office of the Future

---



# Improve How You Acquire and Maintain Technology





# As-a-Service Business Impact

---



Frees up:

- Time
- Resources
- Capital



Improves operational performance:

- User experience
- Minimizes down time
- More technology capability for less cost



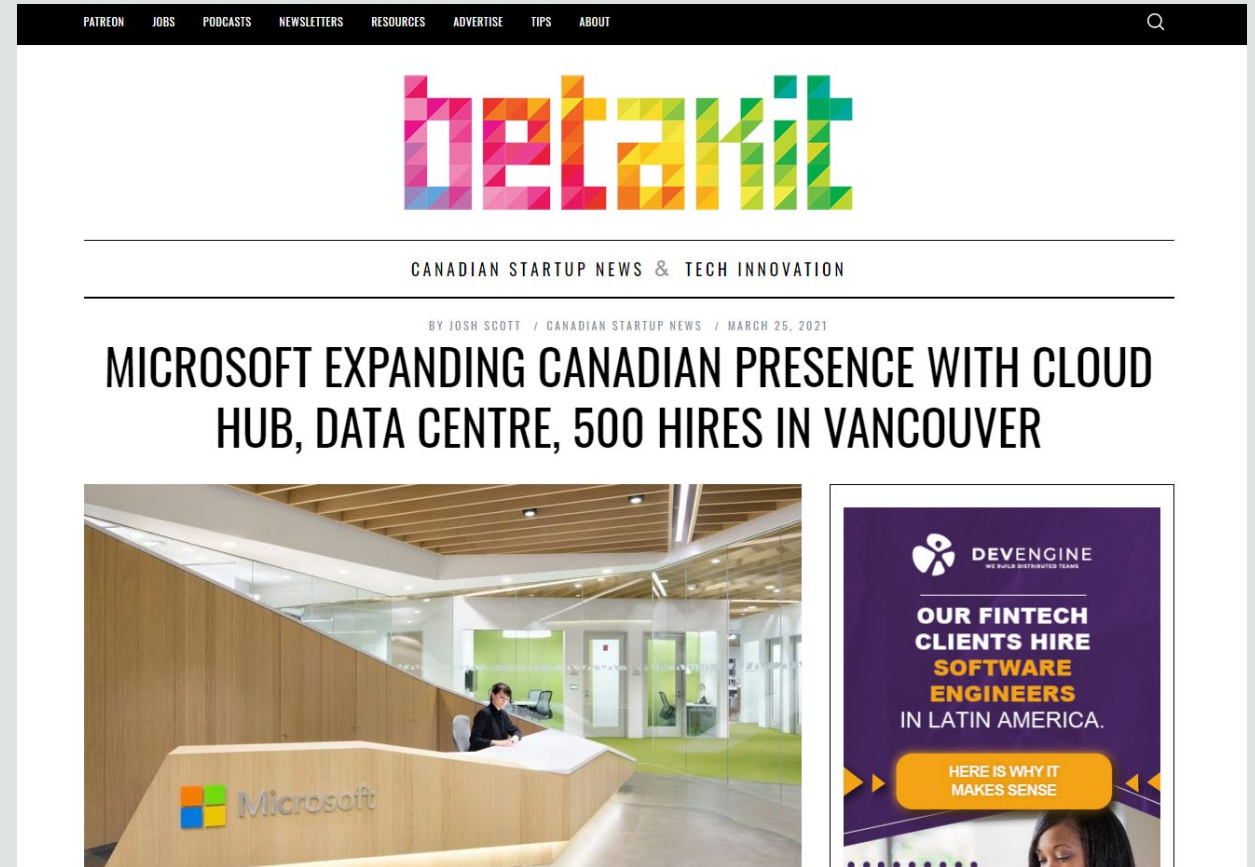
Increases revenue:

- New services
- Performance improvement of core offering

**It is difficult to compete with the security, speed, reliability and economics of specialization**

# Microsoft Security...

- Microsoft employs nearly 4,000 professionals in Canada, more than 100,000 in the U.S.
- Data centres adhere to ISO 27001, ISO 27018, SSAE 16 SOC1 Type II audit and controls standards
- The data centres are built from the ground up for external and internal security
- Massive internal analysis systems employing AI and using advanced signals intelligence protect your data
- Advanced content control and multi-engine malware scanning



# Advanced Threat Protection

FW: Invoice "RNP583879248D11"



Accounts <dispatch3ps-vendor@serviceglobal.com> (Accounts via duc.edu.gh)

To Larry Keating (NPC)

Cc Larry Keating (NPC)

The actual sender of this message is different than the normal sender. Click here to learn more.



Unsafe Attachments Blocked  
Outlook item

Reply

Reply All

Forward



Sun 2022-04-03 9:32 PM

[EXTERNAL - Use caution when opening attachments or links.]

Please find your Invoice attached.

## DISCLAIMER

This email contains proprietary confidential information some or all of which may be legally privileged and/or subject to the provisions of privacy legislation. It is intended solely for the addressee.

If you are not the intended recipient, an addressing or transmission error has misdirected this e-mail; you must not use, disclose, copy, print or disseminate the information contained within this e-mail.

Please notify the author immediately by replying to this email. Any views expressed in this email are those of the individual sender.

This email has been scanned for all viruses and all reasonable precautions have been taken to ensure that no viruses are present.

we cannot accept responsibility for any loss or damage arising from the use of this email or attachments.

## Review your use and adoption of “as-a-service” and cloud computing technologies

- ❑ Check to ensure you have identified any use of online services in your company, and they are within policy and regulatory standards
- ❑ Review the security level, policies and contract terms of any third-party provider
- ❑ Identify opportunities to replace traditional “break/fix” technology supply models
- ❑ Review business processes, methods and tools frequently with your team to identify simplification advantages, given new technology developments and as-a-service capabilities

# Recap

**Attacks are becoming increasingly complex, effective, and costly.**

- Develop a plan to improve your protection strategy
- Consider the Three Pillars of Risk Governance:
  - Policy, Training, Technology
- Embrace a small footprint, secure-cloud strategy
- Secure your systems and endpoint devices
- Use Technology-as-a-Service to lower cost, improve performance and increase security

**Brand and financial damage from an attack  
can be considerable, even for a one-person operation**

**Prepare now**



## Bonus Steps

- ☐ Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- ☐ Conduct a risk assessment of your hybrid environment, preferably using a security professional
- ☐ Acquire a specific cyber package, in addition to your E&O or general liability package, that takes into account your new operating model



## Additional Resources

# NPC Solutions

---

**Secure managed computers and Microsoft 365 for the professional and SMB office**



- NPC Secure Managed Computers
  - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
  - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Cyber Assessments and Pen Testing
- Dedicated Account Manager
  - A custom and consultative approach

# Upcoming NPC Webinars



[npcdataguard.com/webinars](https://npcdataguard.com/webinars)

---

**November 17<sup>th</sup>**  
1:00 PM ET (30 mins)

NPC DataGuard Solutions Overview

---

**December 13<sup>th</sup>**  
1:00 PM ET (60 mins)

Protecting Your Identity Online  
(and Why It's Important to Your Business)

---

**December 15<sup>th</sup>**  
1:00 PM ET (30 mins)

NPC DataGuard Solutions Overview

---

# NPC Webinars Recordings



[npcdataguard.com/webinars](https://npcdataguard.com/webinars)

[Enhancing Password Security and the Power of MFA](#)

---

[Building an Incident Response Plan for the SMB](#)

---

[Implementing and Managing the Secure Hybrid Workplace](#)

---

[10 Steps to Secure Your Business from Ransomware](#)

---

& more, and new topics will be added



# NPC Security Alerts

 [npcdataguard.com/alerts](https://npcdataguard.com/alerts)

## What the Log4j Vulnerability Means for SMB Professionals



NPC Security Alerts



2021-12-21

[EXTERNAL - Use caution when opening attachments or links.]

[Préférez-vous voir ce courriel en Français?](#)

**NPC**™ Security Alerts



### What the Log4j Vulnerability Means for SMB Professionals

A major security flaw in an application used by programmers to record activities for applications and software in devices and various services is making the headlines. National cybersecurity agencies and experts are calling for urgent action after it was reported last week.

Log4j is a component of software that developers use to record activities in an application. It is used in millions of Java applications and when located by hackers it can be exploited with relative ease. Hence, it has received a very high threat rating.

# Q&A

**Darren Mar**

[dmar@npcdataguard.com](mailto:dmar@npcdataguard.com)

905-305-6513

---

**Larry Keating**

[lkeating@npcdataguard.com](mailto:lkeating@npcdataguard.com)

905-305-6501



*Thank You*

Please Be Safe & Stay Healthy



**NPC**<sup>TM</sup>  
Smarter Computing