



Rising Above the Cyber Threat Landscape

March 14, 2023

Larry J. Keating, President
NPC DataGuard

Darren Mar
National Sales Manager

Thank You!



Agenda

- The Cyber Threat Landscape
-

- What to Do
-

- Q&A
-



The New Cyber Threats



Photo Credit: Government of North Korea



INTERPOL



Source: NBC Studios – YouTube - June 7, 2022

21st Century Cyber Threat Tools

- Deep Fake Audio has already been used against SMBs in Canada and the U.S. to commit cyber crime
- ChatGPT and similar AI platforms can:
 - Create high-quality content to enhance the effectiveness of phishing attacks
 - Assist with research on a person or organization to improve the accuracy and efficacy of phishing attacks
 - AI augmented malware development — including polymorphic malware that mutates to avoid detection
 - Design and automate sophisticated attack workflows
- Microsoft RTF text docs self-executing malware

Familiar Business Look

From: Microsoft OneDrive [\[redacted\]](#)
Sent: August 3, 2020 2:28 AM
To: Larry Keating [\[redacted\]](#)
Subject: File:- "Financial Statements - 08.2020.xlsx" Has Been Shared With [\[redacted\]](#)
Importance: High



Attached Is the Financial Statements - 08.2020



Financial Statements - 08.2020.xlsx



This link will work for [\[redacted\]](#)

[View](#)



[Privacy Statement](#)

Familiar Business Look

IMPORTANT: System Notification Error230192



02476Jill673745Jill02476Jill673745Holmes[02476Jill673745Jill02476Jill673745Holmes/02476Jill673745Jill02476Jill673745Holmes <jill.holmes@standrewshouse.org.uk>

To 02476Jill673745Jill02476Jill673745Holmes[02476Jill673745Jill02476Jill673745Holmes/02476Jill673745Jill02476Jill673745Holmes

 This message was sent with High importance.

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



SYSTEM NOTIFICATION

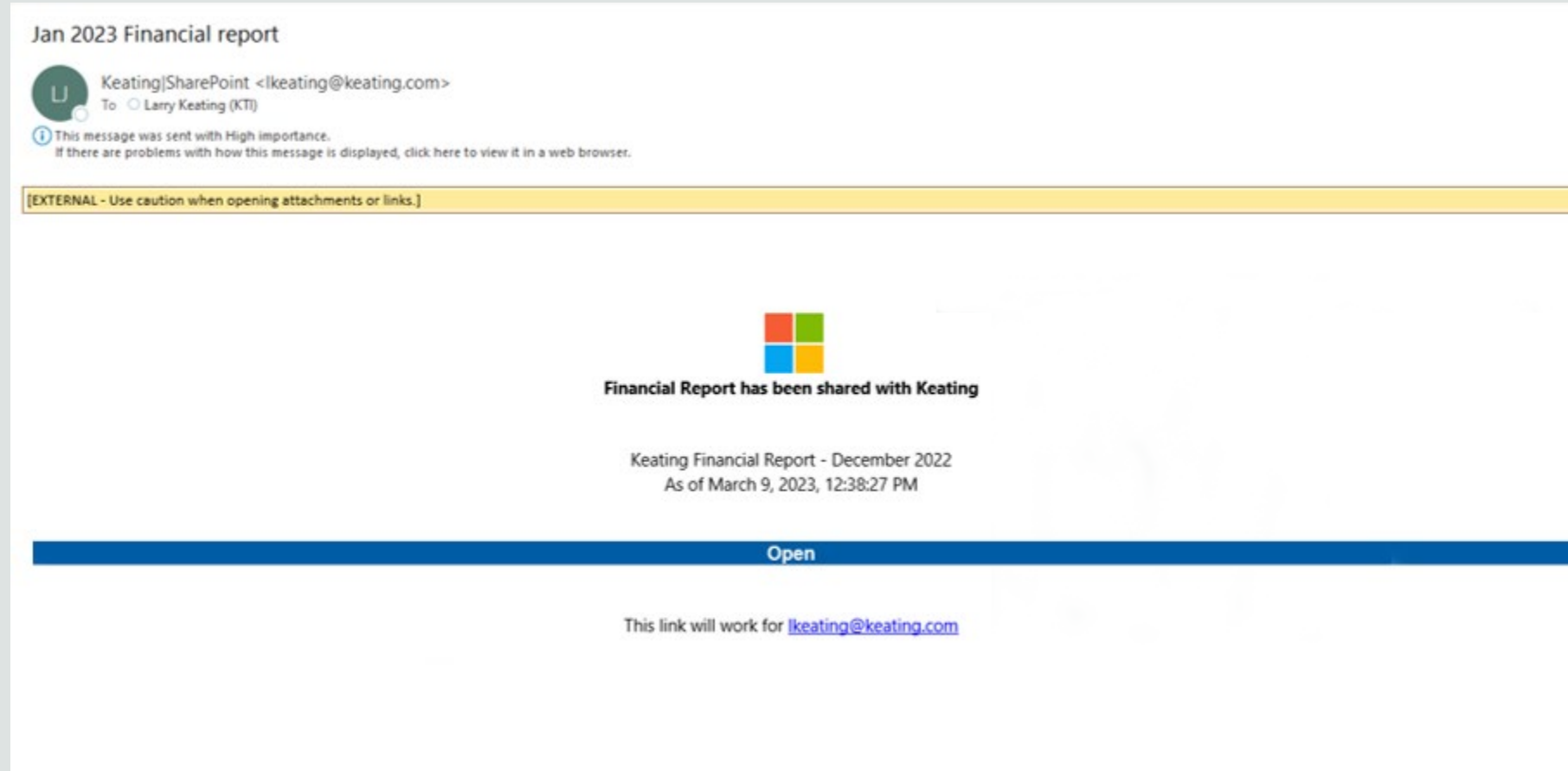
Your **17 unreceived email** are stuck on your mailbox server.

The unreceived emails will be deleted from your email account server within 24Hrs from **03/07/2023**.


This was due to a system rectify error.

[Receive Delayed Messages](#)

Familiar Business Look



Spoof Banking Website



RBC Royal Bank®

RBCRoyalBank.com | Customer Service | Français

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 >](#)



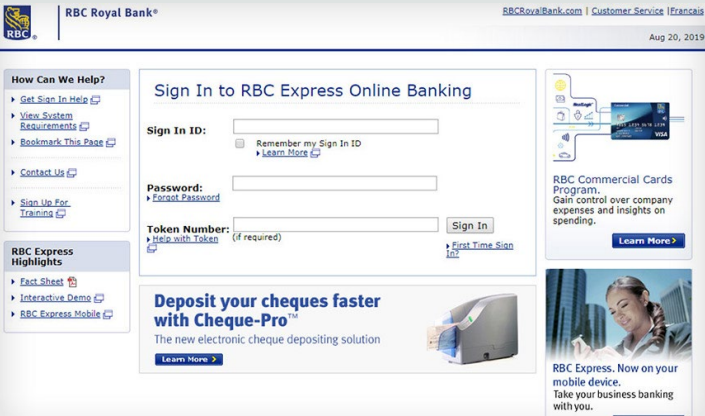
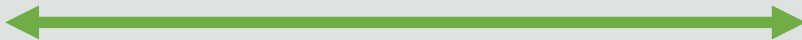


RBC Express. Now on your mobile device.
Take your business banking with you.

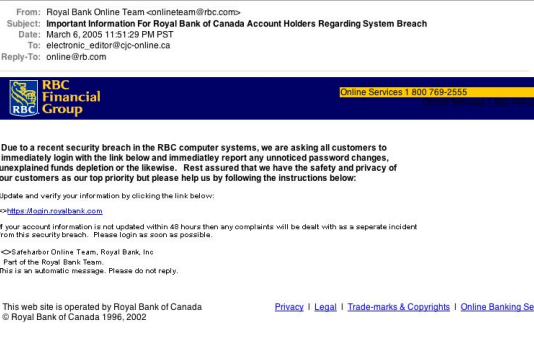
Man-in-The-Middle Attack



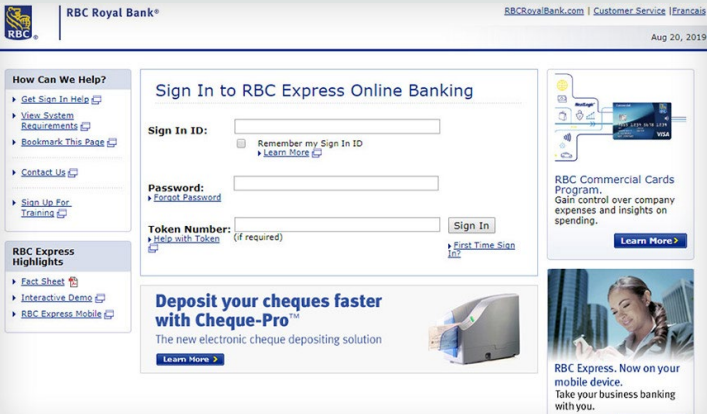
You!



Legitimate Site



Phishing Email



Fake Site

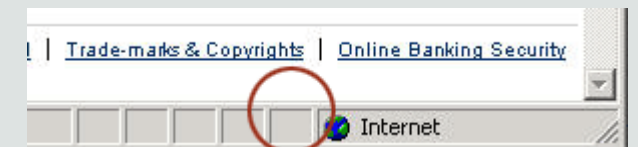
The Bank's Advice



Review the URL



Check the Security Cert of the Site



Really Familiar Business Look



Really Familiar Business Look



Supply Chain Attack



← Infected!

Attack Methods

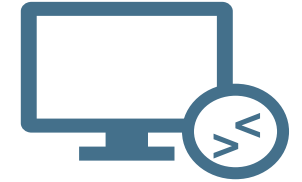
Threats are up

300%

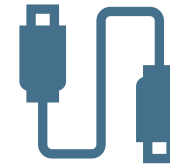
since the pandemic started



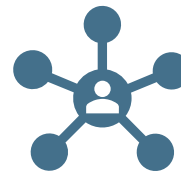
Email and web
browsing



Remote desktop



Improperly Protected Networks



IoT devices



Supply Chain Attacks

Small business is the target...



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

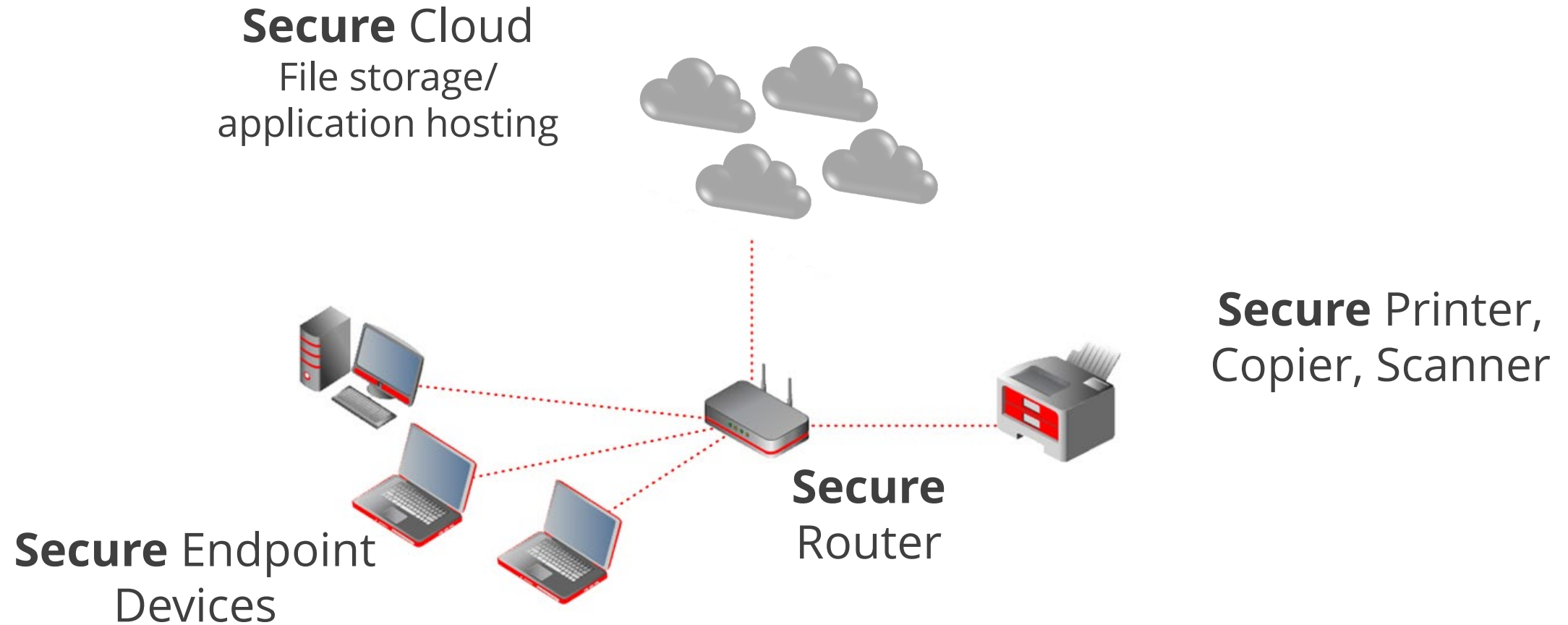
Dramatically increased threat to every business



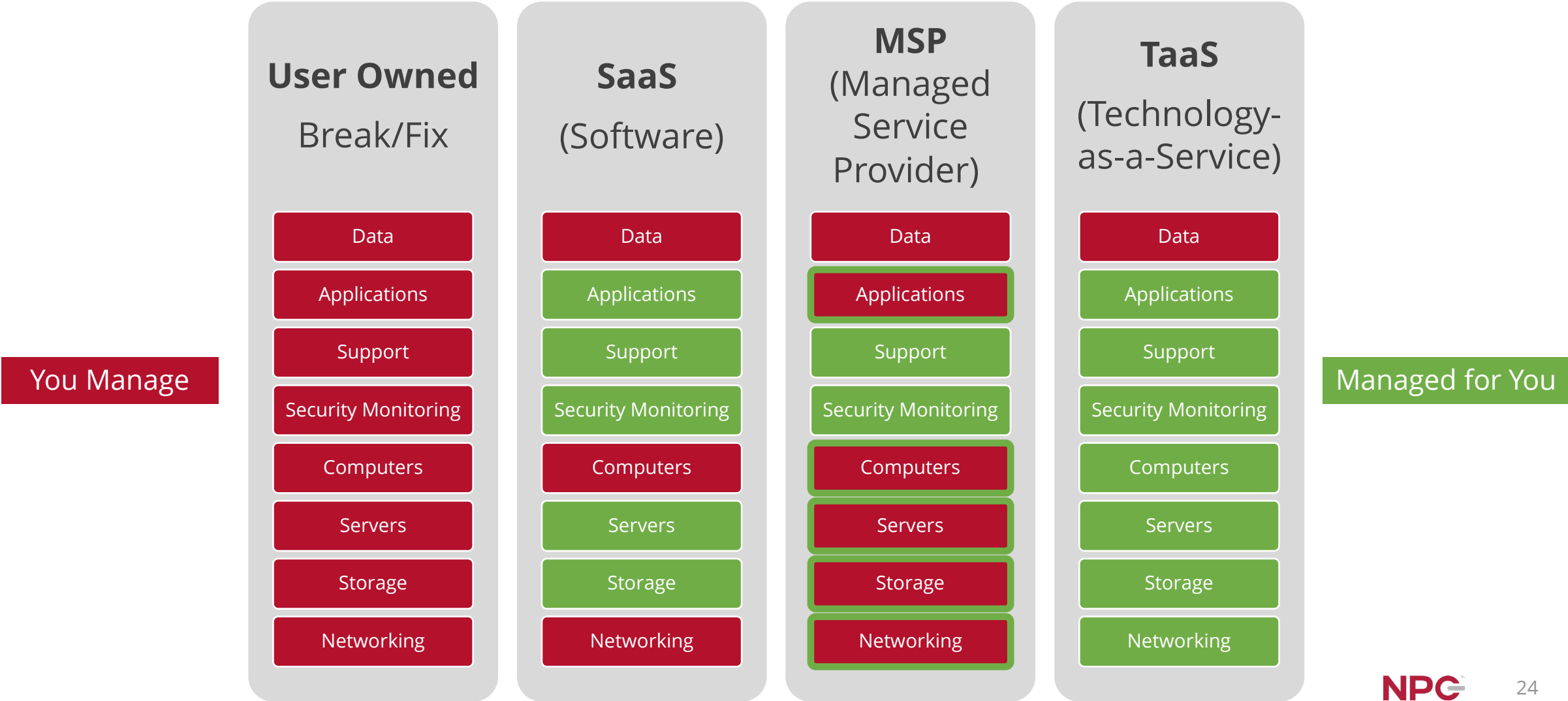
What to do...

[Checklists](#)

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

Protect Your Company

- ☐ Enable Multi-Factor or Two-Factor Authentication
- ☐ Conduct a risk assessment, preferably using a security professional
- ☐ Acquire a specific cyber package, in addition to your E&O or general liability package



Save this **checklist** for later.

Have an Incident Response Plan (IRP)

Plan 1: 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

Recap

Attacks are becoming increasingly complex, effective, and costly.

- Smaller businesses are the target, more severely impacted
- Develop a plan to improve your protection strategy
- Use as-a-service technologies to lower costs, improve performance and security

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

Prepare now!



Additional Resources

NPC Webinars Recordings



npcdataguard.com/webinars

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

[How to Protect Your Business from Email Compromise Attacks](#)

[Protecting Your Identity Online](#)

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

+ New topics added regularly!

Upcoming NPC Webinar



npcdataguard.com/webinars



Thursday, March 16th
1:00 PM

[Register now!](https://npcdataguard.com/webinars)

Agenda:

- Small Business Computing Today
- NPC Solutions
 - NPC DataGuard Pro
 - Managed Microsoft 365
- Q&A

NPC Security Alerts



npcdataguard.com/alerts

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

NPC™ Security Alerts



Update: LastPass Reveals Personal Info and Encrypted Passwords Stolen in Recent Breach

[Click here to read the full alert](#)

Note: This NPC Security Alert updates our [alert issued December 12, 2022](#), regarding the LastPass Breach of August 2022.

What is the Issue?

On November 30, LastPass issued a notice that they had suffered a second data breach, following a breach in August. In November they knew that information gathered during the August breach enabled the threat actors to gain access to their systems, but it was unclear exactly what information had been used or what customer data had been compromised.

In an update published on December 22, 2022, LastPass advised they learned from their ongoing investigation that two types of data have been taken: unencrypted basic customer information like company names, end-user names, billing addresses; and encrypted customer “vault data” — client login and password stores.

This presents two problems for LastPass users. First, the unencrypted basic customer information can be employed to help the threat actors break the vaults and to better

Q&A

Larry Keating

lkeating@npcdataguard.com

905-305-6501

Darren Mar

dmар@npcdataguard.com

905-305-6513



Thank You
Be Safe & Stay Healthy



NPCTM
Smarter Computing

1. Secure your Computers

- ❑ Use a business-class computer, and update the BIOS, OS and security tools
- ❑ Check the default settings in the OS and applications
- ❑ Change default passwords, and don't use the admin password as a user
- ❑ Create strong, unique passwords or passphrases, and employ biometrics to make those long passwords easy to work with
- ❑ Install business-class anti-malware software
- ❑ Choose applications and tools that prioritize security
- ❑ Enable encryption
- ❑ Ensure the device firewall is enabled
- ❑ Only do work on your secured computer

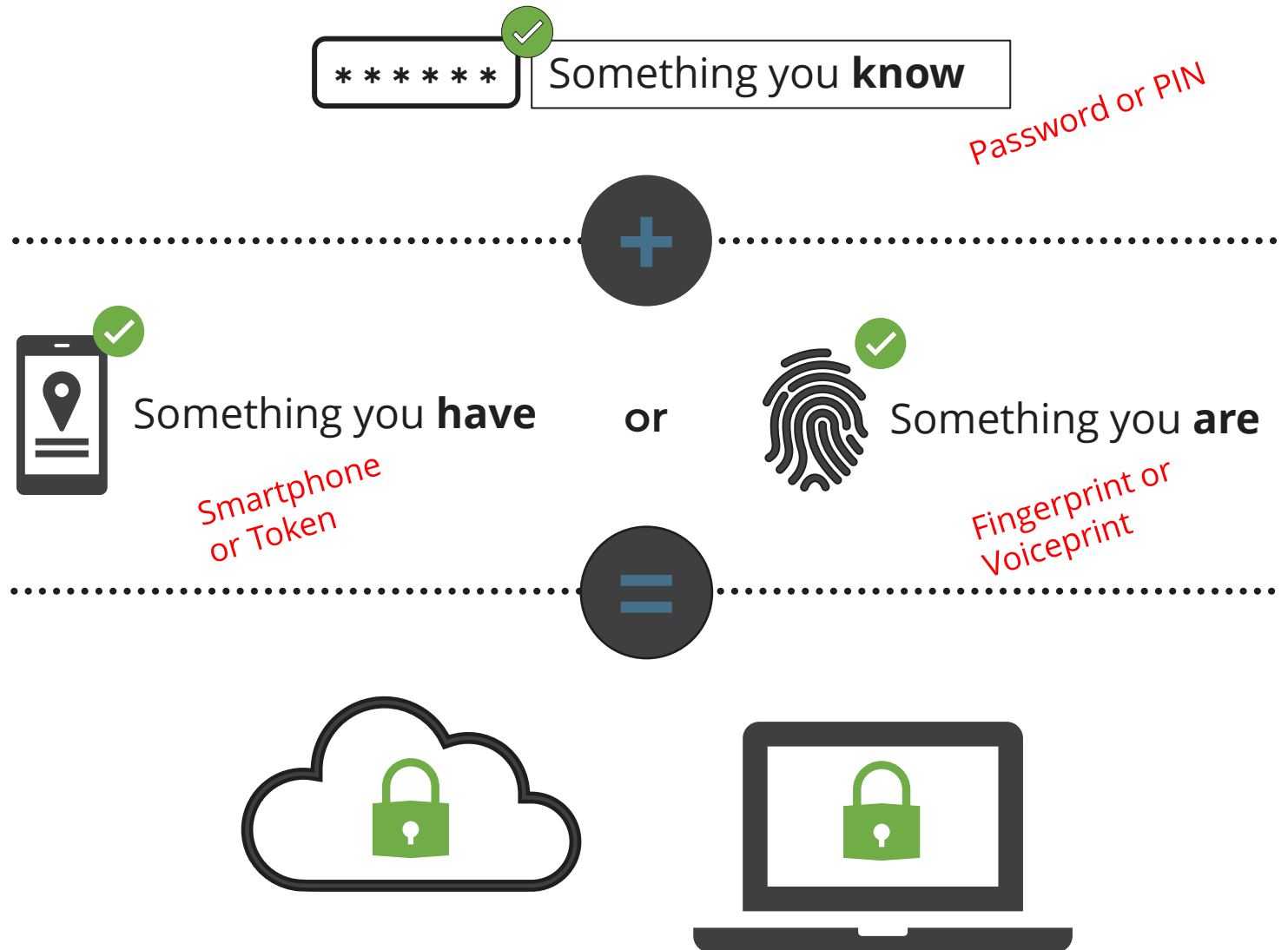
2. Patch, Patch, Patch

- ❑ Everything in computing is fluid. Your computer's BIOS, OS, Office Suite and applications are all constantly being updated and secured:
 - ❑ Enable automatic patching wherever possible
 - ❑ Stop work for 20 minutes to install patches and updates, and reboot. Sorry!
 - ❑ Put an event in your calendar to routinely check that all of your devices, systems and applications are up-to-date

3. Enable 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.



4. Change Your Passwords

- ❑ Set a schedule and take the time to change your passwords
 - ❑ A benchmark is every 90 days, but adjust that based on the importance of the system you are protecting and the level of security offered
 - ❑ Consider how many retry attempts the system allows before lockout
- ❑ Never re-use passwords
- ❑ Use a device-based password management tool on a secure computer
- ❑ Use a fingerprint reader to make longer passwords more convenient to use

5. Back Up Your Files Regularly

The ultimate failsafe against loss, theft, fire, mechanical failure, human error, viruses, Trojans, malware, etc.

- ❑ Sometimes necessary for regulatory compliance
- ❑ Make sure your backup will restore
- ❑ Ensure you have a backup multiple versions deep, and it connects to your computers only when backing up
- ❑ Do not keep your backup in the same place as the computer(s) you are backing up –
 - ❑ Use an online, remote backup service
 - ❑ Distinguish between file sharing and primary storage vs. backup
 - ❑ Ensure your back centre is secure, and the data is encrypted

6. Secure your Remote Access Connections

- Have a professional review your Remote Desktop Protocol (RDP) connection to the office server
- Carefully choose any remote access tool
- Use a Virtual Private Network (VPN) service or technology

Work to eliminate these forms of remote access through a cloud-based “Office of the Future”

7. Train, Train, Train

- ☐ Have clear policies in place for computer use, passwords, information handling, etc.
- ☐ Teach users how to recognize suspicious communications
- ☐ 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 error and warning messages from your computer
- ☐ Observe email addresses
- ☐ Establish email source and address verification process

Make it OK to halt the business process to check

[Back](#)

Ransomware Attack Email Cleaned

Search All Mail Items

All Mailboxes

All Unread

By Date

Netflix

Important : We were unable to renew your membership

2019-12-06

Larry Keating

RE: Package pick up notification!

2019-12-04

Dominic L Petrone

Microsoft Mail Delivery Failure

2019-12-03

Stewart Hazell

RE: Quick Respond!

2019-11-19

service@paypal.com

you've added an address to your PayPal account.

2019

Larry Keating

RE: Phishing Email from You

2019

Albert Han

FW: Quick Respond!

2019

Sarah, (via LinkedIn)

Sarah, made an important post lkeating@keating.com

2019

Microsoft Mail Delivery Failure

DL

Dominic L

To Larry Keating

2019-12-03

<body>

Hello

Your server has delayed the delivery of 5 messages.

On Monday, December 02, 2019 at 2:26:41 AM

REVIEW

eset ENDPOINT SECURITY

Threat removed

A threat (HTML/Phishing.Agent.LO) was found in a file that Microsoft Outlook tried to access.

The file has been cleaned.

Learn more about this message

All folders are up to date.

Connected to: Microsoft Exchange

Display Settings

100%

Ransomware Drive-by Attack Stopped

