10 Steps to Secure Your Business from Ransomware

NPC Safe Computing Webinar Series

July 19th, 2022

Larry Keating, President

NPC DataGuard™

Presenter

Larry Keating
President

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

Thank You!

ALIGNED capital partners inc.

MFDA Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

PPI Solutions

Manulife Securities

Advocis The Financial Advisors Association of Canada

MANDEVILLE™
PRIVATE CLIENT INC.

FaithLife® FINANCIAL

AON

Investment Planning Counsel®
IPC VALEURS MOBILIÈRES

HUB

IIAC ACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

IDC WORLDSOURCE
INSURANCE NETWORK INC.

Advisor Research Group Inc.

CI FINANCIAL

EQUITY Associates Inc.

FINANCIAL LITERACY
COUNSEL INC.

GLOBAL
MAXFIN INVESTMENTS INC.

GROVE POINT
FINANCIAL

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

Agenda

- Ransomware Threats
- 10 Steps to Secure Your Business
- Q&A

What’s the Issue?

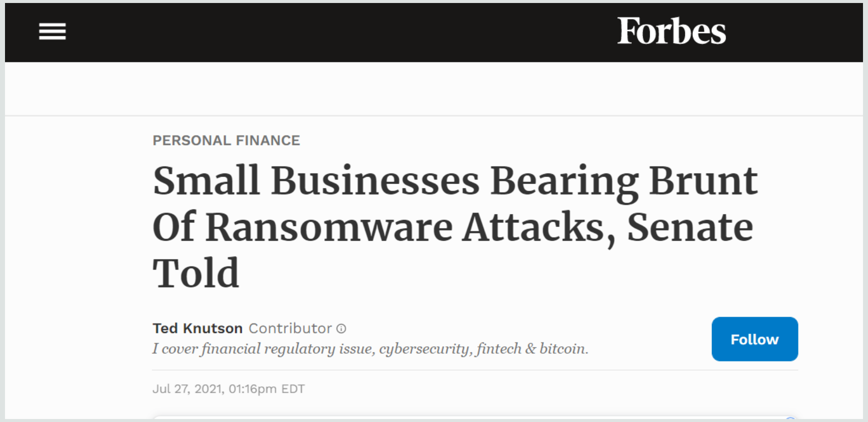
Ransomware is now the leading form of cyberattack causing massive business disruption and losses

Attacks are increasing in effectiveness

Higher costs and business impacts

All business sizes are a target

Bad News for SMB Abounds…



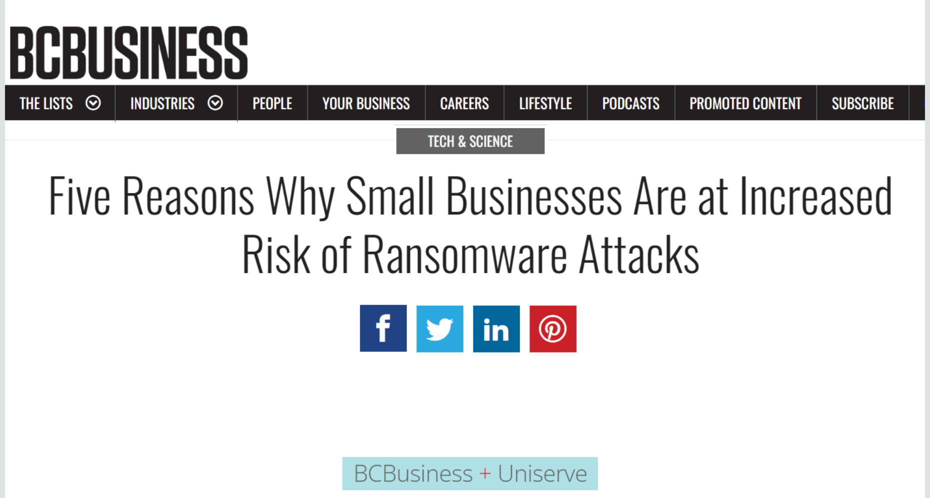
PERSONAL FINANCE

Small Businesses Bearing Brunt Of Ransomware Attacks, Senate Told

Ted Knutson Contributor

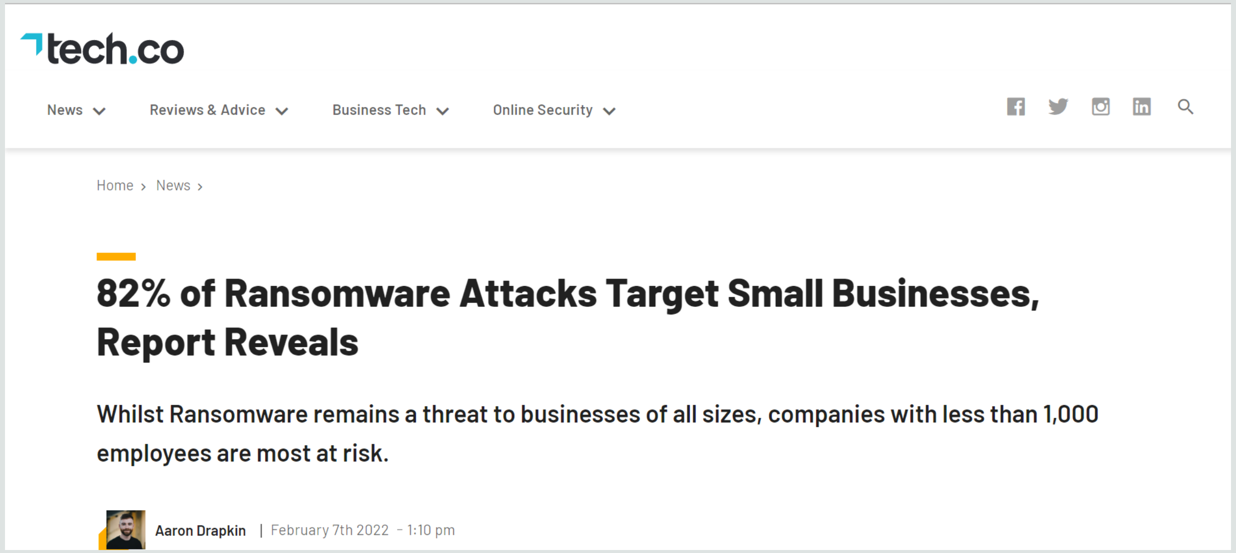
I cover financial regulatory issue, cybersecurity, fintech & bitcoin.

Jul 27, 2021, 01:16pm EDT



Five Reasons Why Small Businesses Are at Increased Risk of Ransomware Attacks

BCBusiness + Uniserve



82% of Ransomware Attacks Target Small Businesses, Report Reveals

Whilst Ransomware remains a threat to businesses of all sizes, companies with less than 1,000 employees are most at risk.

Aaron Drapkin | February 7th 2022 - 1:10 pm

Sources: Forbes Magazine July 27,2021, Tech.co, February 7, 2022, BC Business, July 2022

Survey of 357 Organizations that Paid the Ransom…

Half of respondents (46%) indicated they regained access to their data following payment, but either some or all of the data was corrupted

- On average, ransom-payers got back just 65% of the encrypted data
- 29% got half of the data back
- Just 8% got all their data back undamaged, as a result of paying the ransom

Source: SOPHOS – The State of Ransomware - Survey of 5,400 IT decision-makers from 30 countries.

Attack Methods

Threats are up

300%

since the pandemic started

Source: FBI IC3 (Internet Crime Complaint Centre)

Email and web browsing

Remote desktop

Improperly Protected Networks

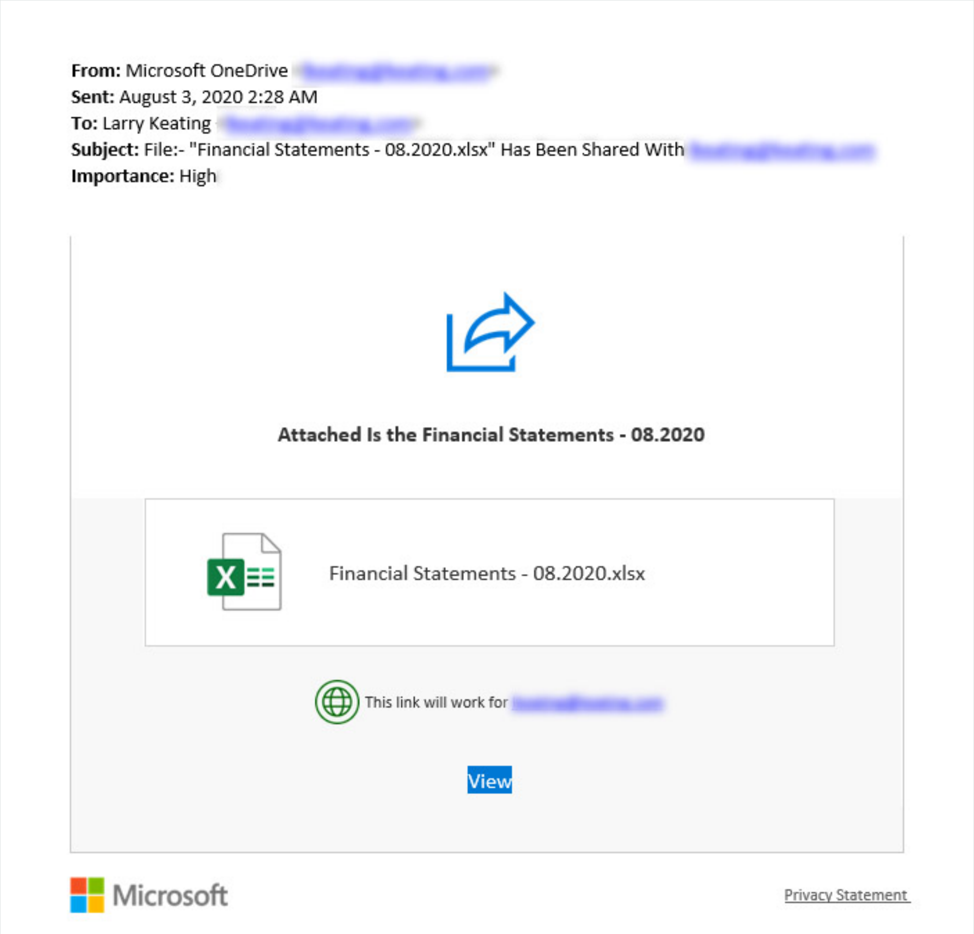
IoT devices

Supply Chain Attacks

Source: Data Breach Today, May 27, 2022.
Photo Credit: Palo Alto Unit 42

INTERPOL

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]

Source: NPC Files

Summary

- Attacks and their impacts are increasing with little end in sight
- Paying a ransom is a bad idea, and ultimately self-defeating. May bring legal risk, certainly an ethical issue
- Damage is increased due to a lack of investment in preventative measures and technology, and poor incident preparation

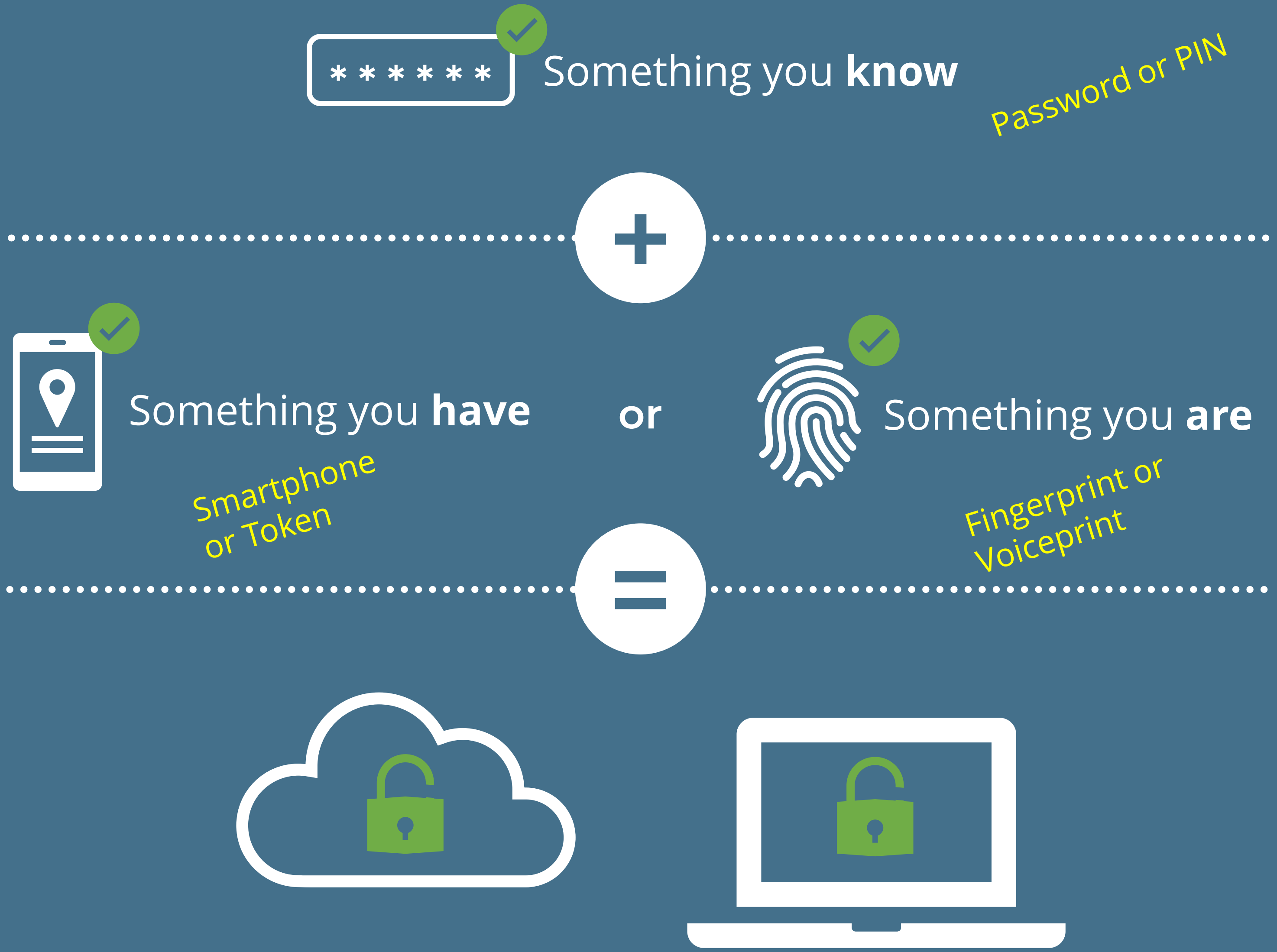
Avoid experiencing your worst day in business

10 Steps to Secure Your Business

1. 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.



Something you **know**

Password or PIN

+

Something you **have**

Smartphone or Token

or

Something you **are**

Fingerprint or Voiceprint

=

Forms of Attacks Prevented

Stops account compromise from lost or stolen passwords/credentials, or poorly constructed primary authentication systems:

Keyloggers

Phishing

Spear Phishing

Brute-Force Attacks

Credential Stuffing

Reverse Brute-Force attacks

Man-in-the-Middle (MITM) attacks

2. 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

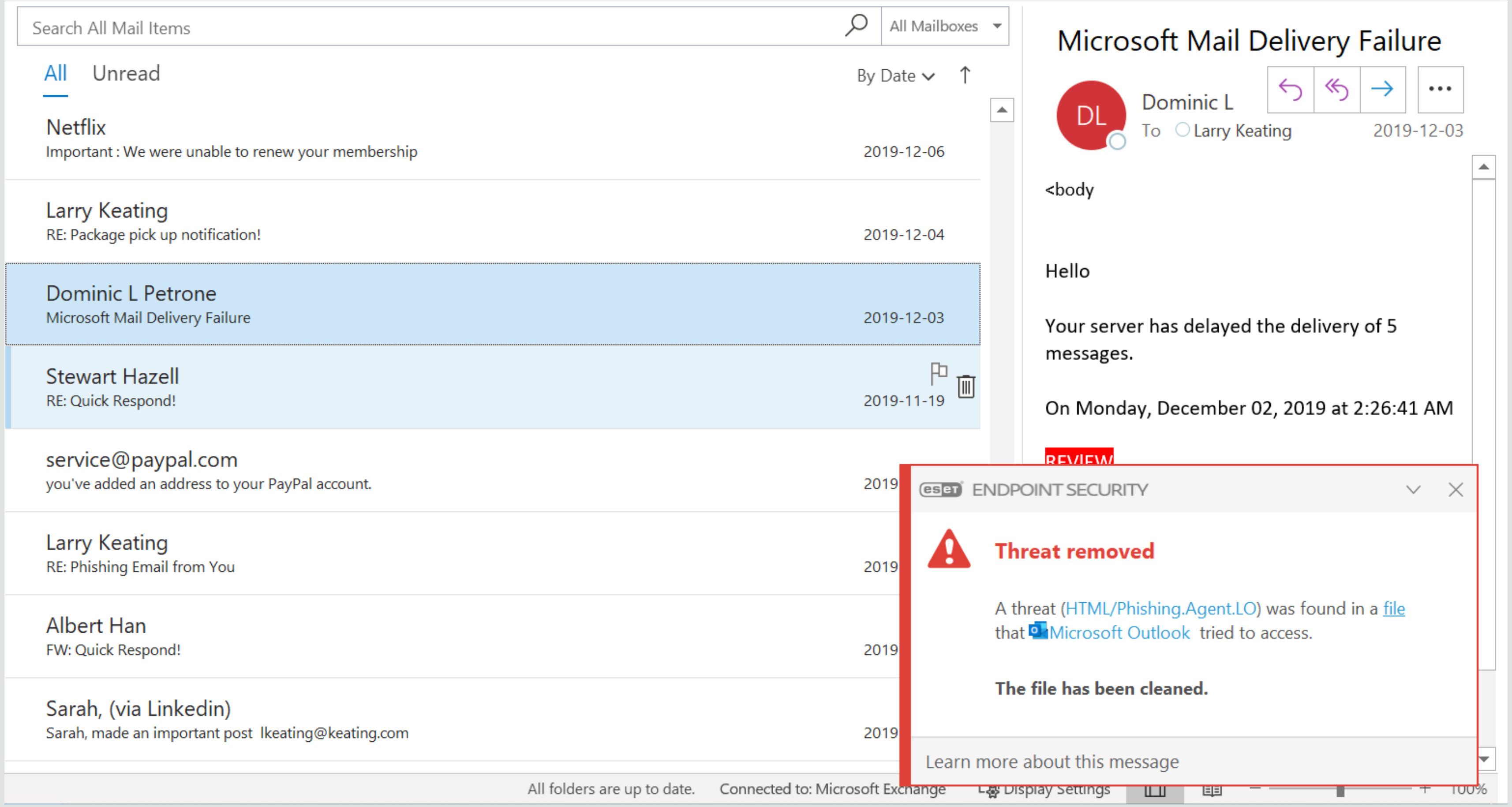
❑ Choose applications and tools that prioritize security

❑ Enable encryption

❑ Ensure the device firewall is enabled

❑ Only do work on your secured computer

Ransomware Attack Email Cleaned



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

All folders are up to date. Connected to: Microsoft Exchange Display Settings 100%

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

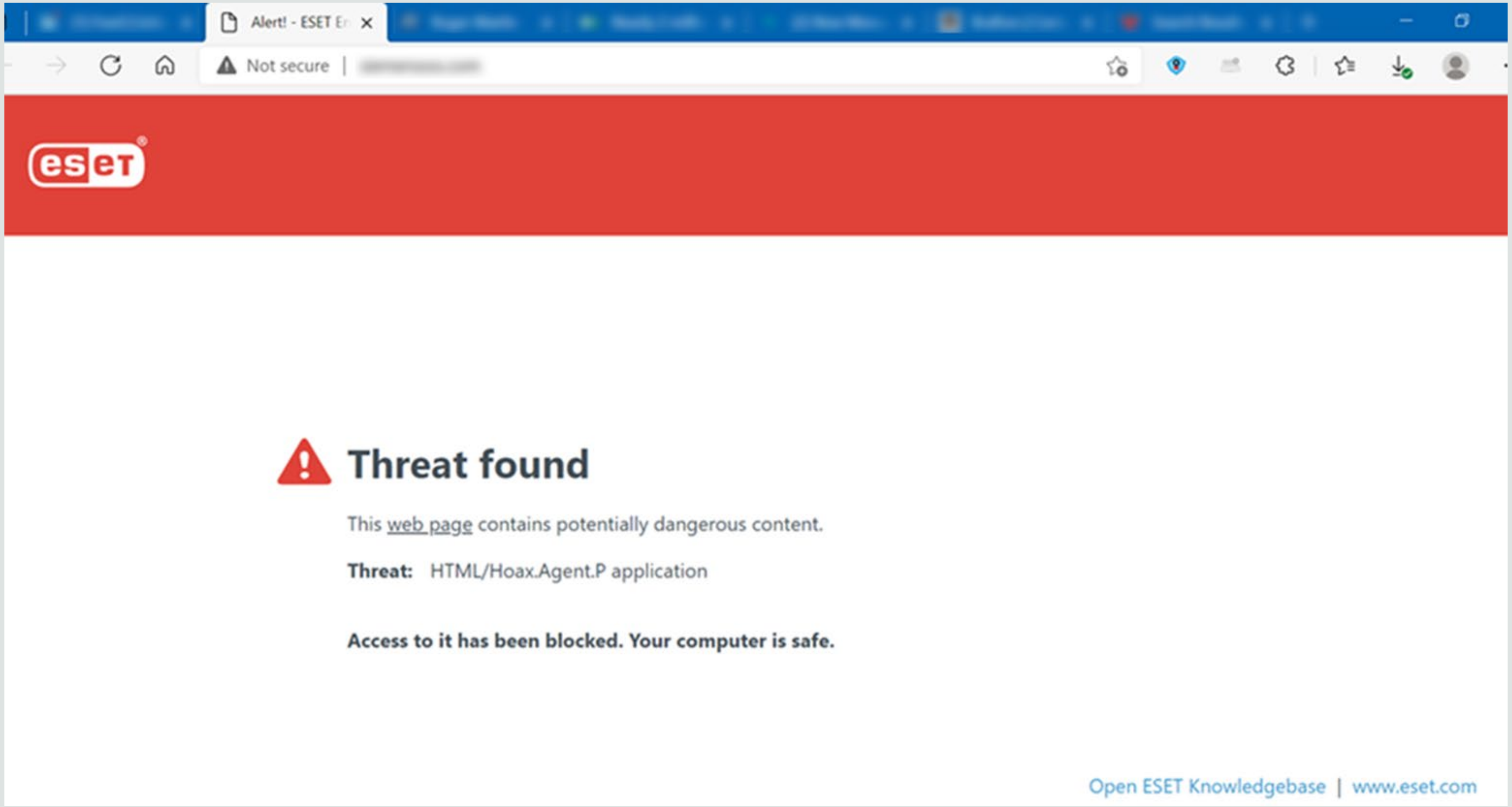
A threat (HTML/Phishing.Agent.LO) was found in a file that Microsoft Outlook tried to access.

The file has been cleaned.

Learn more about this message

Source: NPC Files

Ransomware Drive-by Attack Stopped



Threat found

This web page contains potentially dangerous content.

Threat: HTML/Hoax.Agent.P application

Access to it has been blocked. Your computer is safe.

Source: NPC Files

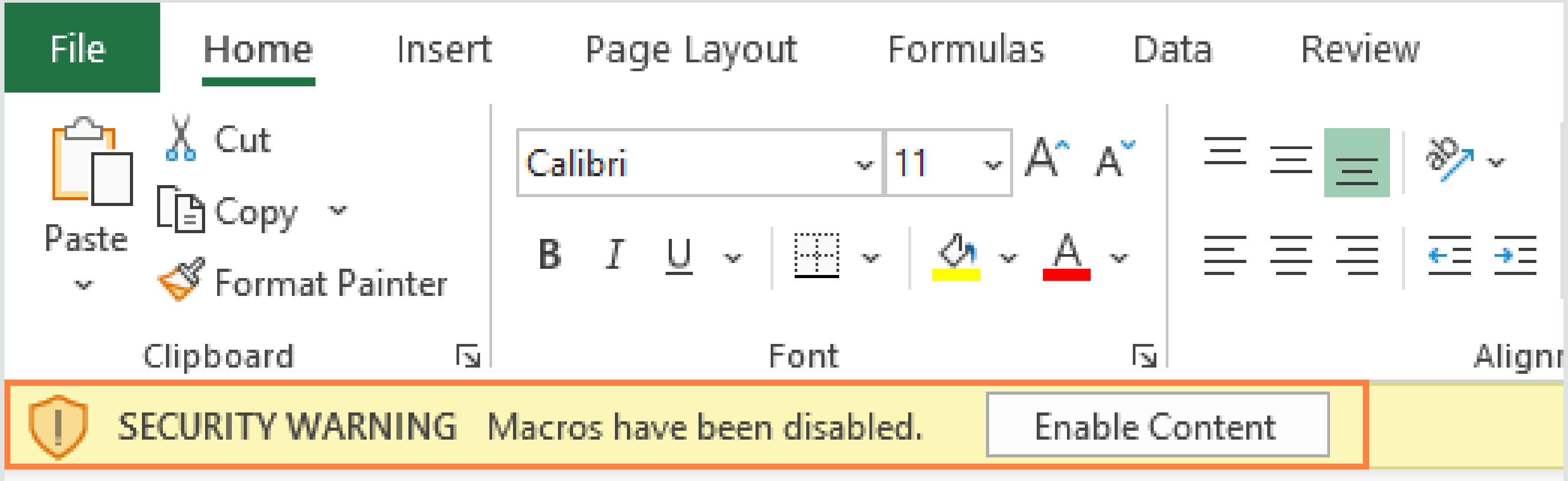
3. Patch, Patch, Patch

- ❑ 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

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 may 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

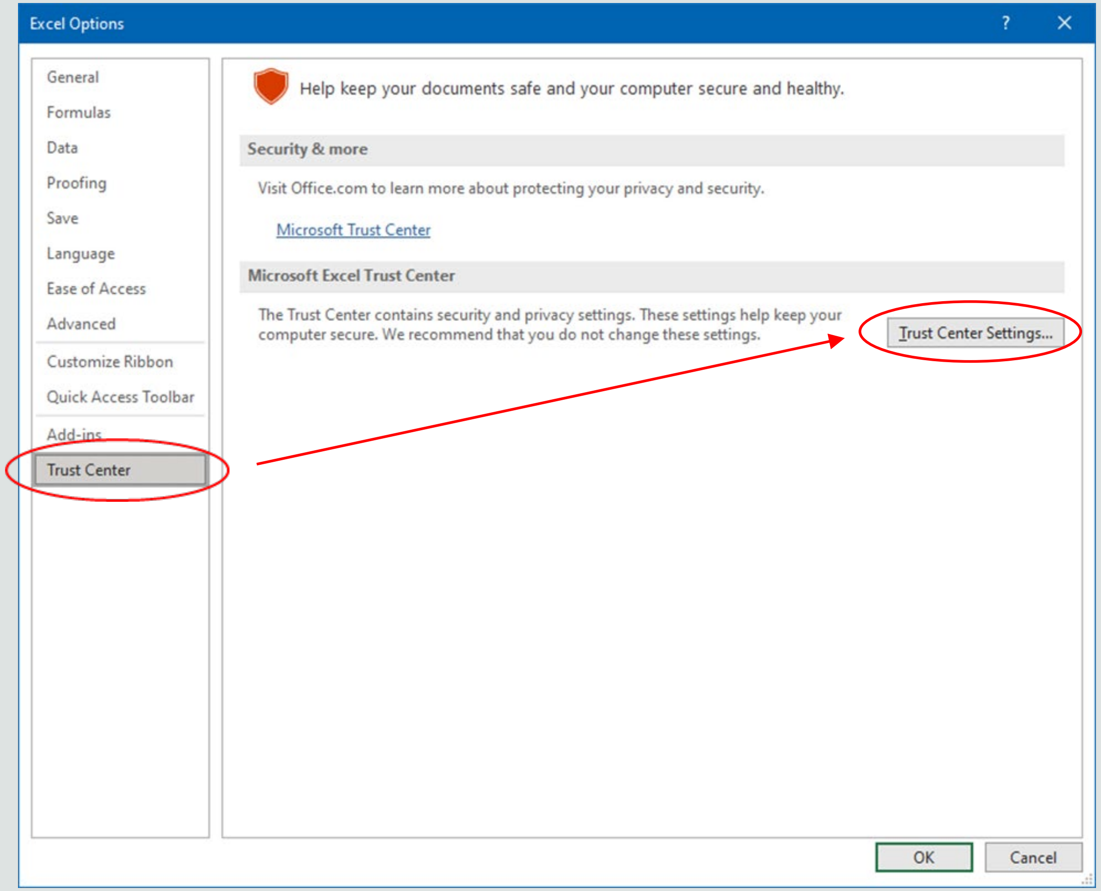
5. Disable Macro Scripts



SECURITY WARNING Macros have been disabled.

Disable Macro Scripts

- ❑ Click File > Options > Trust Center



Help keep your documents safe and your computer secure and healthy.

Security & more

Visit Office.com to learn more about protecting your privacy and security.

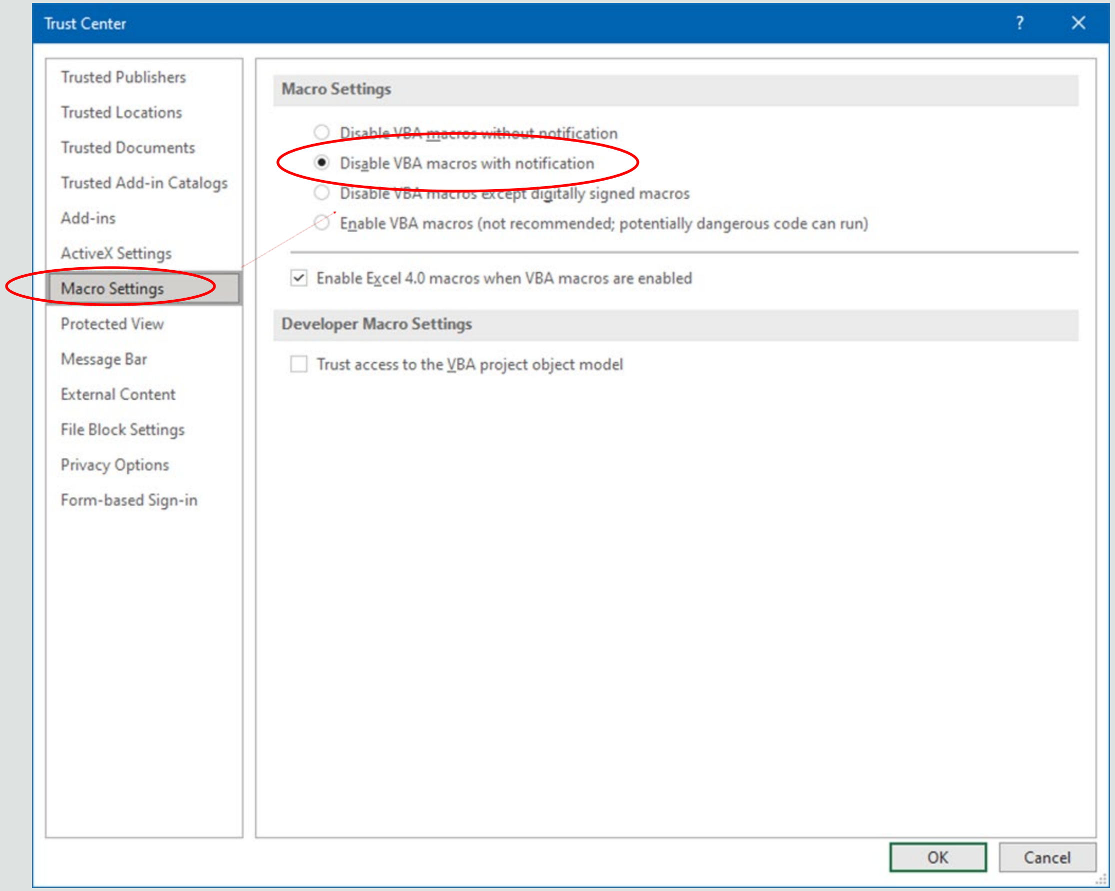
Microsoft Trust Center

Microsoft Excel Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

Trust Center Settings...

Disable Macro Scripts



Macro Settings

○ Disable VBA macros without notification

● Disable VBA macros with notification

○ Disable VBA macros except digitally signed macros

○ Enable VBA macros (not recommended; potentially dangerous code can run)

☑ Enable Excel 4.0 macros when VBA macros are enabled

Developer Macro Settings

□ Trust access to the VBA project object model

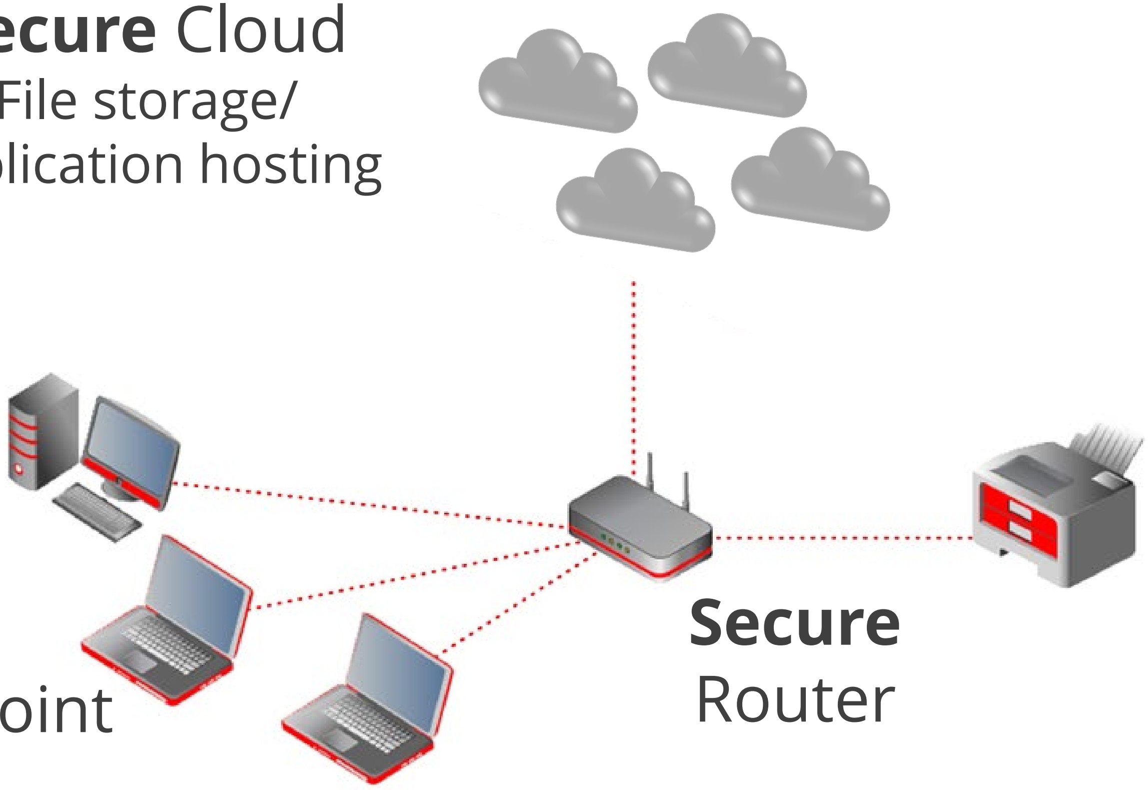
6. Segment Your Network

- ❑ If you have more than one server, or a hybrid-cloud (a local server and a cloud server that talk to each other) require a separate login for each server
- ❑ Segment between applications and cloud instances, where it is not essential they talk. Create workflows that limit the user credentials that cross-talk between systems
- ❑ Control admin credentials and admin tools

Stopping lateral movement in the network limits damage.

Yes, it's inconvenient.

Office of the Future



Secure Cloud
File storage/
application hosting

Secure Printer,
Copier, Scanner

Secure
Router

Secure Endpoint
Devices

7. 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

8. Secure your Remote Access Connections

- Have a professional review you 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"

9. 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

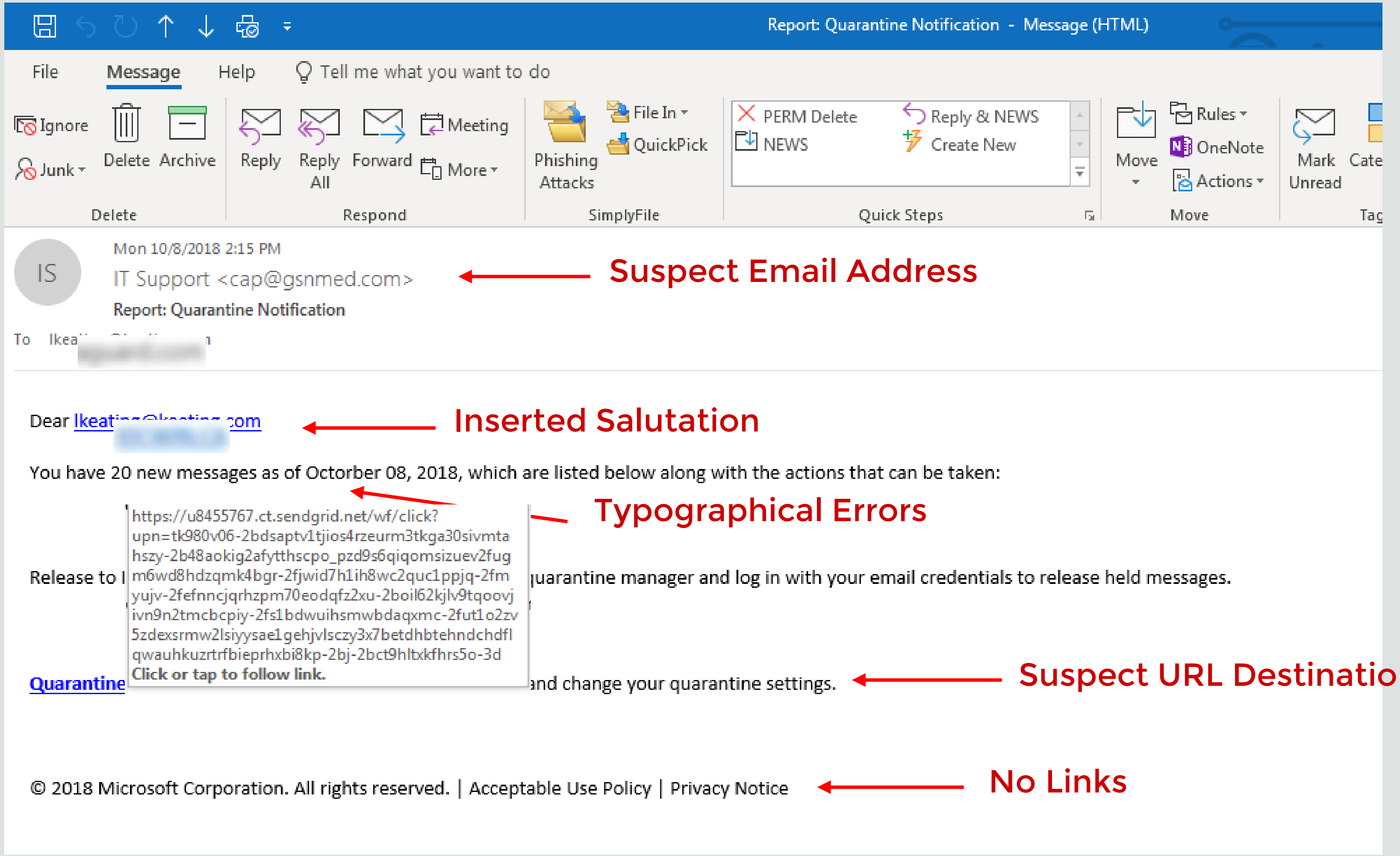
❑ Observe error and warning messages from your computer

❑ Observe email addresses

❑ Establish email source and address verification process

Make it OK to halt the business process to check

Email Attack Clues



IS

Mon 10/8/2018 2:15 PM

IT Support <cap@gsnmed.com>

Report: Quarantine Notification

To lkea[redacted]

Suspect Email Address

Dear lkeat[redacted]com

Inserted Salutation

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

Typographical Errors

https://u8455767.ct.sendgrid.net/wf/click?upn=tk980v06-2bdsaptv1tjios4rzeurm3tkga30sivmtahszy-2b48aokig2afytthscpo_pzd9s6qiqomsizuev2fugm6wd8hdzqmk4bgr-2fjwid7h1ih8wc2quc1ppjq-2fmyujv-2fefnncjqrhzpm70eodqfz2xu-2boil62kjlv9tqoovjivn9n2tmcbcpiy-2fs1bdwuihsmwbdaqxmc-2fut1o2zv5zdexsrmw2lsiyysae1gehjvlsczy3x7betdhbtehndchdflqwauhkuzrtrfbieprhxbi8kp-2bj-2bct9hltxkfhrs5o-3d
Click or tap to follow link.

Release to I … quarantine manager and log in with your email credentials to release held messages.

Quarantine … and change your quarantine settings.

Suspect URL Destination

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

No Links

Source: NPC Files

10. 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

Ransomware Emergency Checklist

❑ Identify what system or device has been attacked, what systems need to be taken off-line, what passwords need to be changed

❑ Look for cause - determine as quickly as possible the source of the infection, method of accessing the system

❑ Disconnect devices from the Internet

❑ Don't immediately shut systems down – shut downs and restarts can trigger additional behaviour in malicious software, destroy forensic information, and cause the loss of other data

❑ Don't start using data cleaning and wiping tools before protecting evidence

❑ Don't immediately use domain administrator credentials. Threat actors may have launched a small attack and are in a system watching for those to do greater damage

❑ Ensure copies of information, damaged computers or affected storage drives are retained for later analysis

❑ Carefully decide where/when/how much to communicate, both internally and externally

❑ Keep an event log of all details

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, preferably using a security professional
- ❑ Acquire a specific cyber package, in addition to your E&O or general liability package

IT Delivery Models

🟥 You Manage

User Owned Break/Fix	**SaaS** (Software)	**MSP** (Managed Service Provider)	**TaaS** (Technology-as-a-Service)
🟥 Data	🟥 Data	🟥 Data	🟥 Data
🟥 Applications	🟩 Applications	🟥 Applications	🟩 Applications
🟥 Support	🟩 Support	🟩 Support	🟩 Support
🟥 Security Monitoring	🟩 Security Monitoring	🟩 Security Monitoring	🟩 Security Monitoring
🟥 Computers	🟥 Computers	🟥 Computers	🟩 Computers
🟥 Servers	🟩 Servers	🟥 Servers	🟩 Servers
🟥 Storage	🟩 Storage	🟥 Storage	🟩 Storage
🟥 Networking	🟥 Networking	🟥 Networking	🟩 Networking

🟩 Managed for You

NPC

Recap

Attacks are becoming increasingly complex, effective, and costly.

- Penetrations and remediation costs are up as the technology used by the criminals is advancing
- Smaller enterprises are more severely impacted
- Invest in up-to-date technologies, and keep it current
- Develop a plan to respond to a successful attack

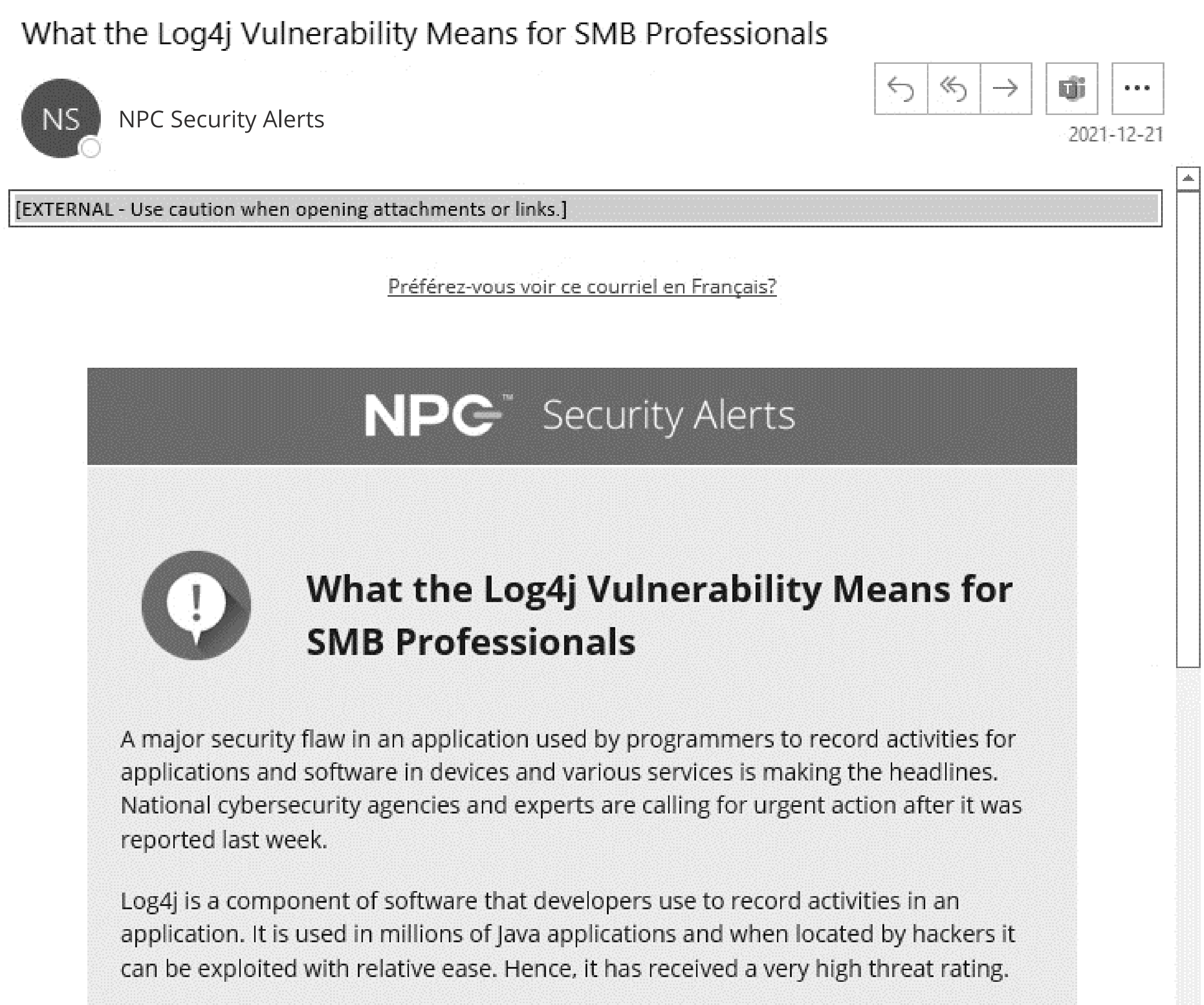
Brand and financial damage from an attack can be considerable

Prepare now

Additional Resources

NPC Security Alerts

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.

Upcoming NPC Webinars

npcdataguard.com/webinars

July 21st 1:00 PM ET (30 mins)	NPC DataGuard Solutions Overview
August 16th 1:00 PM ET (60 mins)	Implementing and Managing the Secure Hybrid Workplace
August 18th 1:00 PM ET (30 mins)	NPC DataGuard Solutions Overview

NPC Webinars Recordings

→ npcdataguard.com/webinars

Enhancing Password Security and the Power of MFA

Building an Incident Response Plan for the SMB

Protecting Your Identity Online

Five-Step Checkup for Your Cyber Protection

& more, and new topics will be added

Thank You

Be Safe & Stay Healthy

lkeating@npcdataguard.com
905-305-6501

NPC™
Smarter Computing