Implementing and Managing the Secure Hybrid Workplace

NPC Safe Computing Webinar Series

August 16th, 2022

Larry Keating, President
Darren Mar, National Sales Manager

NPC DataGuard™

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!


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


IIACCVM
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.

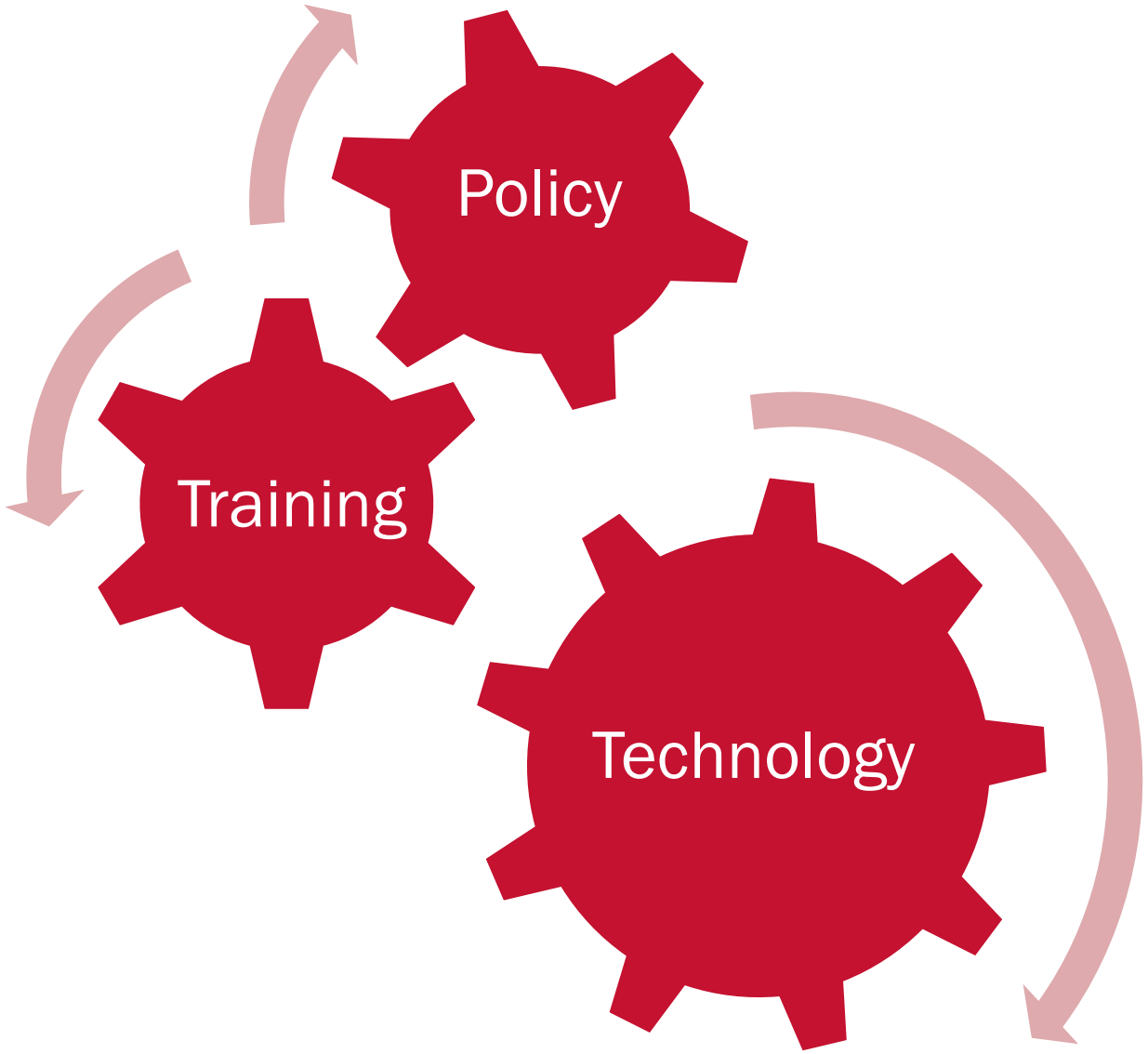

GLOBAL
MAXFIN INVESTMENTS INC.


GROVE POINT
FINANCIAL

Agenda

- Hybrid Work Policies
- Training
- Hybrid Workforce Technology Strategy and Securing the Mobile Workplace
- Q&A

The Three Pillars of Risk Governance



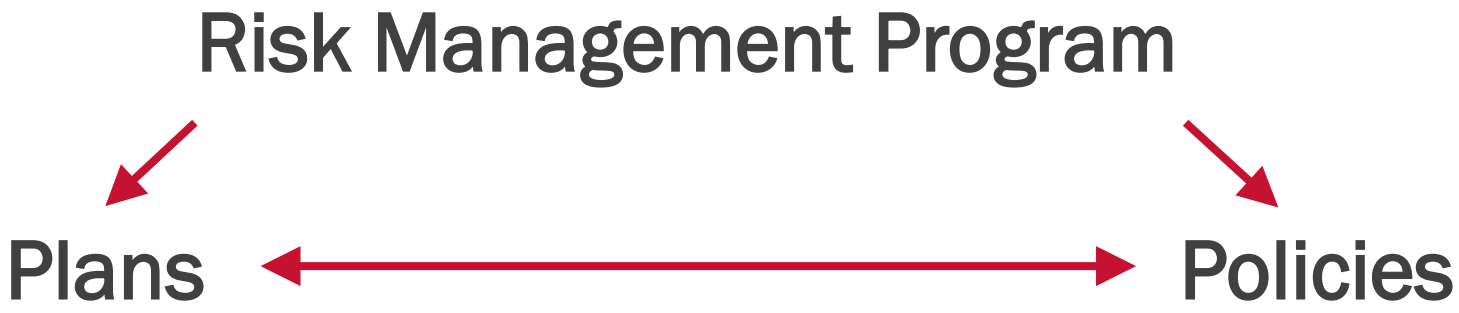
Policy

Policies and Plans Work Together

- Area of concern overview
- Step-by-step actions to achieve a broader goal
- Strategic guidance
- Binds or interlinks some policies

- Descriptive position on key issues
- Specific guidance on key issues
- May set out rules or regulations

Hybrid Work Policies and Plans - Top 5 Picks



1. Incident Response Plan (IRP)
2. Data Collecting, Handling, and Retention
3. Information Security Plan
4. Asset Management Plan
5. Vendor Risk Assessment

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

NPC

NPC IRP Template

Table of Contents

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

https://go.npcdataguard.com/incident-response-template-download

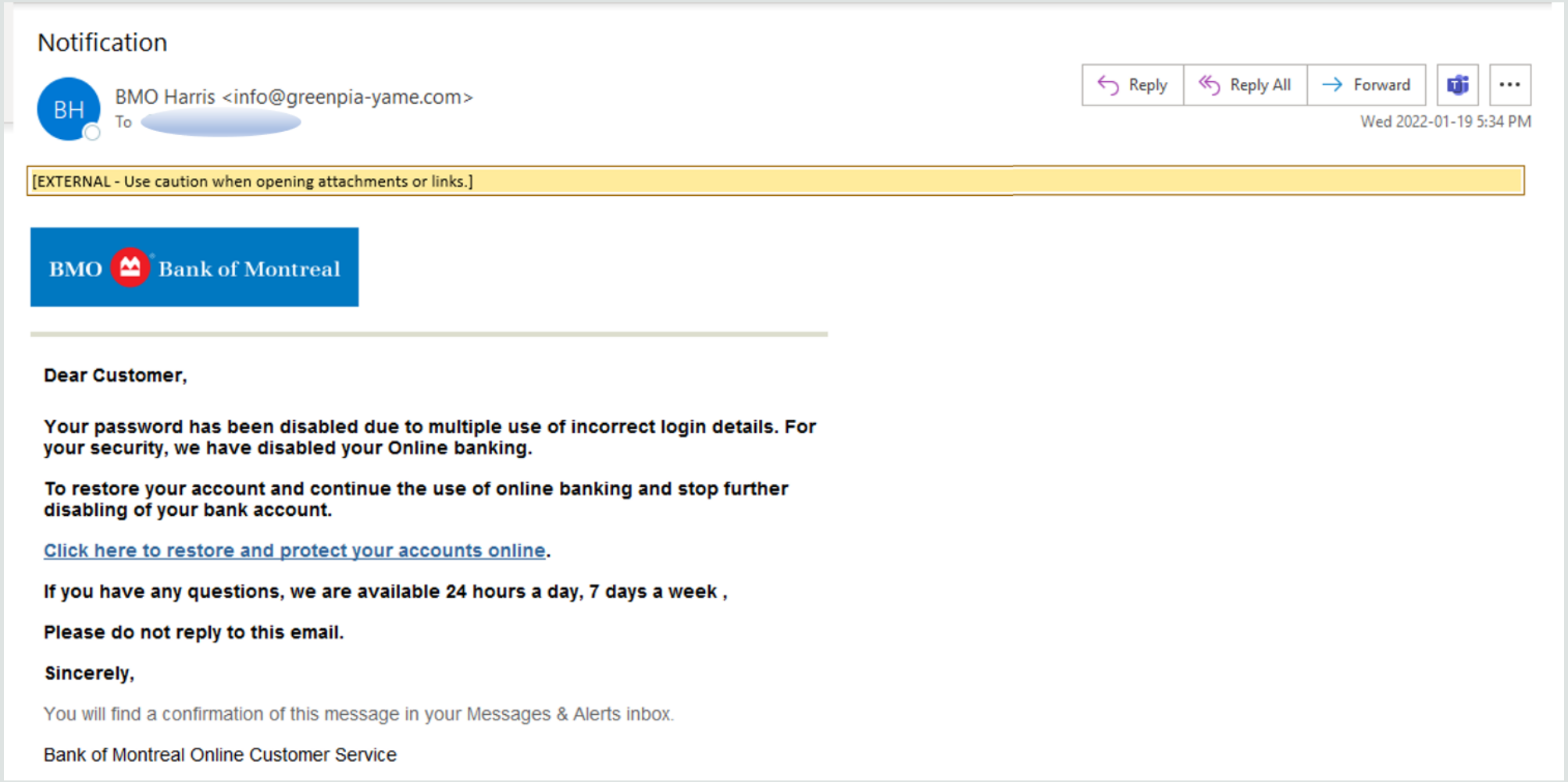
Training

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

Spoof Email



Notification

BH

BMO Harris <info@greenpia-yame.com>

To [redacted]

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 ,

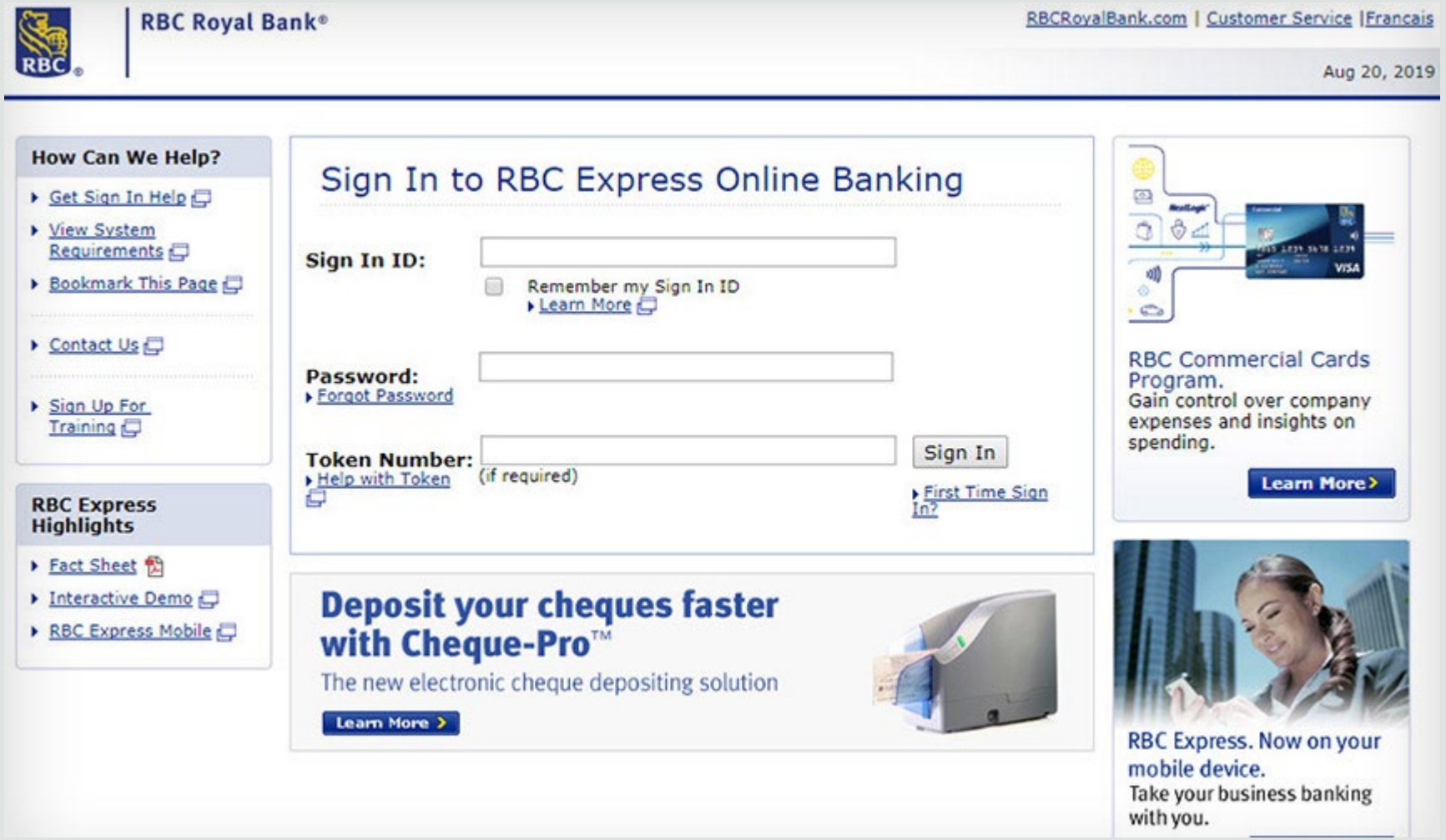
Please do not reply to this email.

Sincerely,

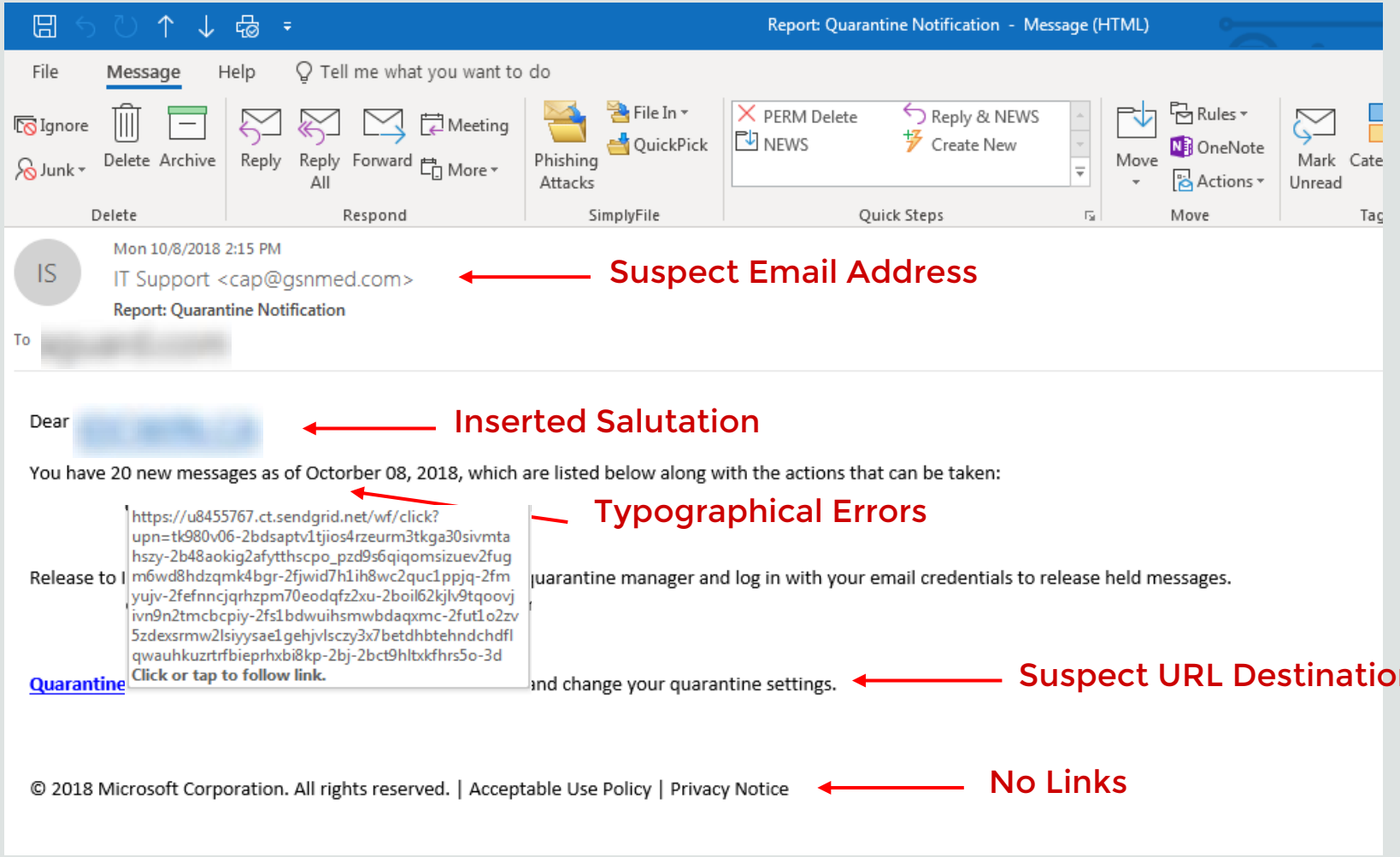
You will find a confirmation of this message in your Messages & Alerts inbox.

Bank of Montreal Online Customer Service

Spoof Banking Website



Email Attack Clues



Source: NPC Files

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

Identity Theft Impact

Fraud and financial theft on an individual can have both an immediate and long-term impact on business credit standing:

- Banking arrangements, payroll and tax payments, etc.
- Illegal purchases from your accounts and credit facilities
- Loans, mortgages and lines of credit taken out in your name
- The sale of your home or other assets
- Crimes committed in your name
- Government benefits and identities in your name

Checklist

Technology

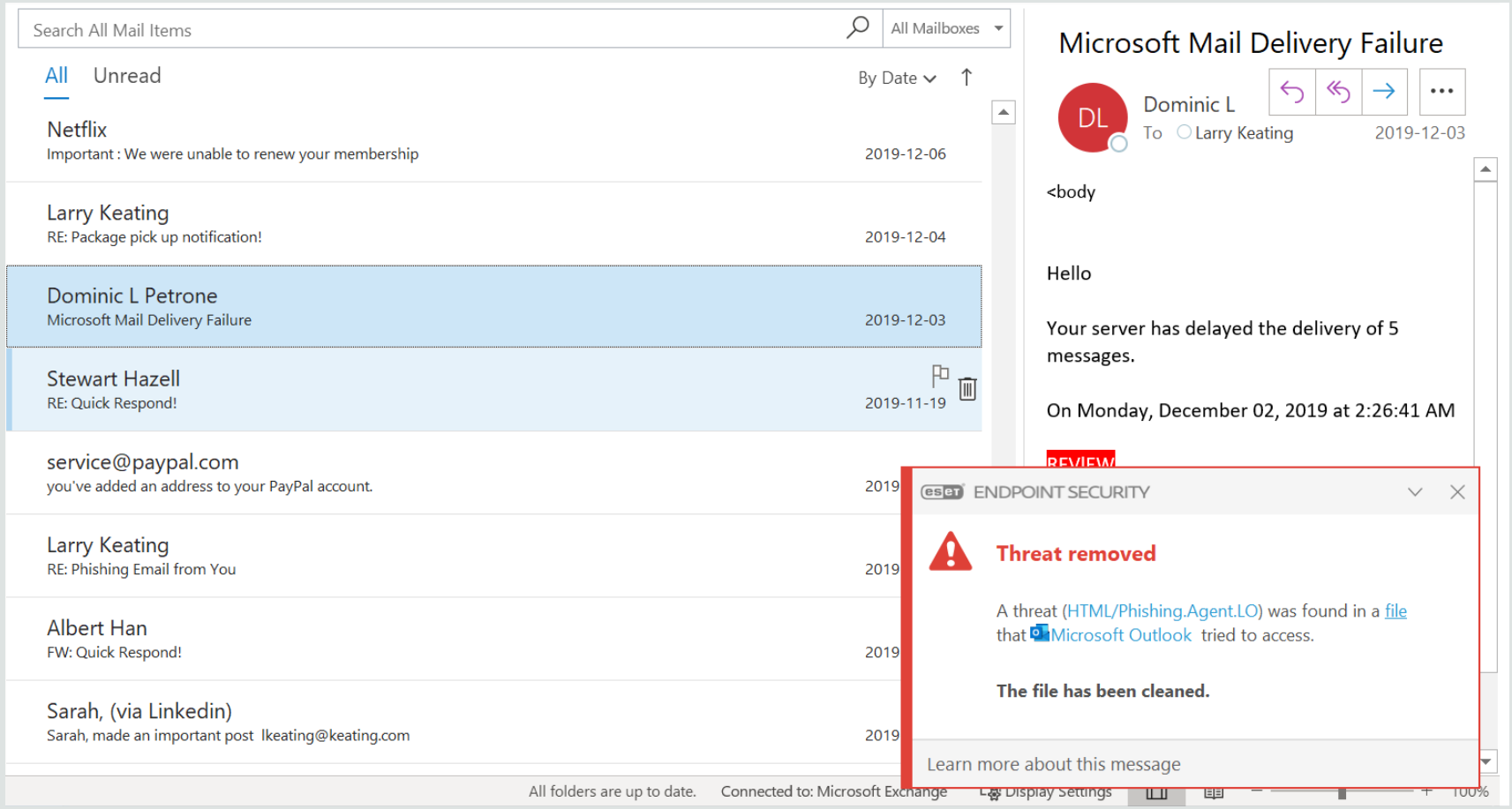
Secure Work From Home

- ❑ Secure your endpoint devices and your office environment
- ❑ Use encryption, back up your data, patch update, use strong anti-malware
- ❑ Use strong passwords, enable two- or multi -factor authentication
- ❑ Secure your Wi-Fi
- ❑ Secure your connections:
  - ❑ Use a VPN
  - ❑ Use only secure (https) connections
  - ❑ Secure your remote desktop tool

Checklist

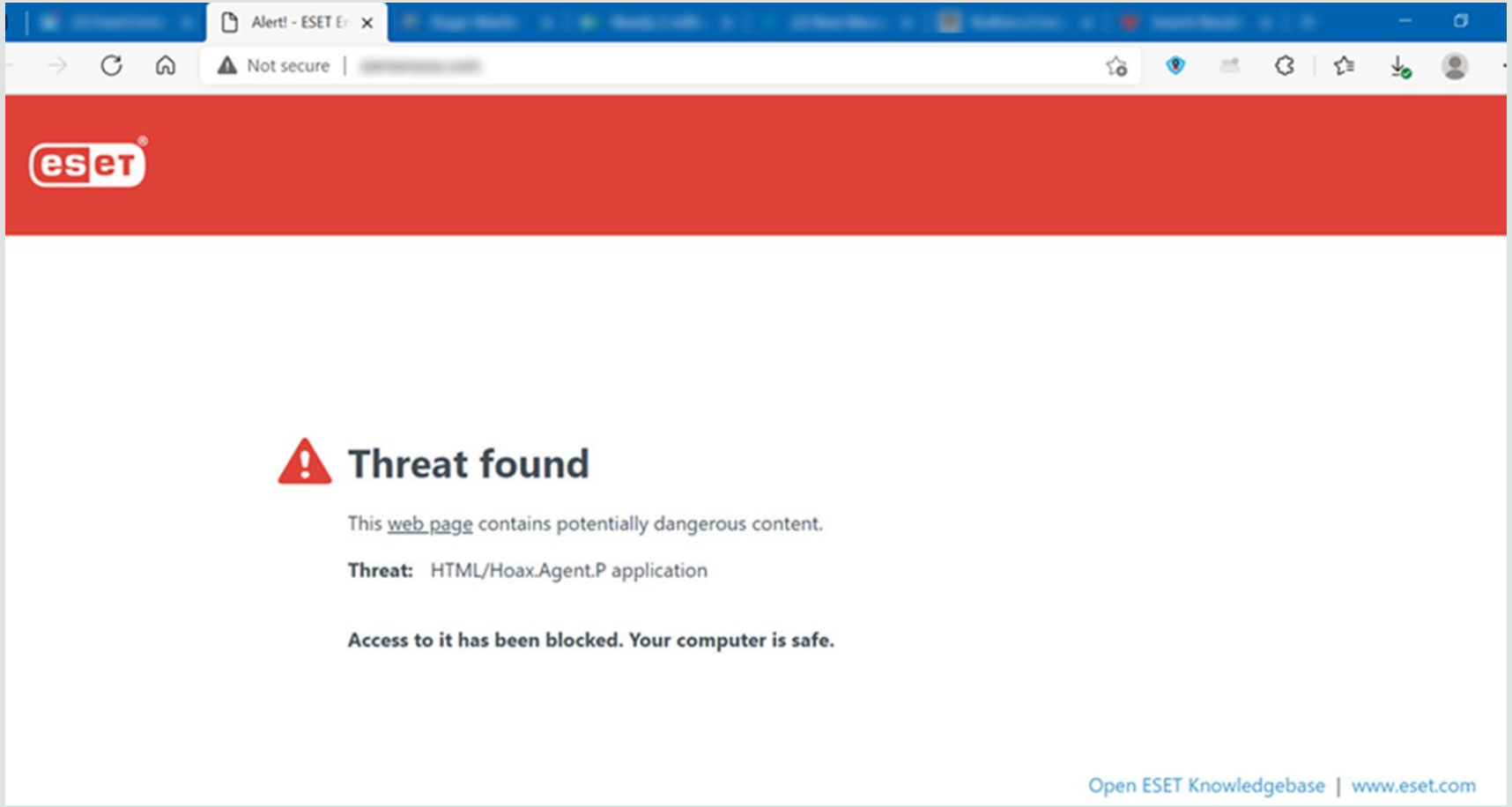
NPC

Ransomware Attack Email Cleaned



Source: NPC Files

Ransomware Drive-by Attack Stopped



Source: NPC Files

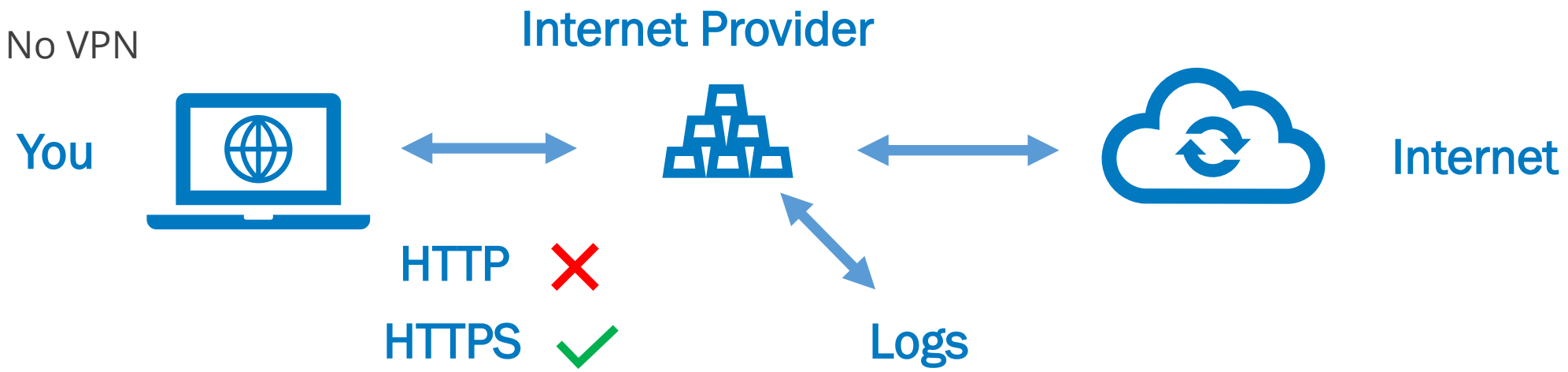
Enable Multi-Factor Authentication

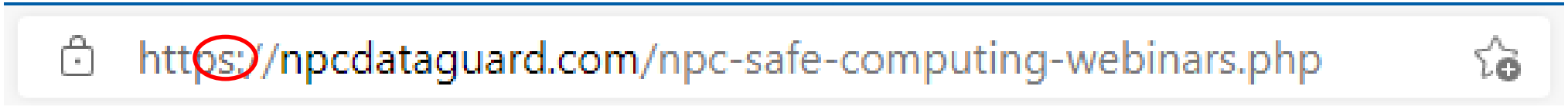
Definition:

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

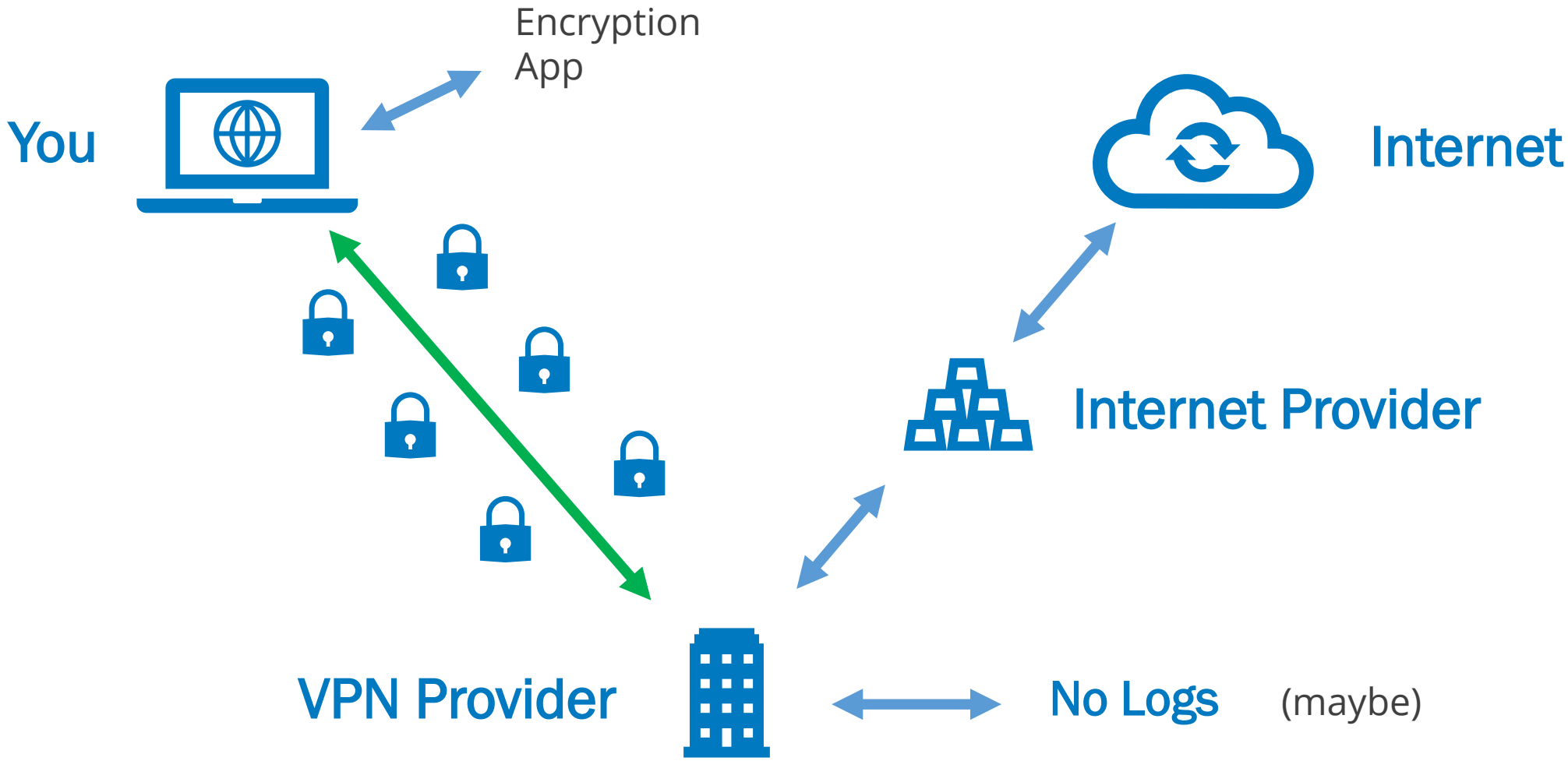
Virtual Private Network (VPN)

Provides a secure “tunnel” to connect to websites and services on the Internet





Virtual Private Network (VPN)

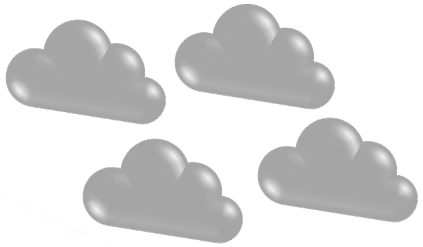


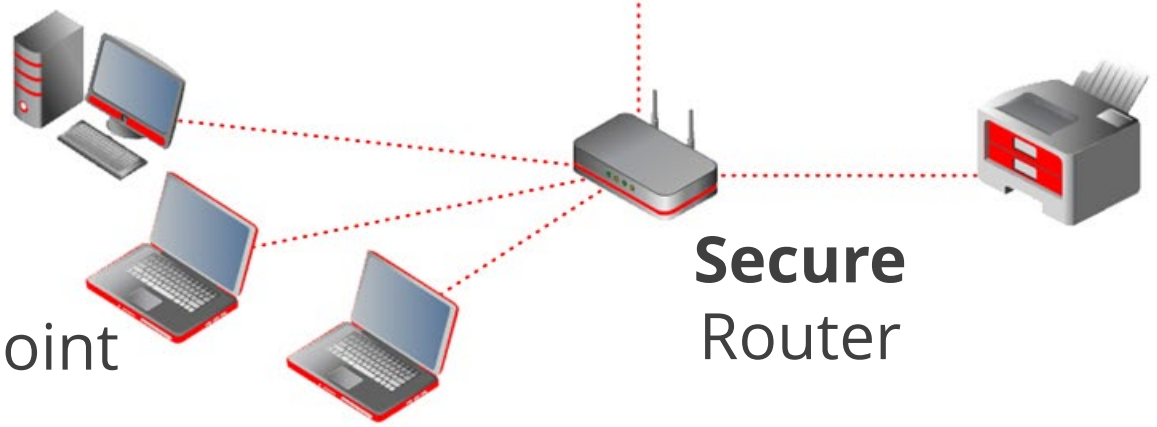
Bonus Steps

- ❑ 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

Office of the Future

Secure Cloud
File storage/
application hosting



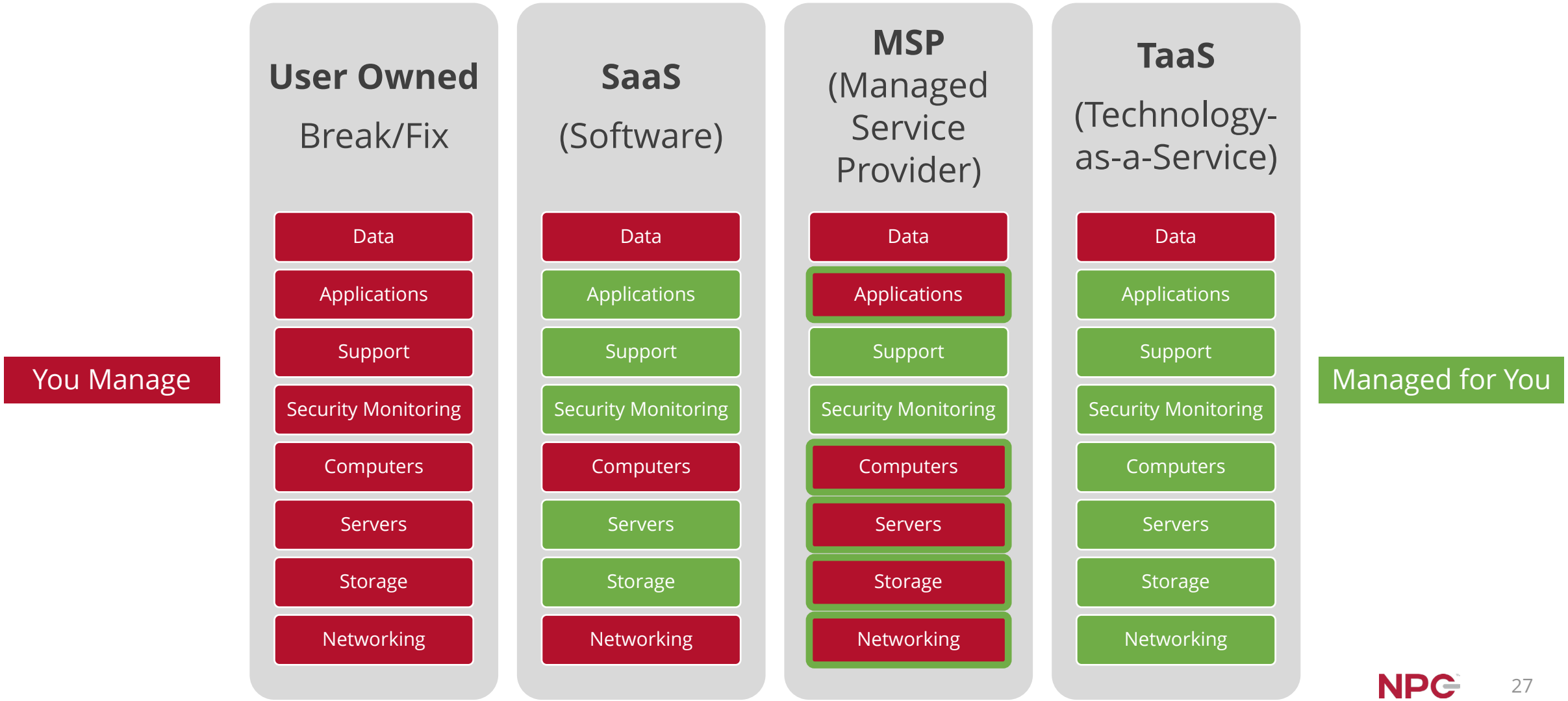


Secure Printer,
Copier, Scanner

Secure
Router

Secure Endpoint
Devices

IT Delivery Models



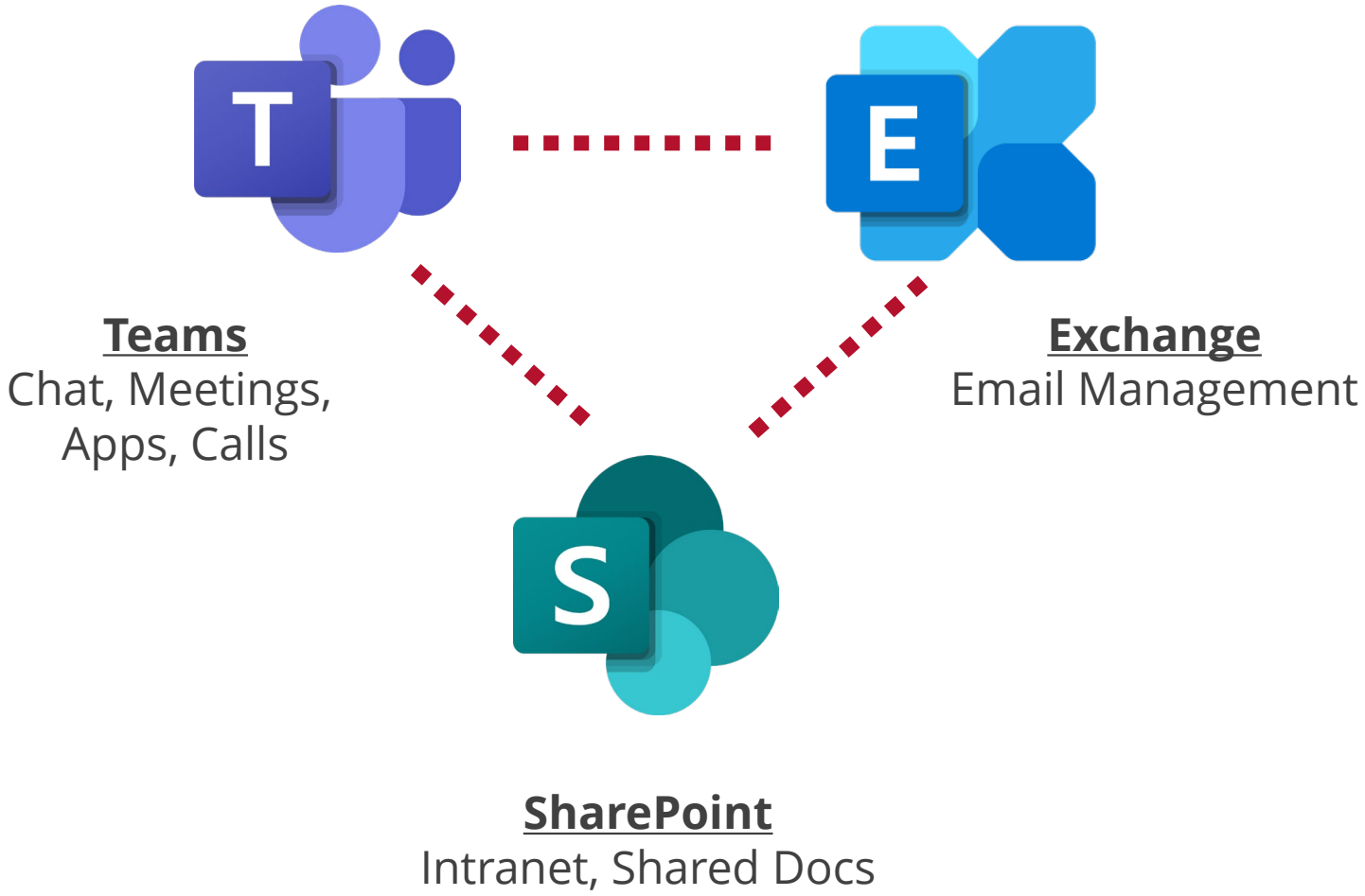
What's the Benefit?

- As-a-service models remove the cost of custom-building common application, network, server, security, and services needs
- Specialization by the provider allows more features for less cost, improved performance, security, and reliability
- Allows for more economical "scaling up" or "scaling down"

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

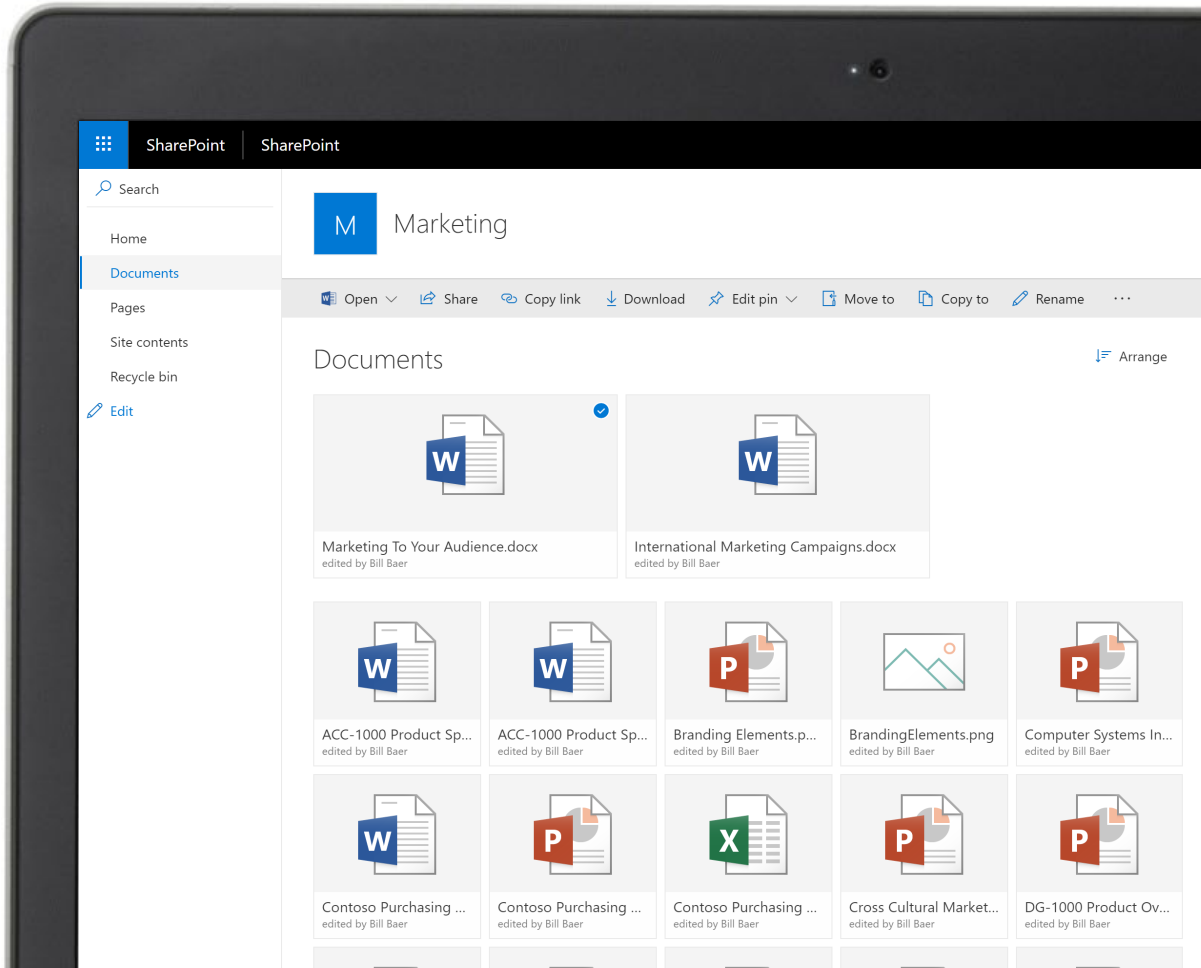
Business Integration of 365 for the SMB

A suite of mobile, desktop and cloud-based productivity tools on a unified communication and collaboration platform



Securely Connect to Your Data with SharePoint

- Replaces your file server, USB drives, or email file sharing
- Mobile access everywhere
- Powerful collaboration and integrated tools and apps
- Generate links for secure file sharing, or grant controlled access
- Data sovereign



Microsoft 365 Business Premium Security…

Multi-factor Authentication with phone call, text, or app as second factor

Location-Based Authentication

Advanced Threat Protection:

- Increased SPAM and threat filtering through AI
- Safe Attachments
- Safe Link Protection

Administrator account control, including user access and password policy management

Email:

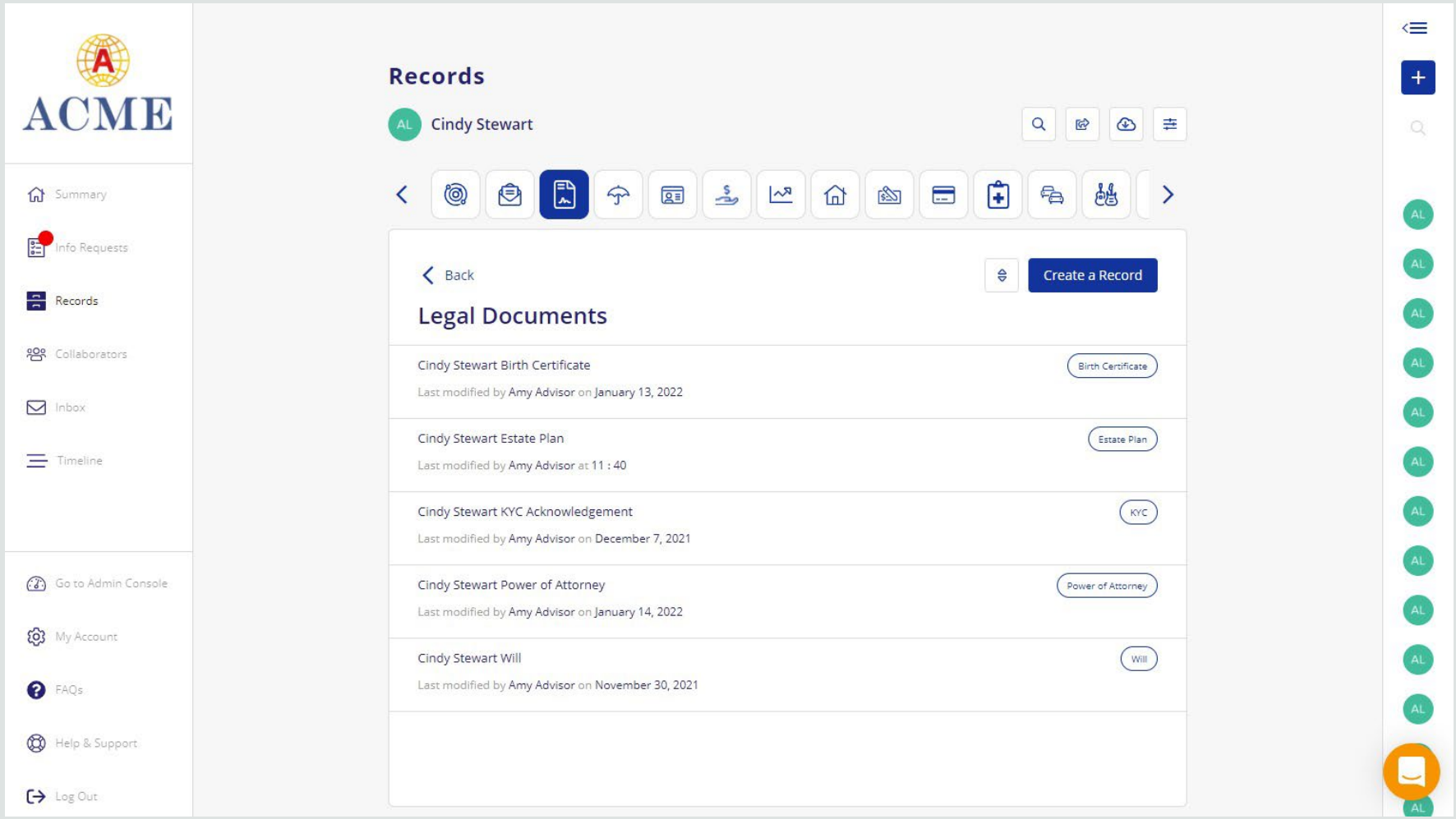
- Auto-forwarding control
- Message encryption
- Advanced anti-phishing capability
- Blocks specific file extensions known to distribute malware
- Data Loss Prevention and Exchange Email Online Archiving

Source: NPC Files

SideDrawer

- **Info Request instantly organizes received documents into relevant Tiles and Records**

SideDrawer



Recap

Hybrid Work From Anywhere

- Consider the Three Pillars of Risk Governance:
  - Policy, Training, Technology
- Secure your devices and your systems
- Embrace a small footprint, secure-cloud strategy
- Invest in up-to-date technologies, and keep it current

Secure Work From Anywhere Can Enable Your Team, and Protect Your Business

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

NPC Security Alerts

npcdataguard.com/alerts

What the Log4j Vulnerability Means for SMB Professionals

NS 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

August 18th 1:00 PM ET (30 mins)	NPC DataGuard Solutions Overview
September 13th 1:00 PM ET (60 mins)	Work From Home Securely with Microsoft 365
September 15th 1:00 PM ET (30 mins)	NPC DataGuard Solutions Overview
October 18th 1:00 PM ET (60 mins)	How to Protect Your Business from Email Compromise Attacks

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

10 Steps to Secure Your Business from Ransomware

& more, and new topics will be added

Thank You

Be Safe & Stay Healthy

lkeating@npcdataguard.com
905-305-6501

dmar@npcdataguard.com
905-305-6513

NPC™
Smarter Computing

Identity Protection Checklists

Computing Security Basics to Protect Your Identity

- ❑ Secure your computer
- ❑ Patch your devices and your software
- ❑ Use top quality anti-virus software
- ❑ Use strong, unique passwords
- ❑ Use Multi-Factor Authentication
- ❑ Secure your Wi-Fi
- ❑ Encrypt your data
- ❑ Identify phishing emails
- ❑ Have a second computer for play
- ❑ Lock your phone, put anti-virus software on it, limit its use for work

Save this **list** for later.

Advanced Computer Hygiene

- ❑ Delete/archive files with personal information when they are no longer required
- ❑ Individually encrypt sensitive files with a long password
- ❑ For long-term documents, print them, store securely, then delete the electronic versions
- ❑ Never store your key identifiers, driver's license number, social insurance number, etc., on your computer or phone
- ❑ Use a shredding tool, for paper and for data on drives and phones
- ❑ Erase your digital footprint on your device
  - ❑ Use a cleaning tool that is stronger than deleting your browsing history, like Disk Cleanup or CCleaner, to delete temp and cache files

Save this **checklist** for later.

Browsing

- ❑ Decline data sharing, restrict cookies
  - A more "personalized" browsing experience is a poor trade-off for your identity
- ❑ Resist saving credit card information and auto-fill information in your browser
- ❑ Don’t overshare on social media
- ❑ Limit information in “About Me” in your social media profiles

Save this **checklist** for later.

Online Identity Protection: Awareness

- ❑ Consider where you give your email address, or personally identifiable information
- ❑ Is your personal email address your business email?
  - Create a second email address for social media, news sites, games, etc. Save your primary for personal communications, banking, etc.
- ❑ Be careful with out-of-office messages
- ❑ Even if you are not going to use a specific social media service, consider creating a profile anyway to consume the use of your email address. Watch it for postings
- ❑ Encrypt your email
  - Office 365 at certain license levels offers this
  - Extensions are available for Gmail to encrypt

Save this **checklist** for later.

Online Identity Protection: Awareness

- ❑ Be careful what apps you download, especially free apps
- ❑ Google Security Check will show you what apps are pulling what from you. Apple will show you what apps have your ID, what is active
- ❑ Only buy online from reputable sites
- ❑ Post nothing that is Personally Identifiable Information (PII) on social media, consider setting your accounts to private
- ❑ Understand your Terms of Service and watch policy changes
- ❑ Use different screen names and images
- ❑ You can blur your house on Street View!

Save this **checklist** for later.

Back

Secure Your Hybrid Workplace Devices

Securing your Workplace Devices

- ❑ Ensure you have up-to-date and fully patched:
  - ❑ Computer BIOS, operating system, Office suite
  - ❑ System apps like Java and Adobe
  - ❑ Web browser
  - ❑ Anti-malware suite
- ❑ Use strong passwords, enable Multi-Factor Authentication
- ❑ Enable encryption, and manage it carefully
- ❑ Enable personal firewall on endpoint computers
- ❑ Change default passwords on all IoT devices
- ❑ Only do your work on a secured device

Save this **checklist** for later.

Protect Your Systems

- ❑ Apply principles of least privilege for user access, lock admin accounts
- ❑ Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- ❑ Ensure all your web connections are https
- ❑ Use a VPN if you are still accessing a private server or using public Wi-Fi
- ❑ Ensure you have a professional look at your remote desktop setup

Save this **checklist** for later.

Backup Your Files

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
- ❑ Do not keep your backup in the same place as the computer(s) you are backing up
- ❑ Ensure you have a backup multiple versions deep, and it connects to your computers only when backing up
- ❑ Distinguish between file sharing, primary storage vs. backup

Save this **checklist** for later.

Secure Your Wi-Fi

- ❑ Ensure that your home Wi-Fi:
  - ❑ Has a strong, long password that has been changed from the default
  - ❑ WPA2 level security is enabled
  - ❑ Disable UPnP - Universals Plug and Play
  - ❑ Disable WPS – Wi-Fi Protected Set-Up
  - ❑ Ensure your home router is patched and up-to-date
  - ❑ The router's firewall, if present, is enabled
  - ❑ Has an obscure SSID, or disable SSID broadcast
- ❑ Change default passwords on all IoT devices

Save this **checklist** for later.

Secure Work From Home Checklist

- ❑ Browsing:
  - ❑ Decline data sharing, restrict cookies
    - A more "personalized" browsing experience is a poor trade-off for your identity
  - ❑ Resist saving credit card information and auto-fill information in your browser
  - ❑ Don’t play, casually browse, or shop on your work computer
- ❑ Ensure your smartphone is secured, consider an anti-malware app for it
- ❑ Don’t forget about physical workspace security:
  - ❑ A separate, low-traffic area
  - ❑ Ensure home bandwidth is adequate

Save this **checklist** for later.

Password and MFA Checkup

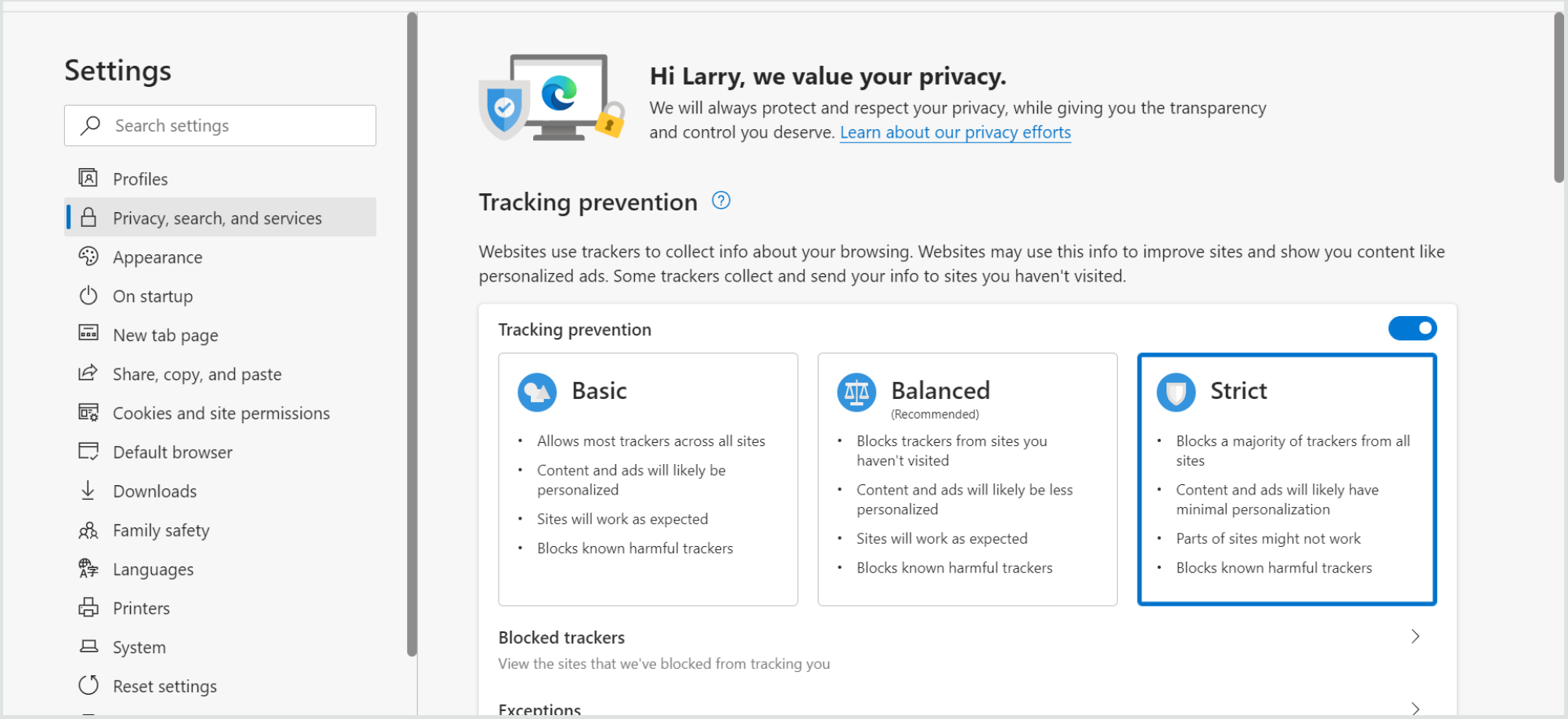
- ❑ Review (or establish) your password and authentication policy
  - ❑ Minimum password lengths
  - ❑ Change requirements
  - ❑ Requirements for 2FA or MFA
- ❑ Inventory what systems and devices require passwords, commenting on length and complexity requirements, risk factors of key systems
  - ❑ Check on staff meeting those requirements
  - ❑ Consider the use of password management tools, and SSO (Single-Sign On) solutions, fingerprint readers

Save this **checklist** for later.

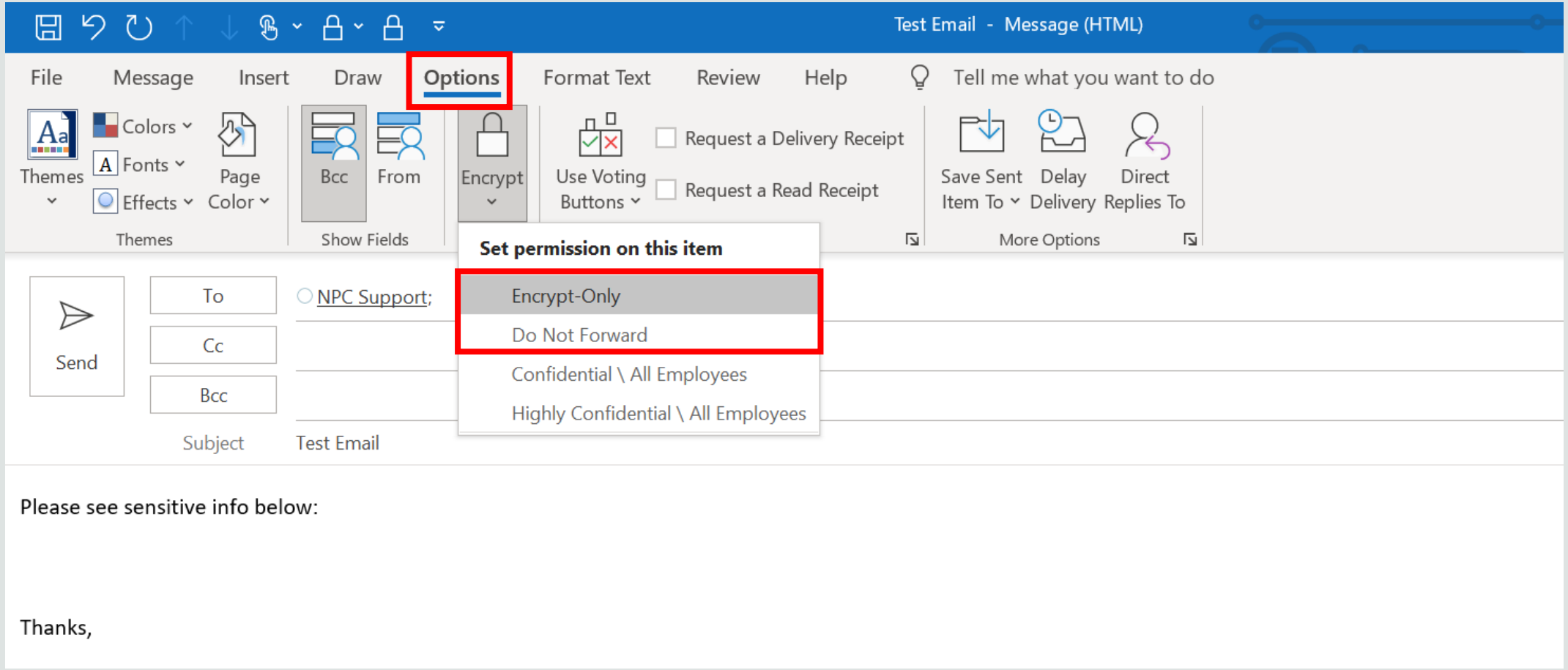
Patch, Patch, Patch

- 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

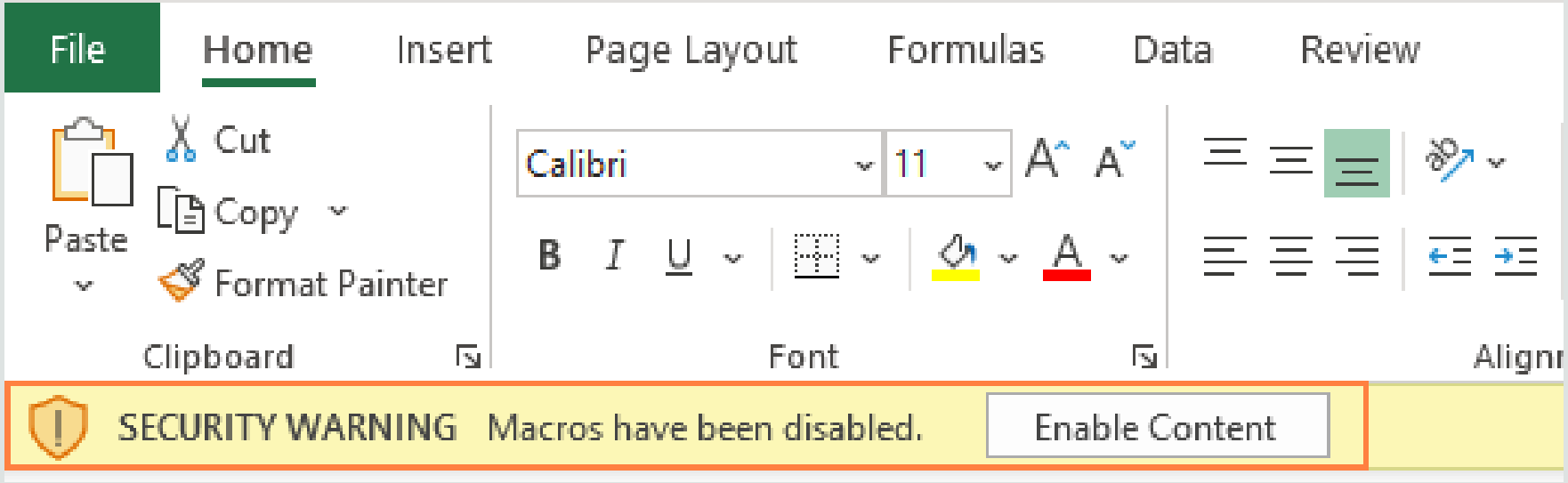
Block Tracking & Data Sharing with Your Browser



Encrypt Email

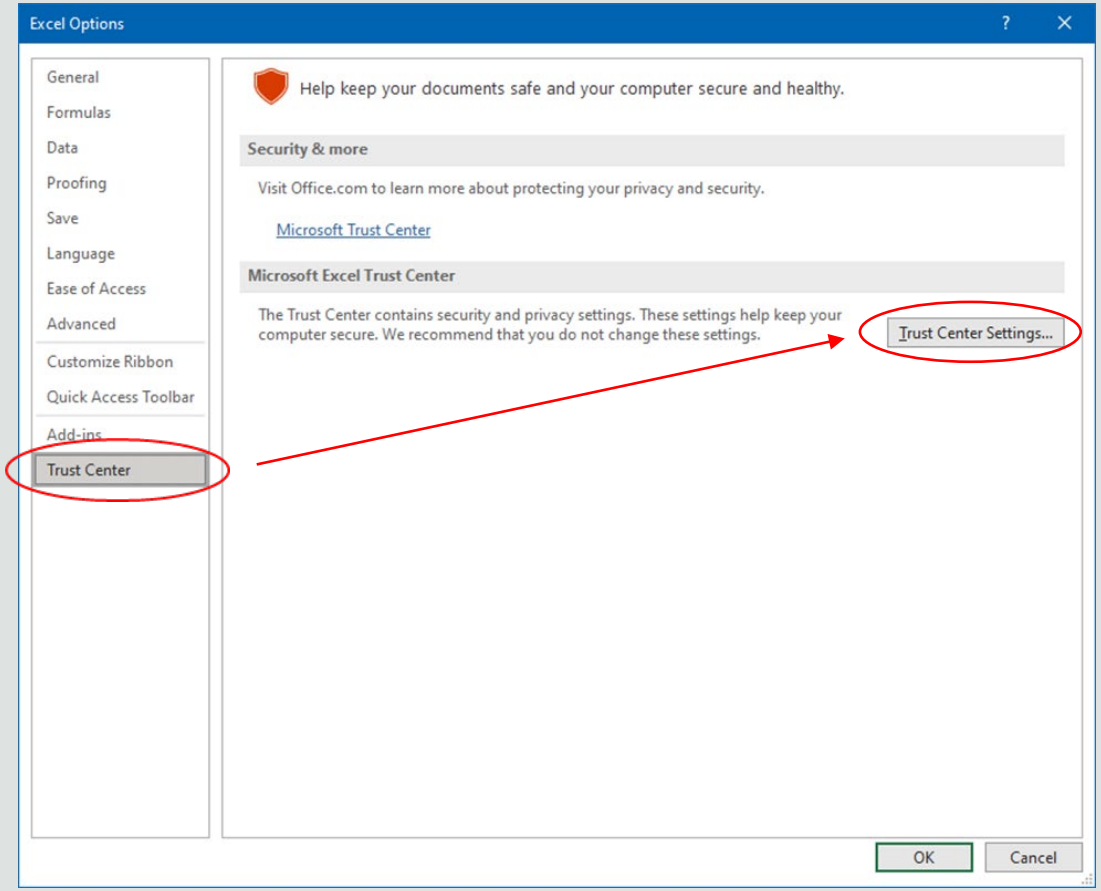


Disable Macro Scripts

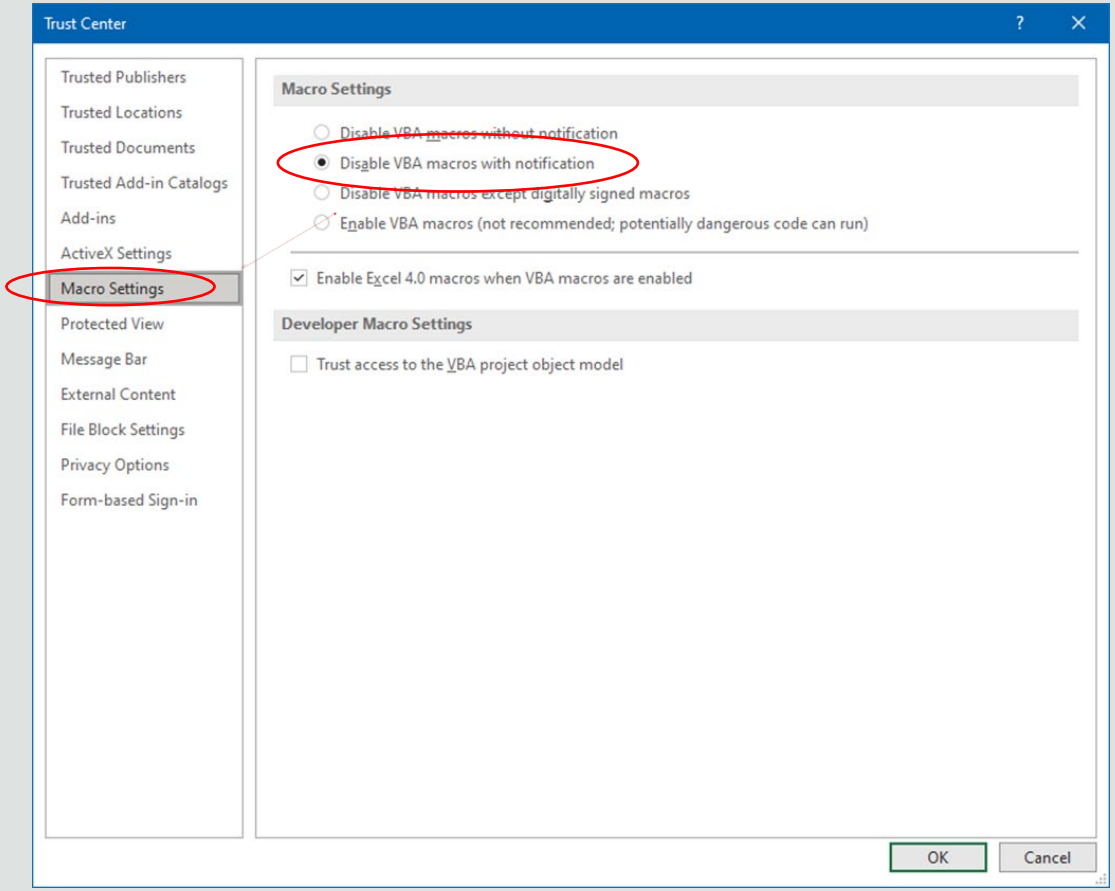


Disable Macro Scripts

- Click File > Options > Trust Center



Disable Macro Scripts



Back