



# How to Protect Your Business from Email Compromise Attacks

NPC Safe Computing Webinar Series

---

October 25<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!



# 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
- Dedicated Account Manager
  - A custom and consultative approach

# Agenda

- What's the Issue?
- 

- Attack Methods
- 

- What to Do
- 

- Q&A



**What's the Issue?**

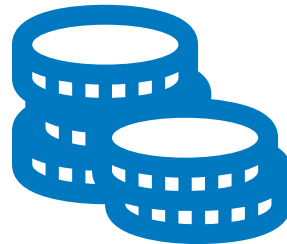
# What's the Issue?

---

**BEC (Business Email Compromise) / EAC (Email Account Compromise)** are the most productive form of cyberattack for threat actors, causing losses to persons and companies of all sizes — 17x greater than ransomware.



Attacks are increasing in effectiveness

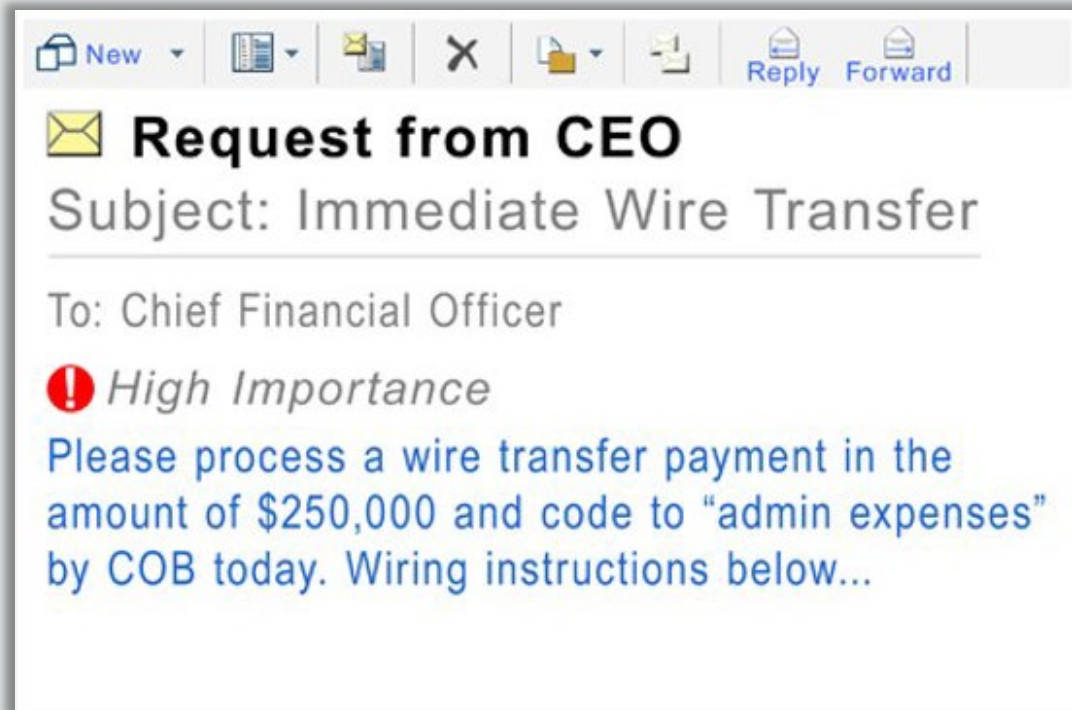


Higher costs and business impacts



All business sizes are a target

# BEC Definition



- A type of email scam combining a malware phishing attack and “social engineering” that includes analysis of the target company and individuals’ publicly available information.
- The victim’s email account and/or computer is compromised.
- The criminal then impersonates the victim or uses their email account to execute fraudulent financial transactions.



# How BEC Works

## Stage 1: Penetration

Hacker targets victim and sends malware via email, phishes login, infected websites, etc.



## Stage 2: Intelligence Gathering



# How BEC Works

## Stage 3: Attack



**Victim**

Opportunistic event occurs:

- Change of personnel or management
- Change of process
- Executive is travelling



**Hacker**

**Impersonate Victim Sending Spoof Emails or Logging into Systems with Stolen Credentials**

**Fake Invoice**



**Fraudulent Transfer**



**Payment Redirect**



**Supplier Side Redirect**

**Business Associates, Suppliers, and Vendors**

# Primary Attack Methods

---

- **Malware:** malicious software that provide access or control of a system or information, delivered via email or web page
- **Spoofing:** faking an email address or creating a similar one that is so close it is not recognized as fraudulent
- **Spearfishing:** focused attacks on an individual, with compelling positioning or information to gain trust prompting target to reveal information or click
- **Honourable mention:**
  - Social media spoofing, texting, fake websites


# 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](#)

# SpooF Banking Website

The image shows a screenshot of a spoofed RBC Royal Bank website. The page layout includes a header with the RBC logo, the text "RBC Royal Bank®", and navigation links for "RBCRoyalBank.com", "Customer Service", and "Français". The date "Aug 20, 2019" is displayed in the top right corner. The main content area features a "Sign In to RBC Express Online Banking" form with fields for "Sign In ID", "Password", and "Token Number". A "Remember my Sign In ID" checkbox is present, along with "Sign In" and "First Time Sign In?" buttons. A sidebar on the left contains "How Can We Help?" and "RBC Express Highlights" sections. A promotional banner for "Cheque-Pro" is located at the bottom center, and a "RBC Commercial Cards Program" advertisement is on the right. The overall design mimics the official RBC 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.

# Spoof Text


RBC suspended your services for security maintenance.  
Please activate your account below.  
<http://rbc.com.verify-banks.com/?activate>

# Compromised Email Account

Re: Re: Meeting

Eric [redacted]  
To: Larry Keating <lkeating@[redacted]>

[If there are problems with how this message is displayed, click here to view it in a web browser.](#)

 [redacted].zip  
41 KB

Please see the attached document.

zip pass 333

Thx  
Eric [redacted]

---

**From:** Eric [redacted]  
**Sent:** Thu, 22 Aug 2019 17:36:14 +0000  
**To:** Larry Keating <lkeating@[redacted]>  
**Subject:** Re: Meeting

Yes let u know

Sent from my BlackBerry 10 smartphone on the Bell network.

---

**From:** Larry Keating  
**Sent:** Thursday, August 22, 2019 1:30 PM  
**To:** Eric [redacted]  
**Subject:** RE: Meeting

Still working on this. Are you around next week [redacted]

Reply Reply All Forward

Tue 8/27/2019 9:17 AM

← Fake

← Real

← Real

# BEC Evolution

- BEC scams are going undetected longer for greater takes
- Attacks can include live threat actor impostors who will phone for verbal confirmations and payment intimidation
- Increased “social engineering” – using information found on the web, both corporate and personal, to aid the attack
- Most frequently enabled by an initial malware attack





**What to Do?**

# What to Do?

**Create a Culture of Awareness, Technology and Security Leadership, and Proactive Measures**

# What to Do?

## Step 1.

### Train You and Your Team

# Educate Management and Staff

- ❑ Train from the top down
- ❑ Don't click what you don't know:
  - ❑ Links or attachments in unexpected emails
  - ❑ Websites you are uncertain of
  - ❑ Unsolicited texts
- ❑ Observe error and warning messages from your computer
- ❑ Observe email addresses and content carefully
- ❑ Be careful responding to account recovery or requests to change/increase the security of your accounts

# BEC Defense Training Tips

Watch for:

- Senior executives, partners, staff with financial authority, HR, etc., asking for unusual information, more detail than usual
- A request not to discuss with others, or suddenly, and it is not the norm, a project is top-secret
- Anything that bypasses normal channels or processes
- A rush requirement

# BEC Defense Training Tips

Watch for:

- Supplier or client change of bank account, email address, or daily contact
- Better than usual, or different, grammar or layout, unusual data formats
- “Reply To” address does not match the norm or sender

# BEC Defense Training Tips

- ❑ Establish email source and address verification processes
- ❑ Establish person to person authentication policies
- ❑ Confirm payment pattern change requests with verifiable contacts
- ❑ Do not provide personal information when answering an email, unsolicited phone call, text message or instant message, even payroll change requests and confirmations

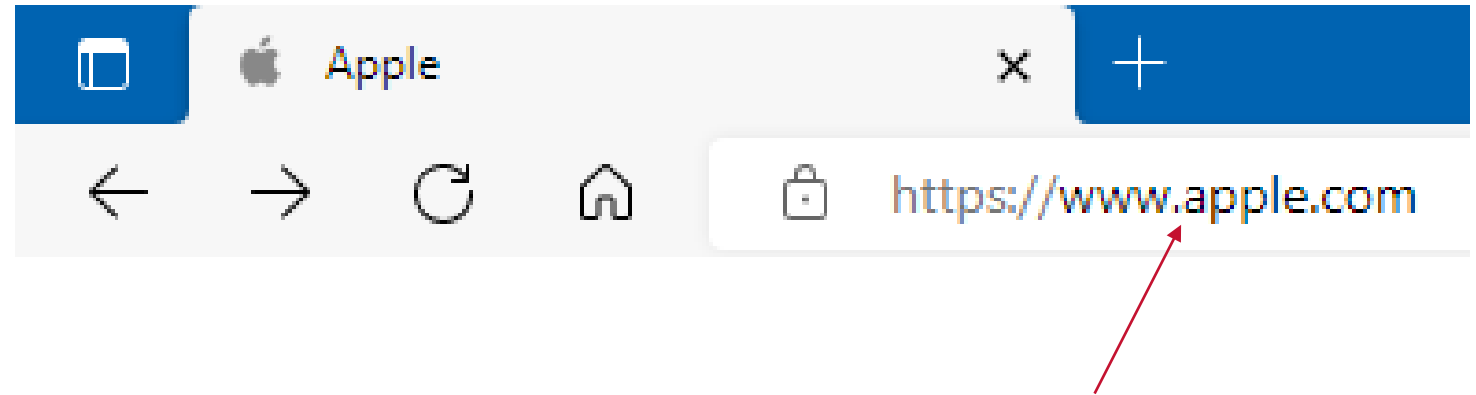
# What to Do?

## Step 2.

**Keep the Bad Guys Out of Your Systems,  
Especially Email**



# 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

# 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.

# Attack Email Cleaned

The screenshot shows a Microsoft Outlook interface. The inbox on the left contains several emails, with the one from Dominic L Petrone selected. The selected email is titled "Microsoft Mail Delivery Failure" and is dated 2019-12-03. The right pane shows the details of this email, including the sender's name and profile picture, and the start of the message body which says "Hello". A red "REVIEW" banner is visible above the email content. In the foreground, an "ESet ENDPOINT SECURITY" window is open, displaying a "Threat removed" notification. The notification states that a threat (HTML/Phishing.Agent.LO) was found in a file that Microsoft Outlook tried to access, and that the file has been cleaned. The notification also includes a link to "Learn more about this message".

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**

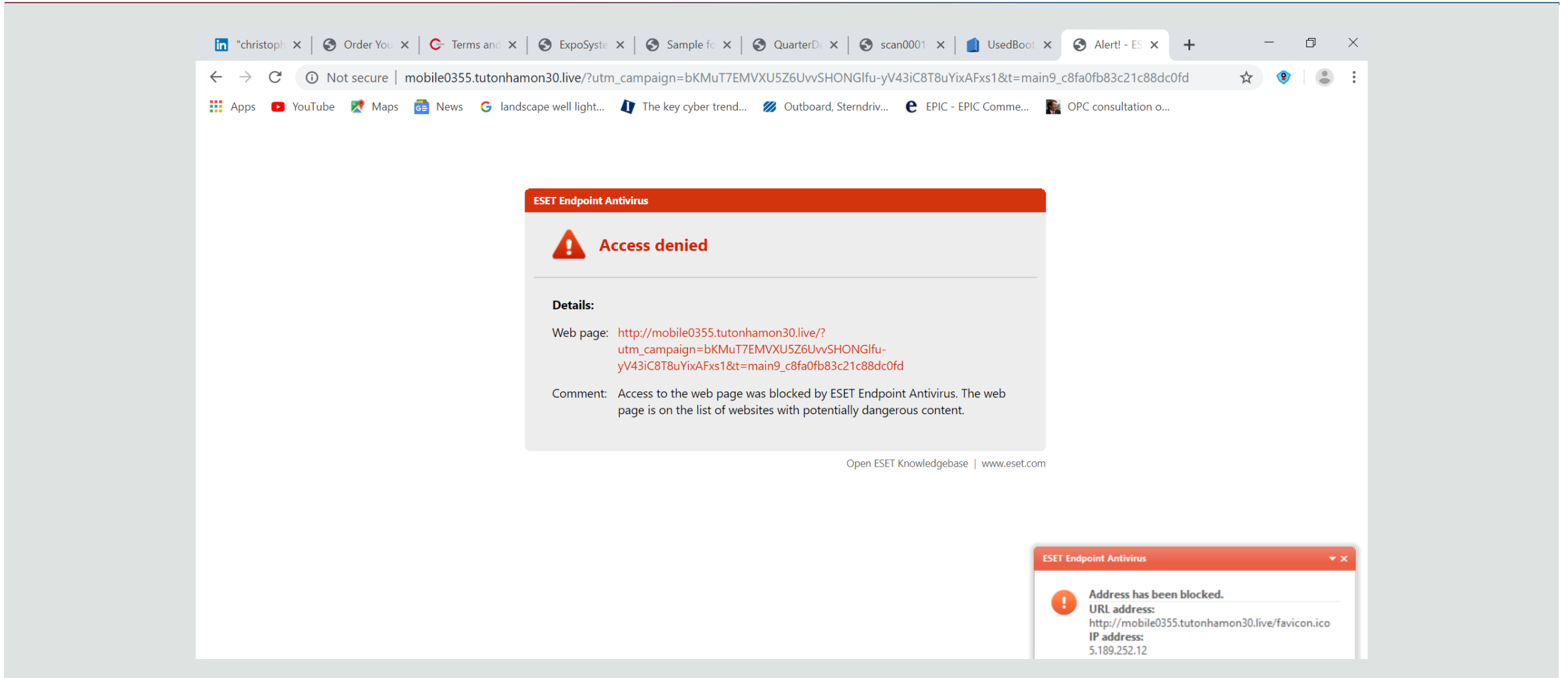
A threat (HTML/Phishing.Agent.LO) was found in a file that Microsoft Outlook tried to access.

**The file has been cleaned.**

Learn more about this message

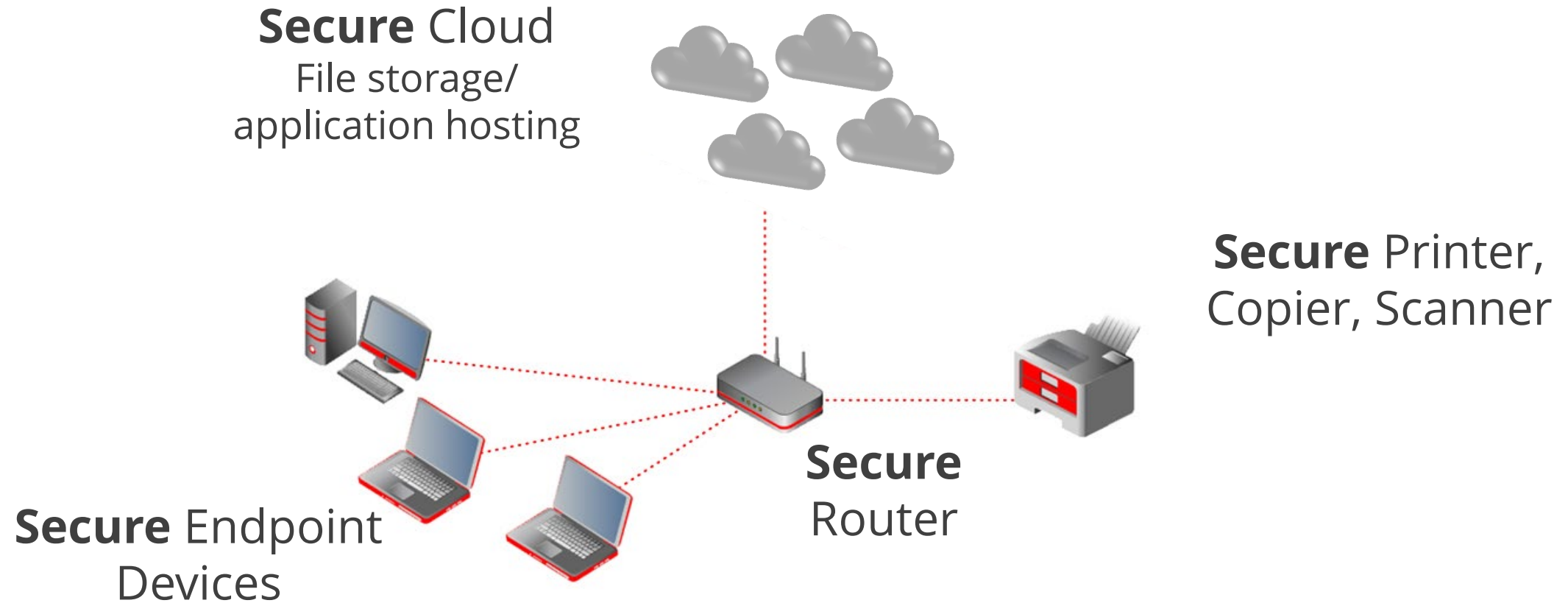
All folders are up to date. Connected to: Microsoft Exchange Display Settings 100%

# Drive-by Attack Blocked



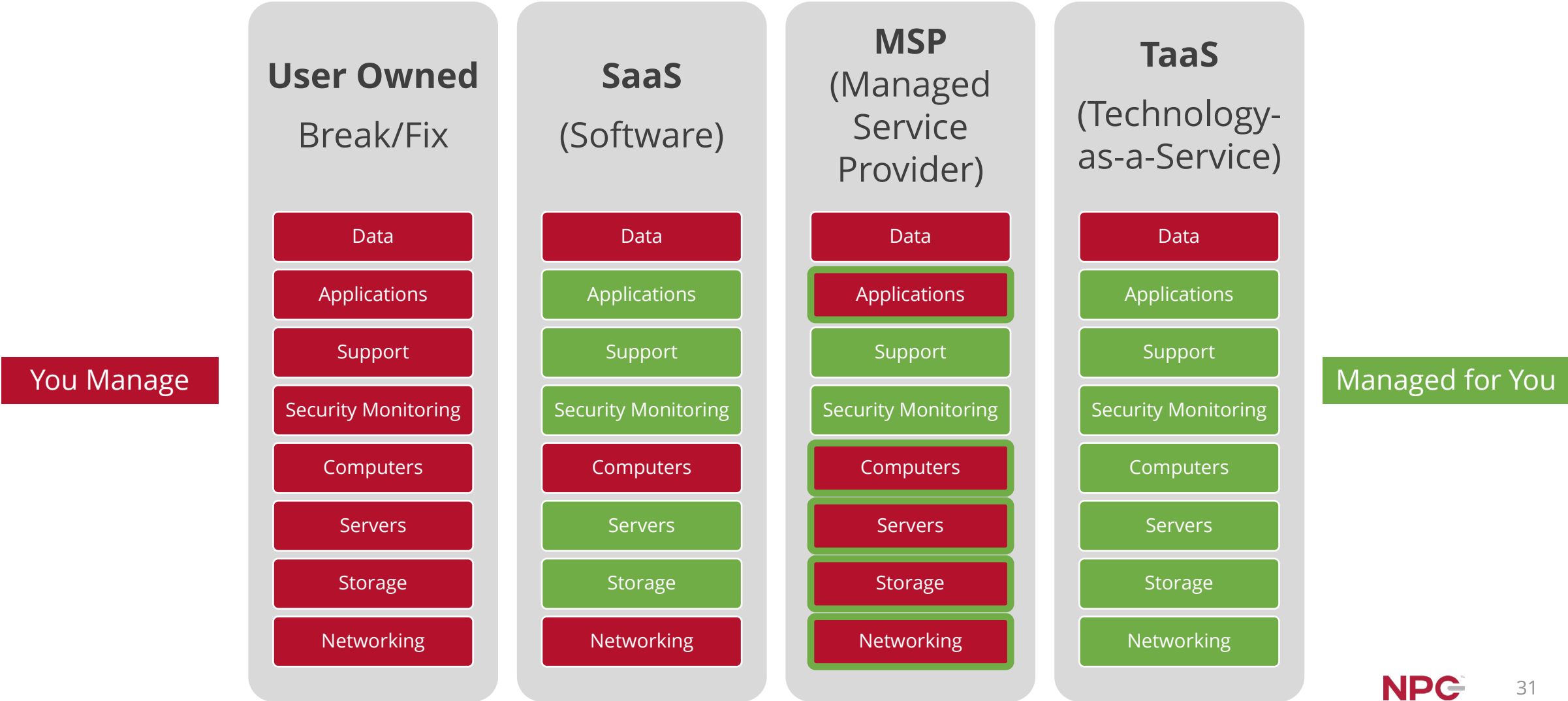
# Office of the Future

---



[Checklists](#)

# IT Delivery Models



# What's the Benefit?

---

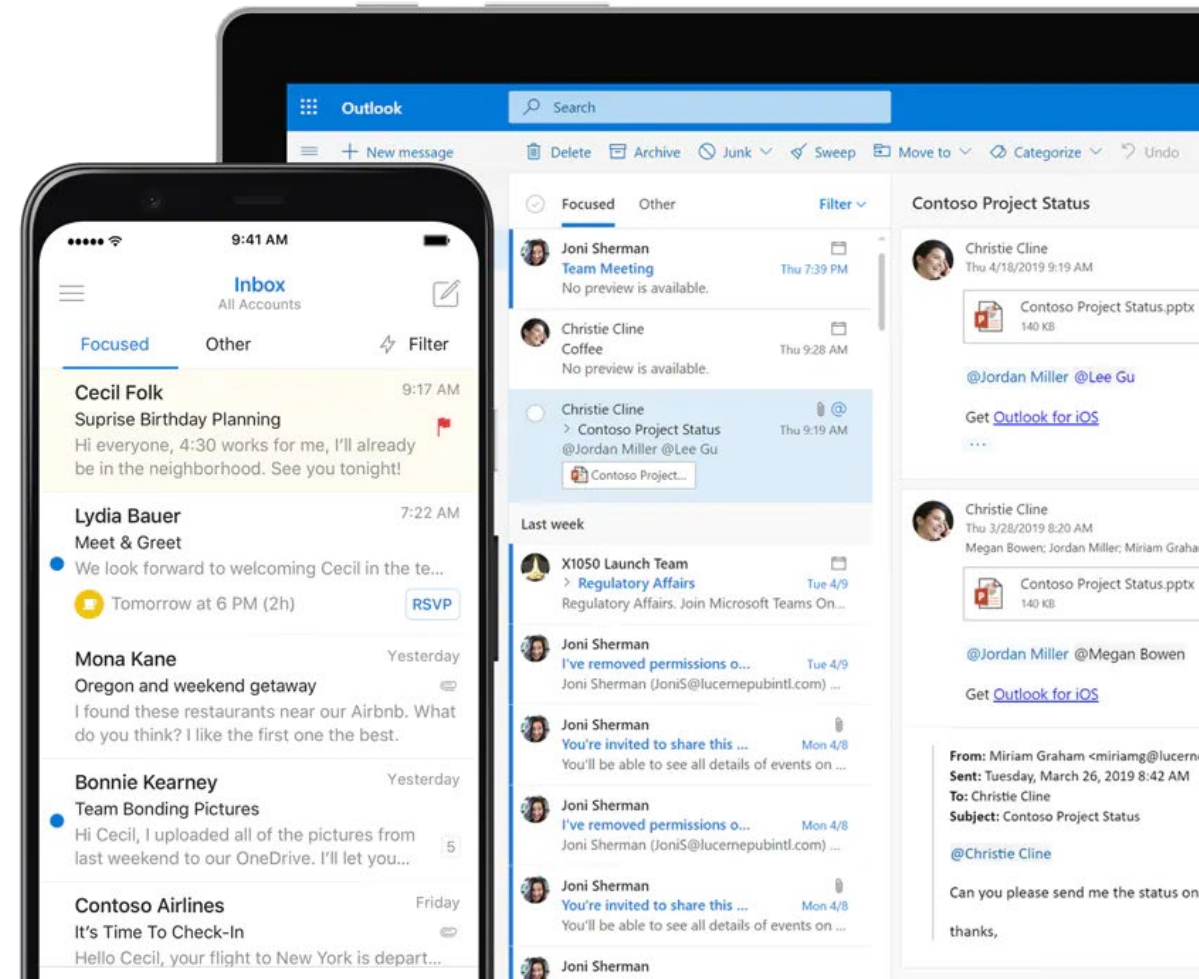
- As-a-service models remove the cost of custom-building common application, network, server, security, and services needs
- Specialization by the provider allows more features for less cost, improved performance, security, and reliability
- Allows for more economical “scaling up” or “scaling down”

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

# Secure Email and Email Management with Exchange Email



- Professional-grade email system for your team's improved performance and security
- Both in-the-cloud and integrated device access for mobility and organization
- In-Canada or U.S. data sovereignty to meet your compliance requirements
- Seamlessly integrated with Teams, SharePoint, OneDrive and your calendar
- Integrated advanced capabilities such as DLP and Email Archiving





# Microsoft 365 Business Premium Security...

---



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



Administrator account control, including user access and password policy management



Location-Based Authentication



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



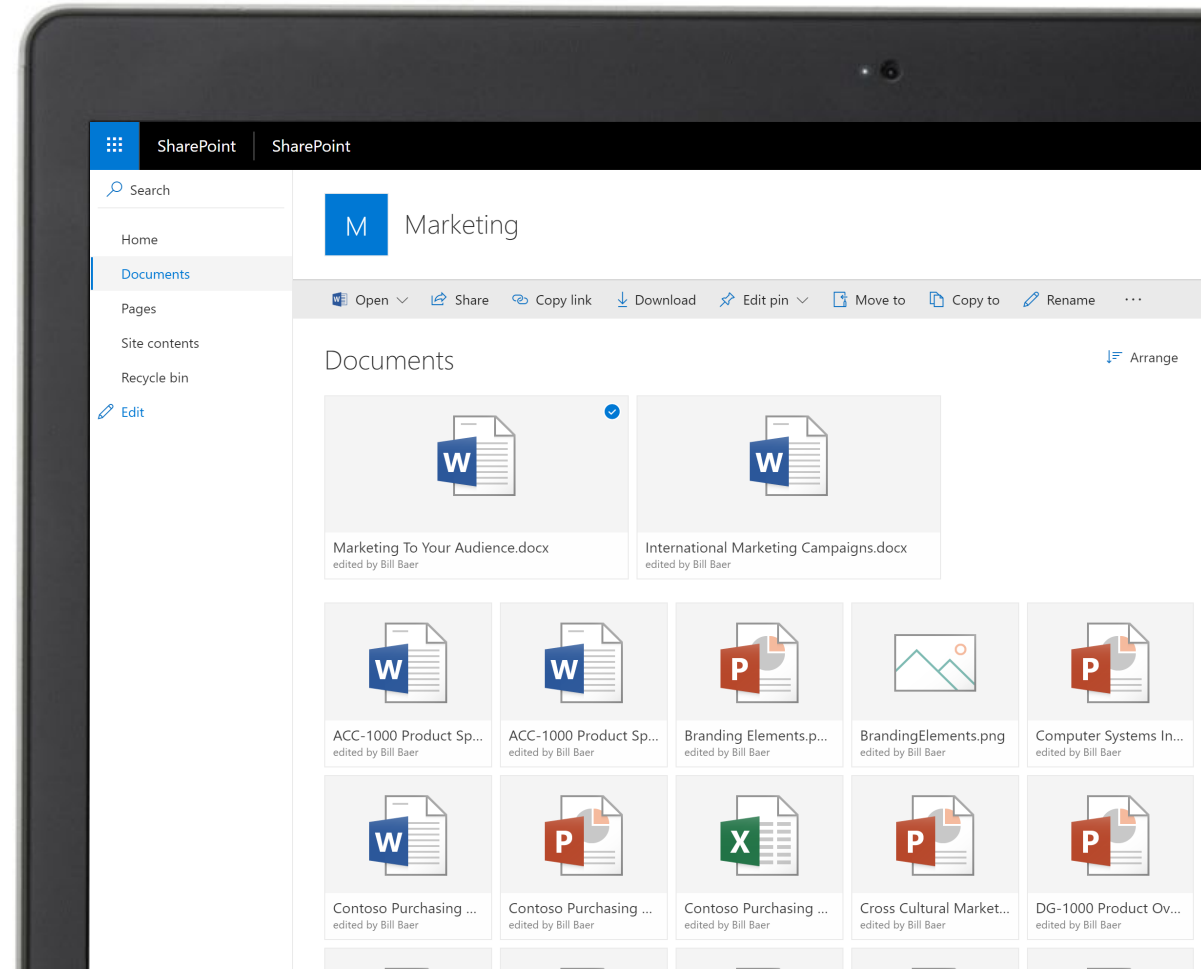
Advanced Threat Protection:

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

# Secure File Sharing Eliminates Emailing Files



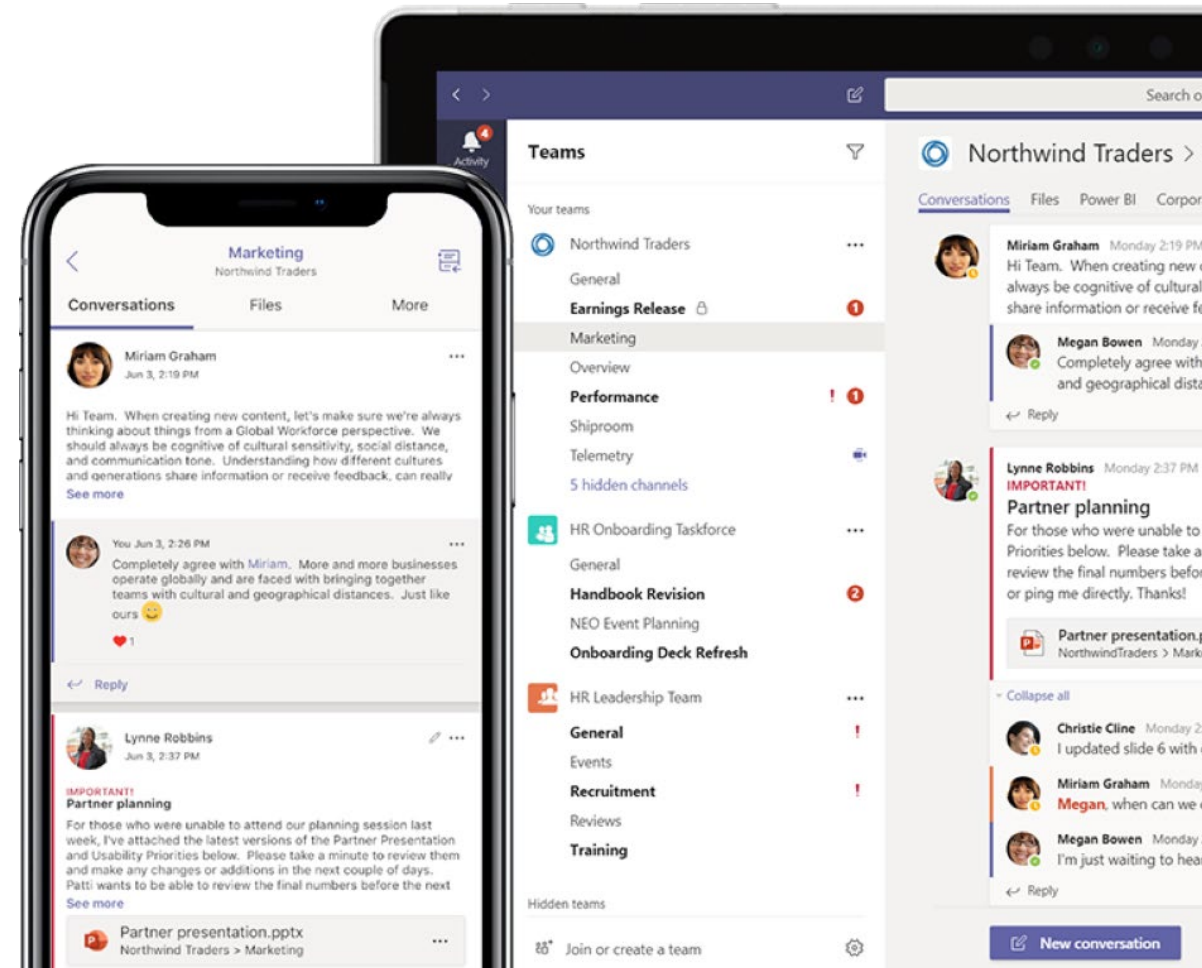
- Replaces your file server, USB drives, or email file sharing
- Mobile access everywhere
- Powerful collaboration and integrated tools and apps
- Generate links for secure file sharing, or grant controlled access
- Data sovereign



# Securely Connect People with Teams



- Everything brought together, unified communications
- Chat, video, calls, conference calls, screen sharing, set appointments, mark events, share files, create groups, call recording, guest access



# Recap

- Become cyber-threat aware; educate yourself and your team on BEC threats that can harm your business, and what to do about them
- Don't click what you don't know, treat everything you are not familiar with as suspicious
- Develop confirmation methods for transactions, do not rely on email
- Secure your computers and systems, invest in up-to-date technologies
- Eliminate sending transactions through email using secure file sharing



## Additional Resources

# Upcoming NPC Webinars



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

**October 27<sup>th</sup>**  
1:00 PM ET (30 mins)

NPC DataGuard Solutions Overview

**November 15<sup>th</sup>**  
1:00 PM ET (60 mins)

How to Prepare for the Most Common  
Cyber Threats Facing SMBs

**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

**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

**Larry Keating**

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

905-305-6501

---

**Darren Mar**

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

905-305-6513



*Thank You*

Please Be Safe & Stay Healthy



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

# Protect Endpoint Devices

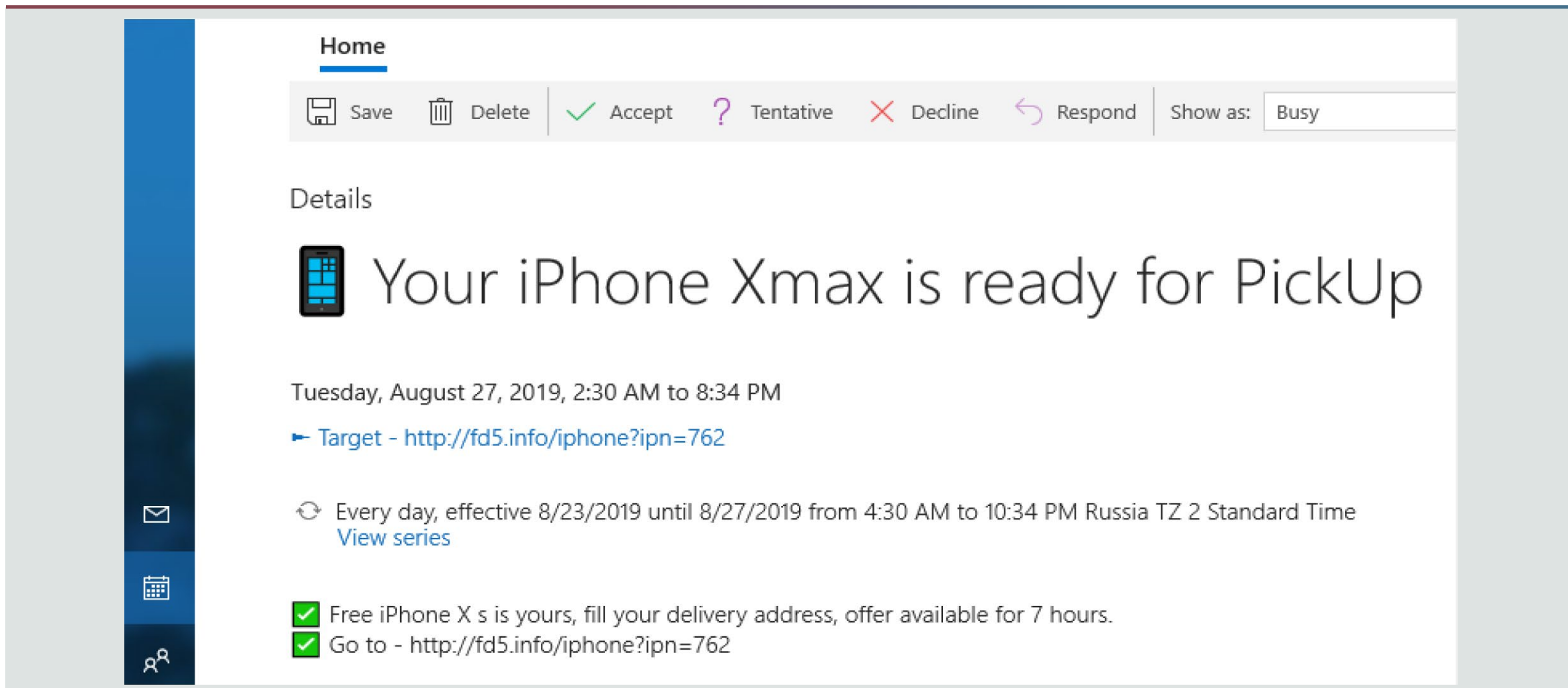
- Ensure you have up-to-date and fully patched:
  - Computer BIOS, operating system, office suite
  - System apps like Java and Adobe
  - Web browser
  - Anti-malware suite
- Encrypt your files, consider using file-by-file encryption
- Enable personal firewall on endpoint computers
- Only do your work on a secured device
- Change default passwords on all IoT devices
- Secure your WFH environment

# Protect Your Systems

---

- Use strong, unique passwords, change occasionally on computers and systems
- Apply principles of least privilege for user access, lock admin accounts
- Prohibit automatic forwarding of email to external addresses
- Add an email banner to messages coming from outside your organization
- Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- Know who and what is connecting to your network; guests, employee devices, etc.
- Conduct a risk assessment, preferably using a security professional
- Ensure you have adequate cyber insurance, and your WFH is covered

# Compromised Calendar



The screenshot shows a Microsoft Outlook calendar interface. At the top, there is a navigation bar with the word "Home" and a set of action buttons: Save, Delete, Accept, Tentative, Decline, Respond, and a "Show as:" dropdown menu set to "Busy". Below this is a "Details" section for a calendar event. The event title is "Your iPhone Xmax is ready for PickUp" with a small iPhone icon to the left. The event time is "Tuesday, August 27, 2019, 2:30 AM to 8:34 PM". The location is "Target - <http://fd5.info/iphone?ipn=762>". The recurrence is "Every day, effective 8/23/2019 until 8/27/2019 from 4:30 AM to 10:34 PM Russia TZ 2 Standard Time" with a "View series" link. At the bottom, there are two checklist items, both marked with green checkmarks: "Free iPhone X s is yours, fill your delivery address, offer available for 7 hours." and "Go to - <http://fd5.info/iphone?ipn=762>". On the left side of the interface, there is a vertical navigation bar with icons for Mail, Calendar, and People.

# Calendar Defense

- Delete the invitation email without opening it — hover over it, right click, delete
- Do not click on the calendar appointment, any links, or attachments. This includes not clicking “Decline”
- Consider changing your calendar options to restrict what your email client will automatically place or show in your calendar

# 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.

[Back](#)

