Microsoft

How Enterprise Tackles Phishing

Nelson Yuen

Technology Manager, Cybersecurity

Microsoft Hong Kong

Hackers turning to easy marks - Social engineering

Phishing was the #1 threat vector (> 50%) for Office 365-based threats.

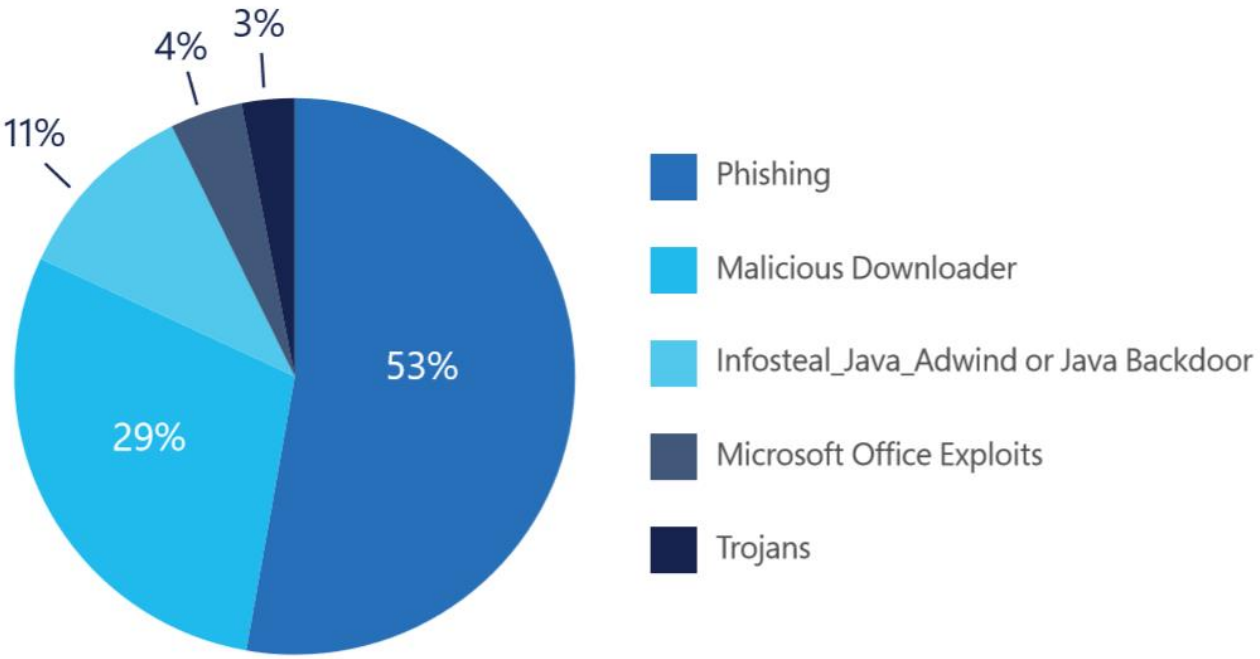
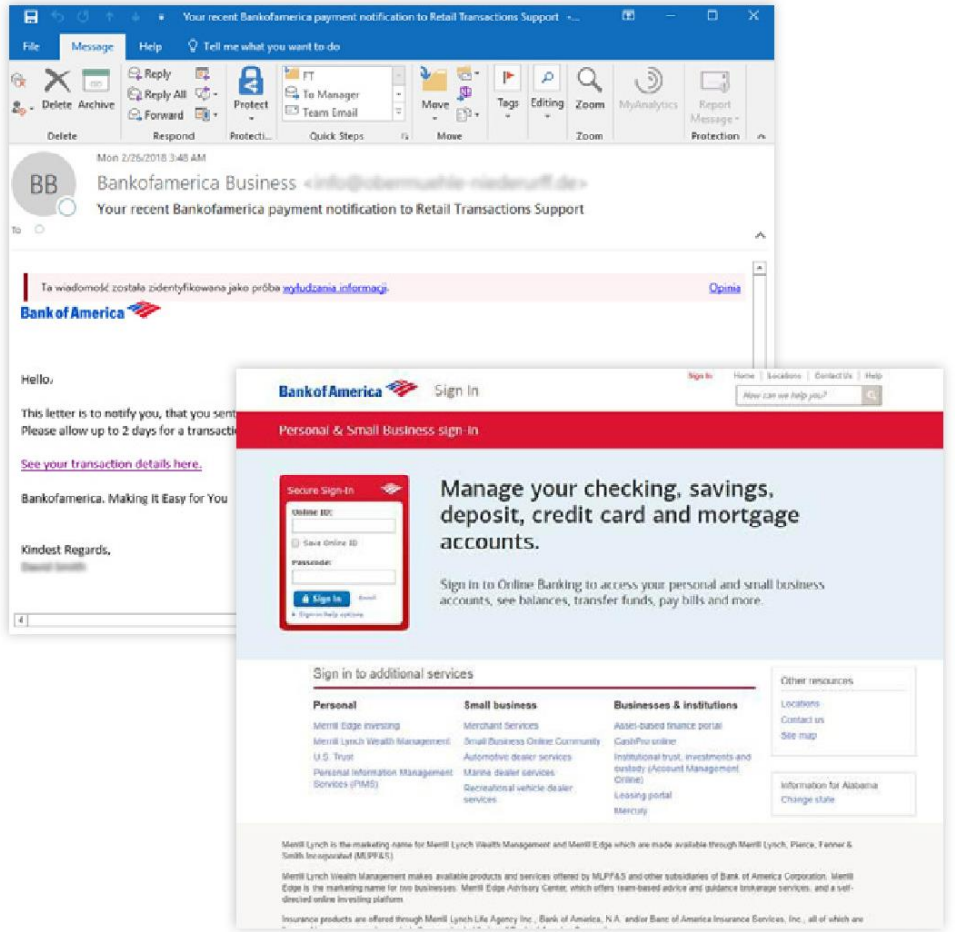


Figure 7: Top threats detected by Microsoft Office 365 ATP

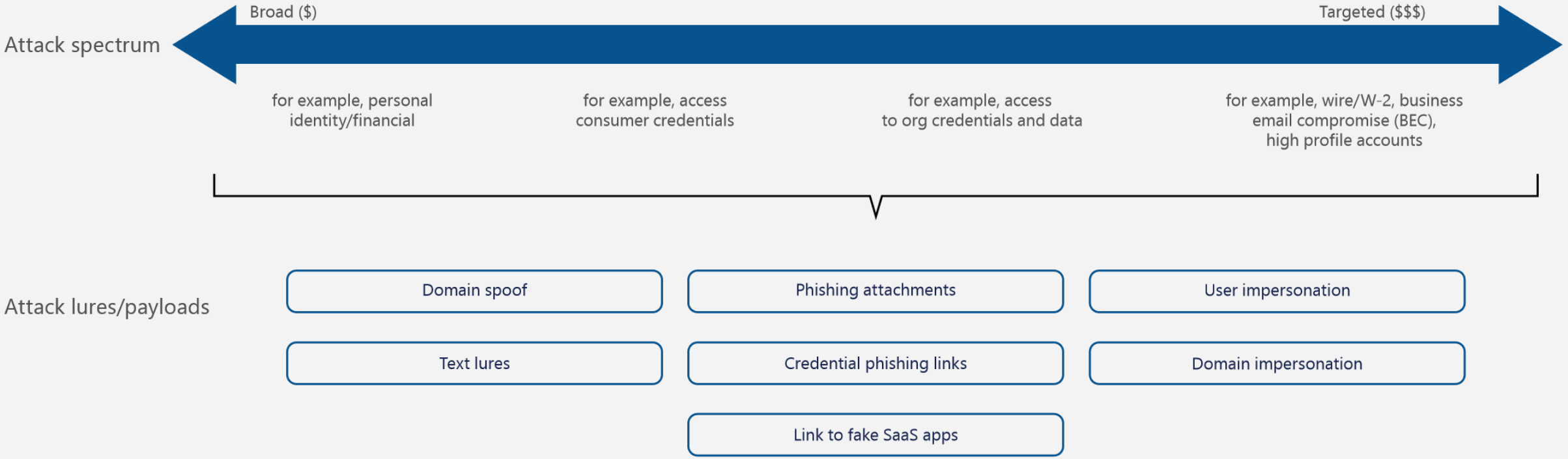
Analysis and explanation

- An attacker sending a phishing email in bulk to 1,000 individuals just needs to successfully trick one person to obtain access to that person's credentials.
- If users are distracted and quickly scan the seemingly legitimate but fake phishing email, they may accidentally click a link and share details such as entering their credentials.
- Phishing is an easier way to obtain credentials as compared to exploiting a vulnerability, which is increasingly costly and difficult.



Phishing comes in many forms

Phishing attack landscape



Phishing in real life

What you see

Are you at your desk

What the machine sees

Areeyoueatyouredesk

Key phishing related findings

- The research team has seen about 30% of domain spoof attacks.
- More than 75% of phishing mails include malicious URLs to phishing sites. Other variations include malicious phishing attachments and links in attachments.
- Phishing mails impersonate popular brands:
    - Microsoft associated brands (for example, Office 365)
    - Other commonly abused brands include, but are not limited to, DocuSign, Dropbox, Apple, and Amazon.
    - Recent investigations show attacks that impersonate popular courier services such as FedEx, DHL, and UPS.
    - The research team also detected impersonation related to banks and government services.
- User impersonation and domain impersonation techniques were low in volume, but they were high-severity attacks.

Low-hanging fruit keeps changing

Downward trend of exploitation, the exploitation of macros was very prevalent.

Most vendors have since been offering more enhanced and effective email sandboxing technology to detect and defend against **macro-based malware** threats. As a result, when macro-based attacks became unsuccessful, adversaries **turned to exploitation of PDFs**.

Vendors improved detection of **PDF based exploits** over time, and attackers moved toward **phishing-based attacks**.

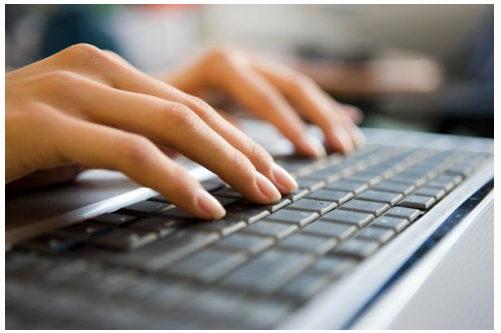
Other low-hanging fruit for attackers are **poorly secured cloud apps**.
79% of SaaS storage apps and 86% of SaaS collaboration apps **do not encrypt data both at rest and in transit**.

Learn to spot a phishing email

- **Spelling and bad grammar**. Cybercriminals are not known for their grammar and spelling.
- **Suspicious links**. If you suspect that an email message is a scam, do not open any links that you see. Instead, rest your mouse but **don't click- on the link to see if the address mismatches** the link that was typed in the message.

- **Threats**. These types of emails cause a **sense of panic** to get you to **respond quickly**. For example, it may include a statement like "You must respond by end of day." Or saying that you might face **financial penalties** if you don't respond.
- **Spoofing**. Spoofing emails appear to be connected to legitimate websites or companies, but actually take you to phony **scam sites or display legitimate-looking** pop-up windows.
- **Altered web addresses**. A form of spoofing where web addresses that closely resemble the names of well-known companies, but are **slightly altered**; for example, **www.micorsoft.com** or **www.mircosoft.com**.
- **Incorrect salutation of your name**.
- **Mismatches**. The link text and the URL are different from one another; or the sender's name, signature, and URL are different.
- **BCC**. The mail is sent to multiple recipients or to you in BCC.

Protect yourself from phishing



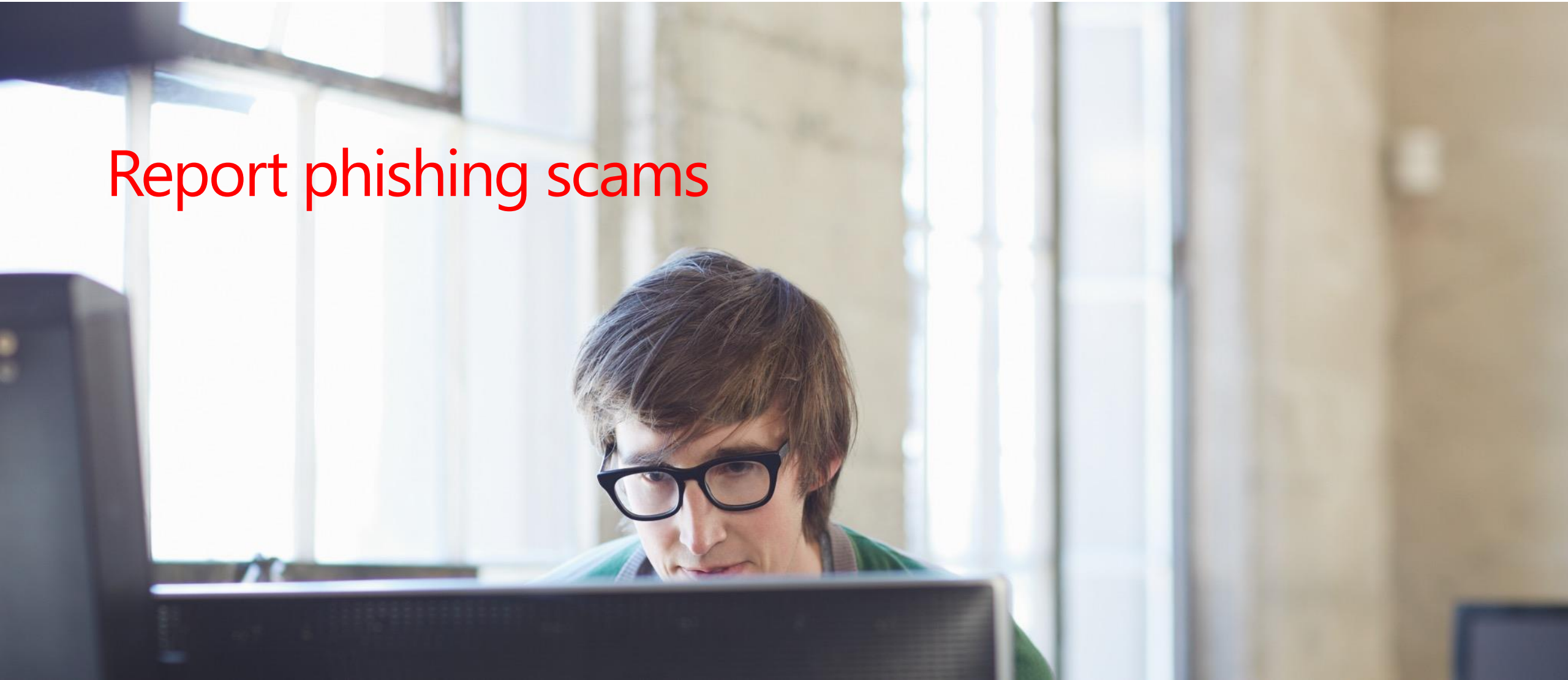
Do your own typing. If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself.

Make the call if you're not sure. Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.

Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

Microsoft

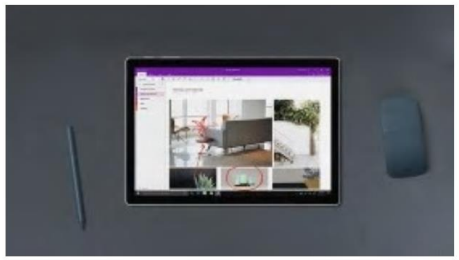
Report phishing scams



Microsoft – 官方網頁

https://www.microsoft.com/zh-hk

Microsoft Office Windows Surface Xbox 支援 All Microsoft 登入



Surface Pro

Surface Go

Xbox One S

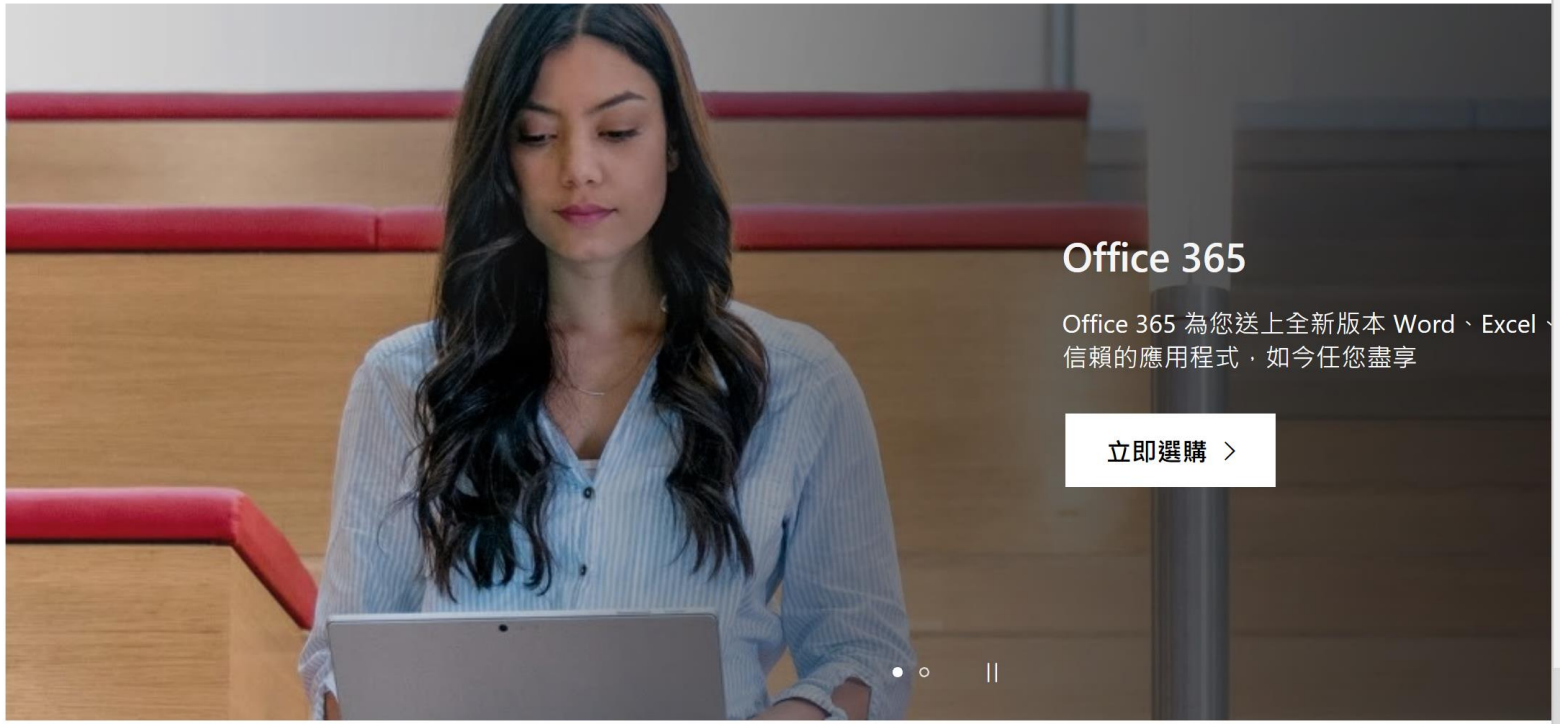
Windows 10 更新

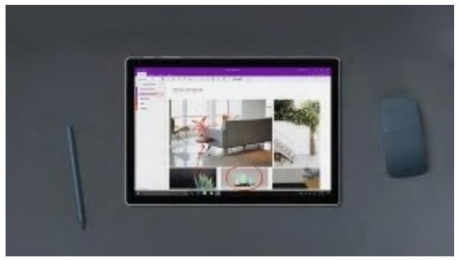
ENG 10:42 AM

Microsoft – 官方網頁

https://www.microsoft.com/zh-hk

Microsoft Office Windows Surface Xbox 支援 All M





Surface Pro

Surface Go

Xbox One S

Windows 10 更新

- New window
- New InPrivate window
- Zoom — 94% + ⤢
- Favorites
- Cast media to device
- Find on page
- Read aloud
- Print
- Pin this page to the taskbar
- Pin this page to Start
- Developer Tools
- Open with Internet Explorer
- Send feedback
- Extensions
- What's new and tips
- Settings

ENG 10:42 AM

Microsoft – 官方網頁

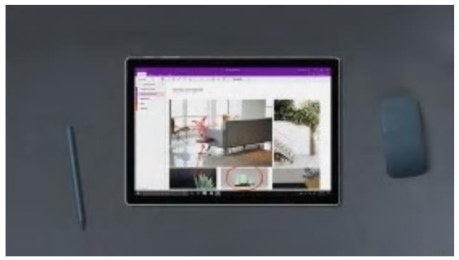
https://www.microsoft.com/zh-hk

Microsoft Office Windows Surface Xbox 支援

Surface Laptop

高效型格

立即選購 >



Surface Pro

Surface Go

Xbox One S

Feedback & reporting

Tell us what's going on

Website problems

The site or parts of the site are broken, don't look right, or are slow to load.

Report site issue

Unsafe website

The site contains threats, like malicious software, or is impersonating another site to steal your personal info.

Report unsafe site

Microsoft Edge problems or suggestions

Problems with Microsoft Edge browser features or suggestions to make them better.

Open Feedback Hub

Rate Microsoft Edge

Take a minute to rate and review this app. To send us more detailed feedback, use the Feedback Hub.

Rate it

We'll send the URL of this site to Microsoft.

ENG 10:43 AM

Feedback

https://feedback.smartscreen.microsoft.com/feedback.aspx

Microsoft

Report a website

Resources

Windows Defender SmartScreen FAQ

Website you are reporting:

https://tw.answers.yahoo.com/question/index?qid=20180910185937AAO6NA9

- [x] **I think this is a phishing website**
  Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information. This information is often used for identity theft.
- [ ] **I think this website contains malicious software**
  Malicious software or malware is software which is deceptive about functionality and is a security risk or privacy risk. The term malicious software or malware refers to programs that demonstrate illegal, viral, fraudulent, or malicious behavior. For example, viruses, worms, and Trojan horses are malicious software.

Language used on the website:

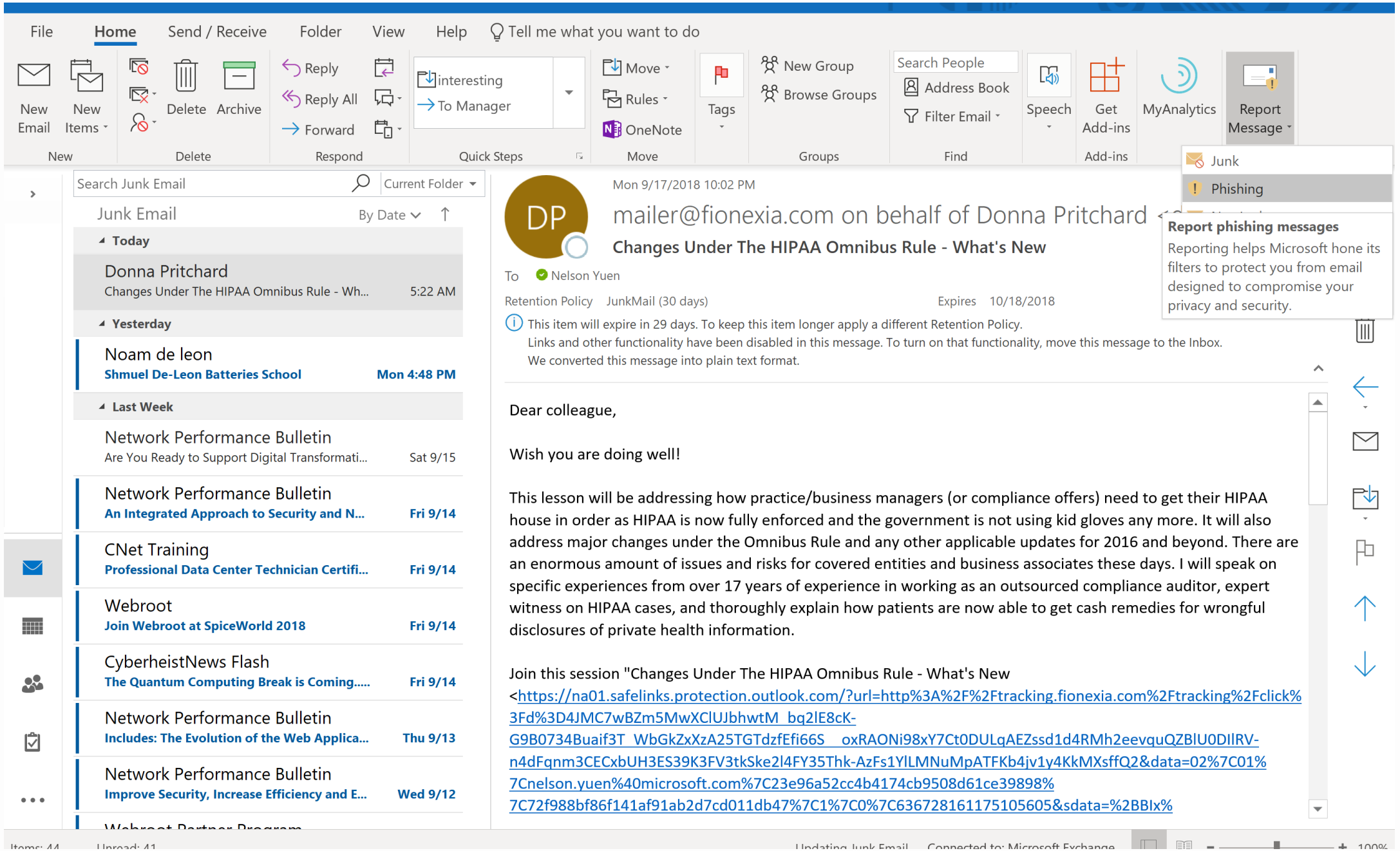
Chinese (Traditional)

Enter the characters you see

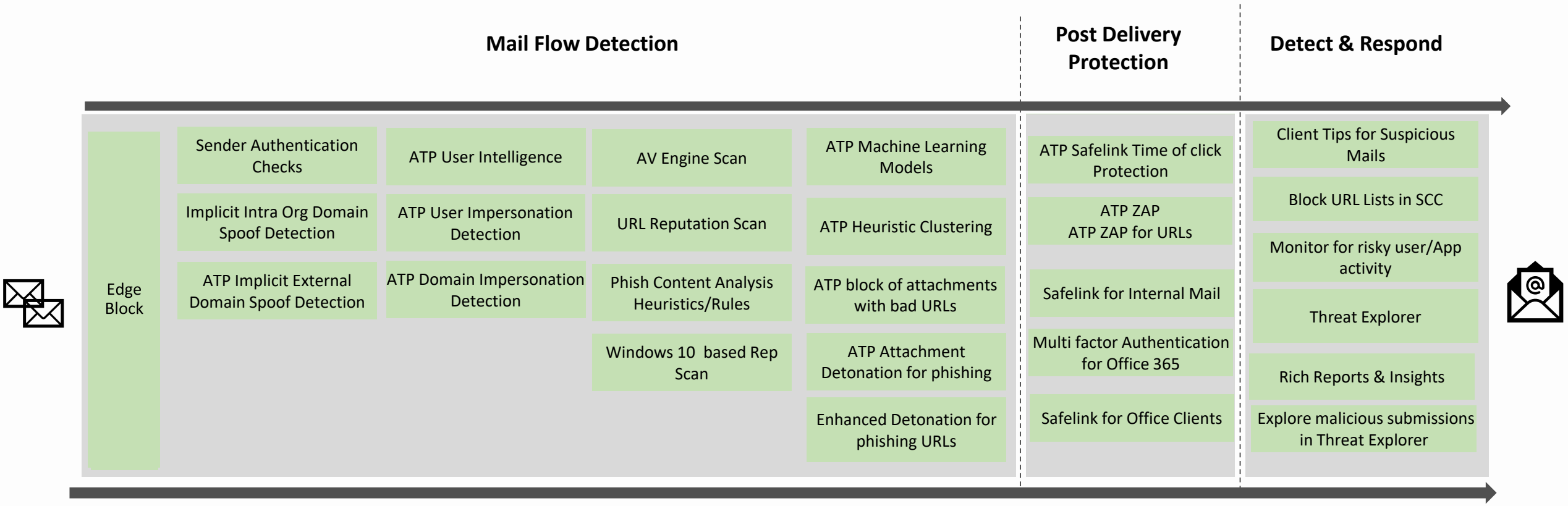
New | Audio

Submit

ENG 10:44 AM

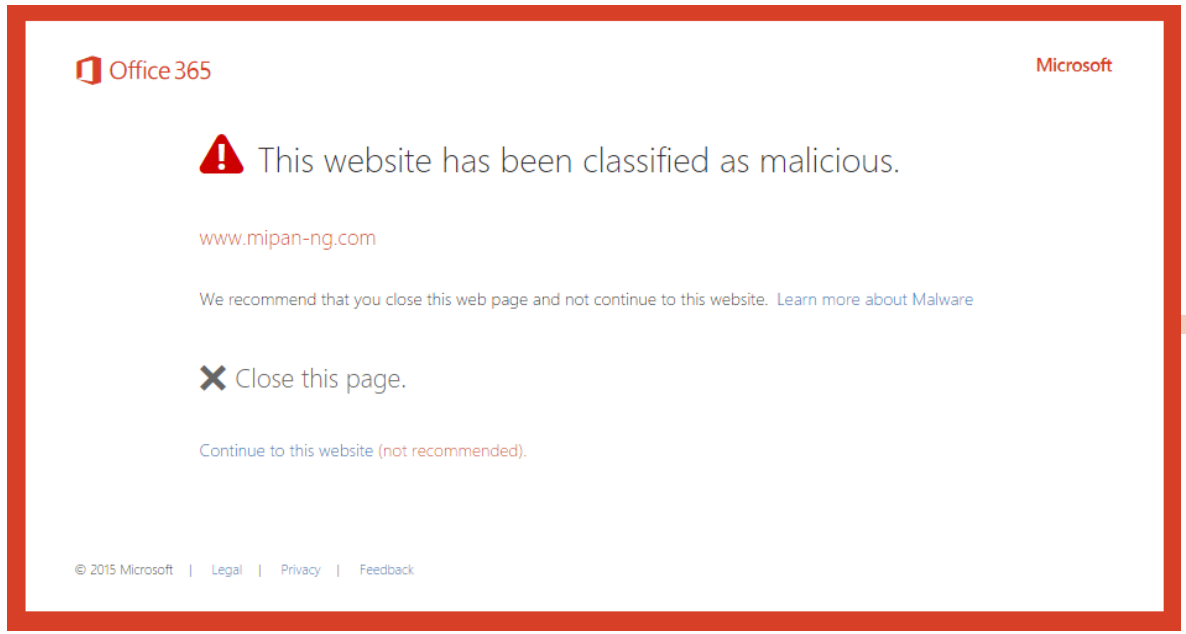

File
Home
Send / Receive
Folder
View
Help
Tell me what you want to do
New Email
New Items
Delete
Archive
Reply
Reply All
Forward
interesting
To Manager
Move
Rules
OneNote
Tags
New Group
Browse Groups
Search People
Address Book
Filter Email
Speech
Get Add-ins
MyAnalytics
Report Message
New
Delete
Respond
Quick Steps
Move
Groups
Find
Add-ins
Junk
Phishing
Report phishing messages
Reporting helps Microsoft hone its filters to protect you from email designed to compromise your privacy and security.
Search Junk Email
Current Folder
Junk Email
By Date
Today
Donna Pritchard
Changes Under The HIPAA Omnibus Rule - Wh...
5:22 AM
Yesterday
Noam de leon
Shmuel De-Leon Batteries School
Mon 4:48 PM
Last Week
Network Performance Bulletin
Are You Ready to Support Digital Transformati...
Sat 9/15
Network Performance Bulletin
An Integrated Approach to Security and N...
Fri 9/14
CNet Training
Professional Data Center Technician Certifi...
Fri 9/14
Webroot
Join Webroot at SpiceWorld 2018
Fri 9/14
CyberheistNews Flash
The Quantum Computing Break is Coming.....
Fri 9/14
Network Performance Bulletin
Includes: The Evolution of the Web Applica...
Thu 9/13
Network Performance Bulletin
Improve Security, Increase Efficiency and E...
Wed 9/12
DP
Mon 9/17/2018 10:02 PM
mailer@fionexia.com on behalf of Donna Pritchard
Changes Under The HIPAA Omnibus Rule - What's New
To
Nelson Yuen
Retention Policy
JunkMail (30 days)
Expires
10/18/2018
This item will expire in 29 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We converted this message into plain text format.
Dear colleague,
Wish you are doing well!
This lesson will be addressing how practice/business managers (or compliance offers) need to get their HIPAA house in order as HIPAA is now fully enforced and the government is not using kid gloves any more. It will also address major changes under the Omnibus Rule and any other applicable updates for 2016 and beyond. There are an enormous amount of issues and risks for covered entities and business associates these days. I will speak on specific experiences from over 17 years of experience in working as an outsourced compliance auditor, expert witness on HIPAA cases, and thoroughly explain how patients are now able to get cash remedies for wrongful disclosures of private health information.
Join this session "Changes Under The HIPAA Omnibus Rule - What's New
<https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Ftracking.fionexia.com%2Ftracking%2Fclick%3Fd%3D4JMC7wBZm5MwXClUJbhwtM_bq2lE8cK-G9B0734Buaif3T_WbGkZxXzA25TGTdzfEfi66S__oxRAONi98xY7Ct0DULqAEZssd1d4RMh2eevquQZBlU0DIlRV-n4dFqnm3CECxbUH3ES39K3FV3tkSke2l4FY35Thk-AzFs1YlLMNuMpATFKb4jv1y4KkMXsffQ2&data=02%7C01%7Cnelson.yuen%40microsoft.com%7C23e96a52cc4b4174cb9508d61ce39898%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636728161175105605&sdata=%2BBIx%

Microsoft Exchange Online Anti-Phishing Protection Stack



Protect your data

- Advanced threat protection: Time of click protection for malicious links



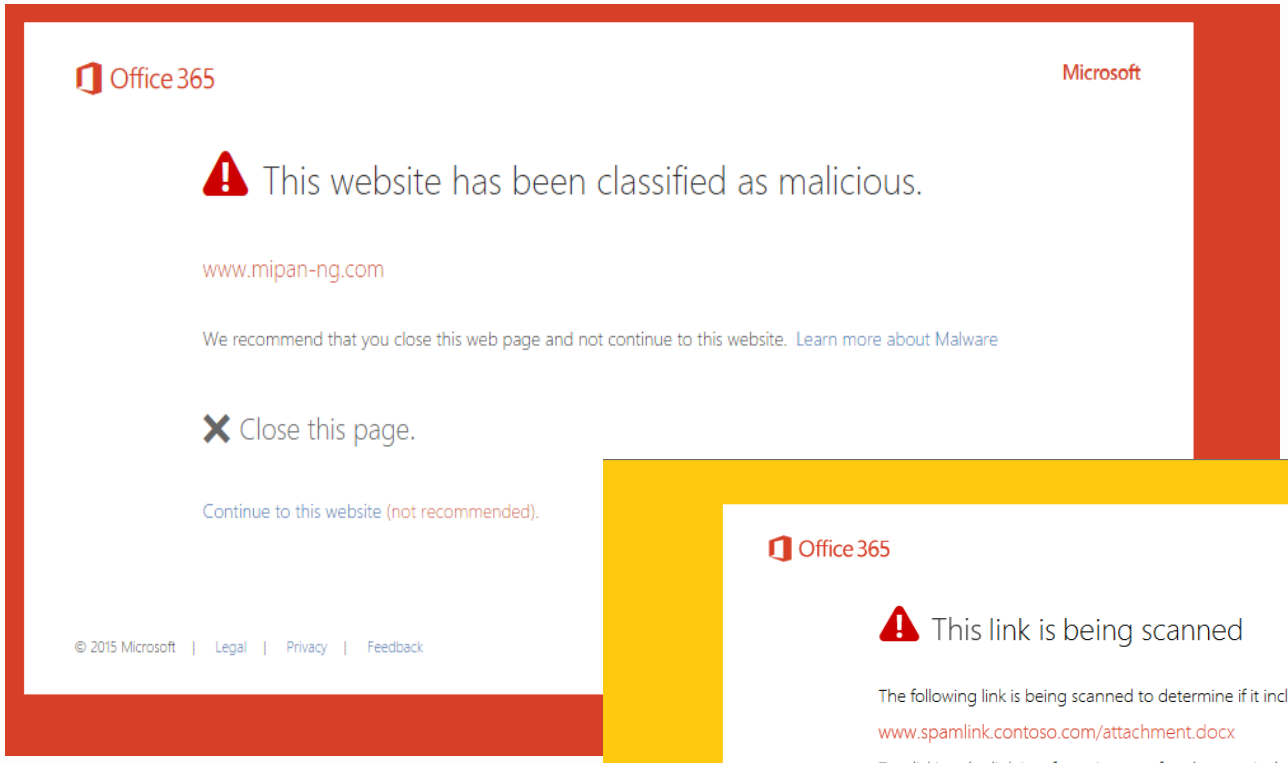
Rewriting URLs to redirect to a web server.

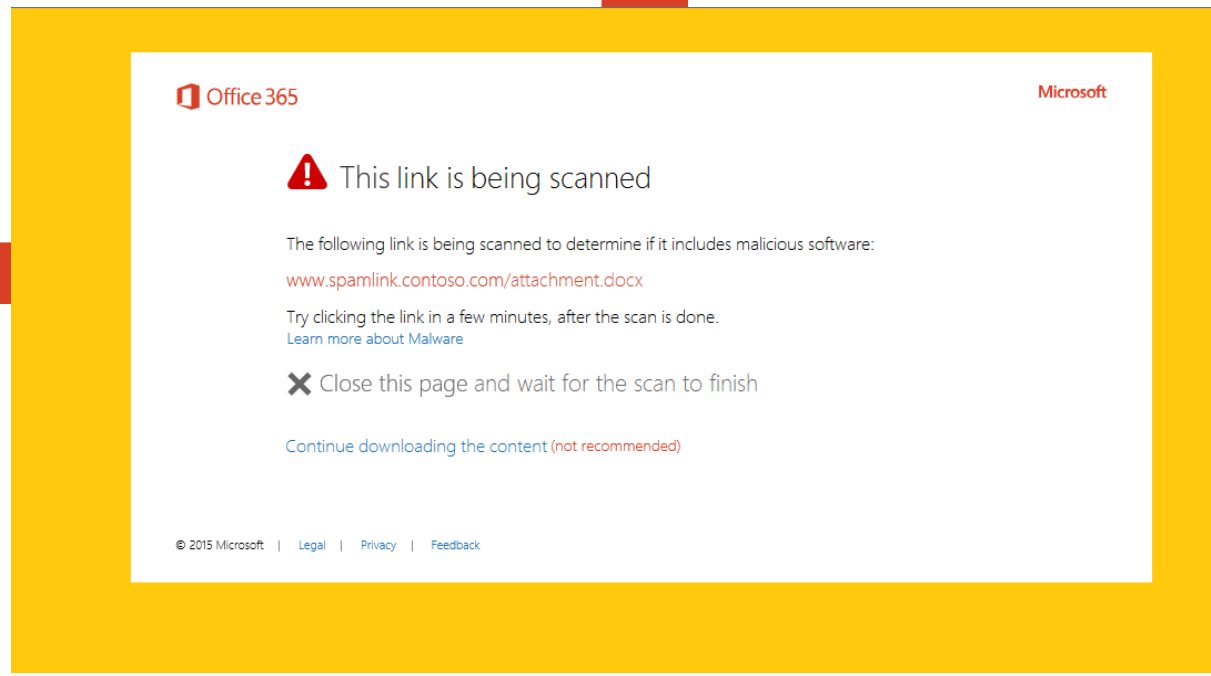
User clicking URL is taken to EOP web servers for the latest check at the "time-of-click"

Web servers perform latest URL reputation check

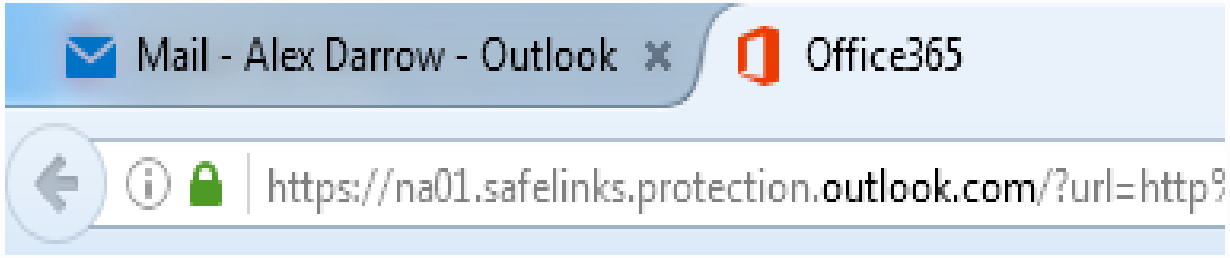
Safe links – users messages

Users notified if a malicious link is clicked in email



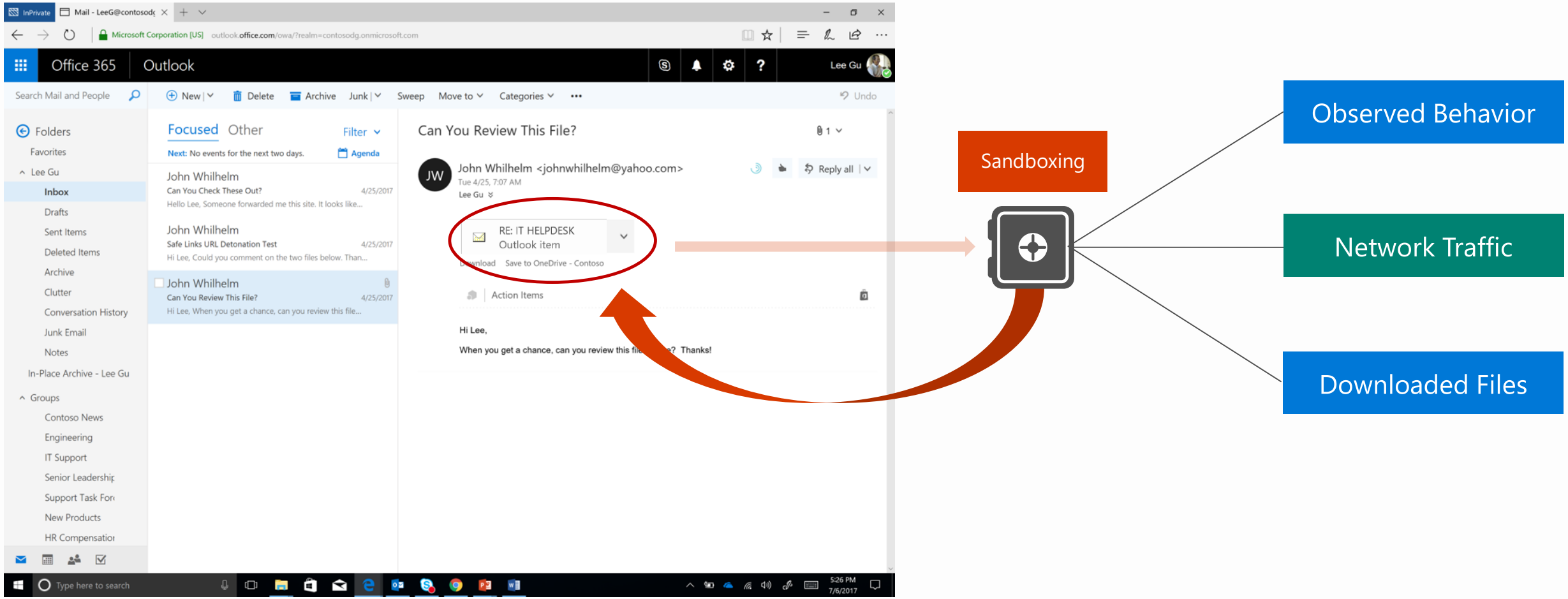


Url rewritten to web server for check against list of malicious Urls



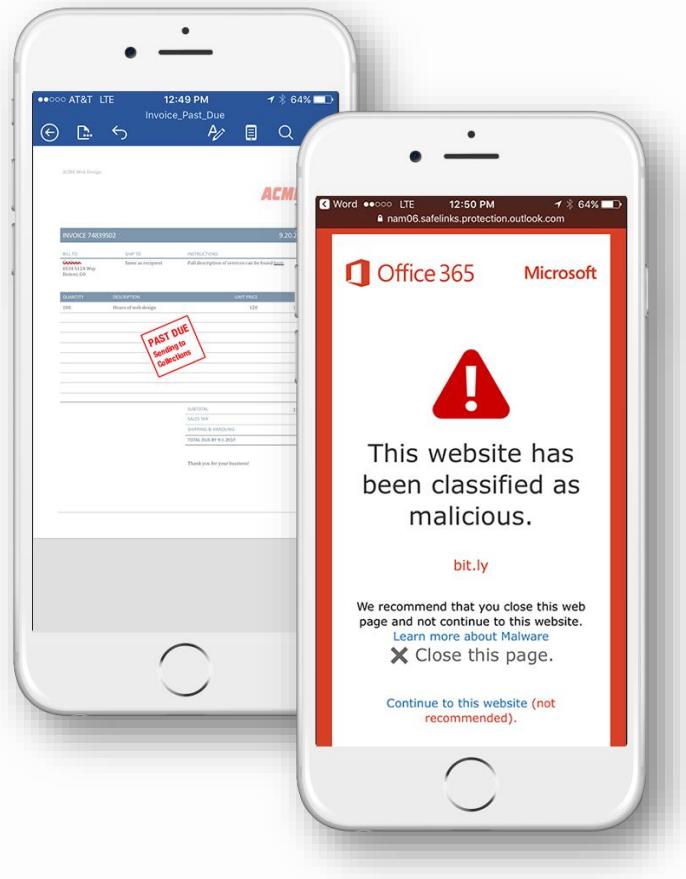
Protect your data

- **Advanced threat protection:** Sandboxing technology for malicious attachments



Protect – Post Delivery

- ✓ **Safe links provides Time of click protection**
  - ✓ Client Agnostic
  - ✓ Location agnostic
  - ✓ Tenant level block list
  - ✓ Detonation
- ✓ **Integrated directly into Office clients**
- ✓ **Zero hour Auto purge (ZAP) Files/URLs (New)**
  - ✓ High Confidence URL lists
  - ✓ Doesn't matter if the message was read or moved
  - ✓ Moves complete message to Junk



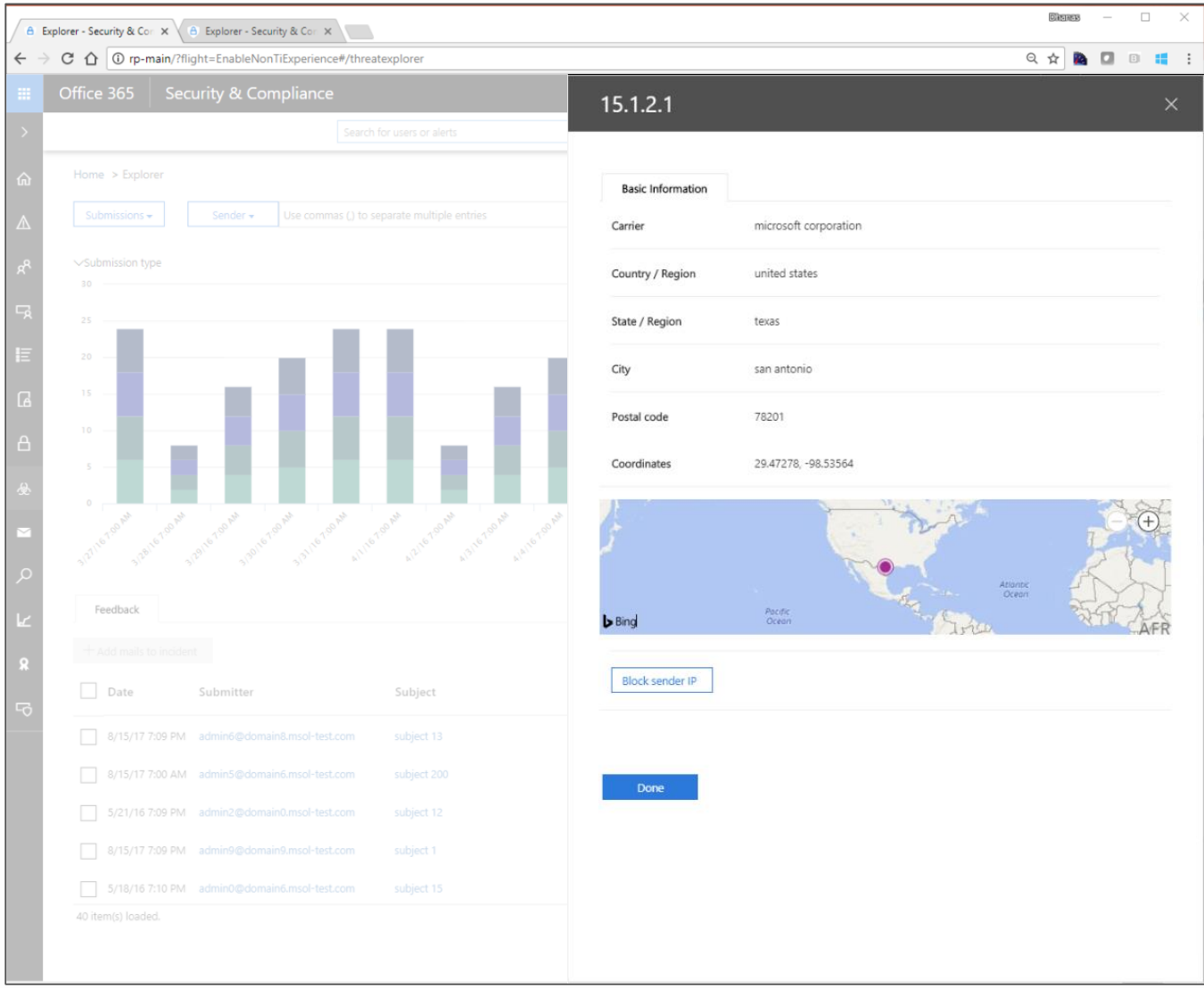
Zero-Hour Auto-purge

Safe Links for Office Clients

Safe Links

Detect & Respond: User Submissions/Real time Reports

- ✓ View of what users are reporting
  - ✓ Phish and Spam
- ✓ Benefits
  - ✓ ML Models use this data
  - ✓ Analysts cluster on missed phish
  - ✓ Highlight configuration issues related to submissions
- ✓ Realtime reports
  - ✓ Phishing including spoof and impersonation
  - ✓ Details of messages with rich search



Educating users through attack simulation