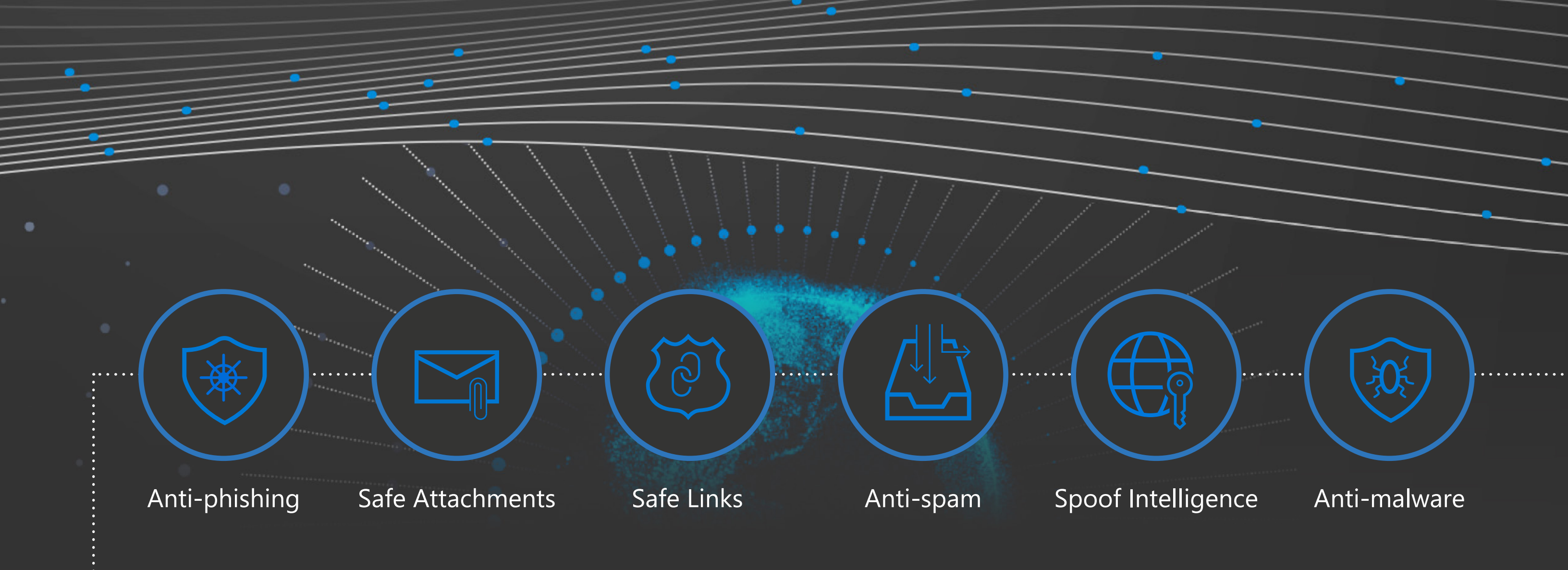
Advanced Threat Protection in Office 365



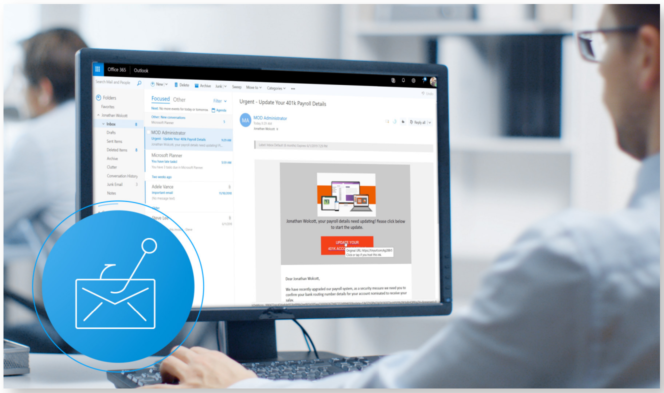
Catch threats before they disrupt your organization, keeping your data, intellectual property and users safe from email phishing attacks and zero-day malware.

Email: a trojan horse for cyber-attacks

We all use email. It's one of the most pervasive and powerful forms of communication and collaboration, but it's also the most prolific attack vector that we see today. Emails often serve as a trojan horse for attackers to target and compromise your users by "phishing" their credentials.

Some phishing attacks can be blatant as in the case of ransomware; others can remain undiscovered allowing assailants to silently move laterally within your network to breach your data and potentially steal intellectual property.

Phishing is a primary vehicle for malicious Ransomware code



Phishing email designed to steal user credentials

Industry leading threat detection

Keeping up to date with the threat landscape can be nearly impossible as the increasing sophistication of rapidly evolving unknown threats, can quickly outdate the protections that you may have put in place. At the core of preventing any malicious attack is how quickly we can detect malicious activity. To help you to stay ahead of the threat landscape, Microsoft invests at least a billion dollars in this area annually.

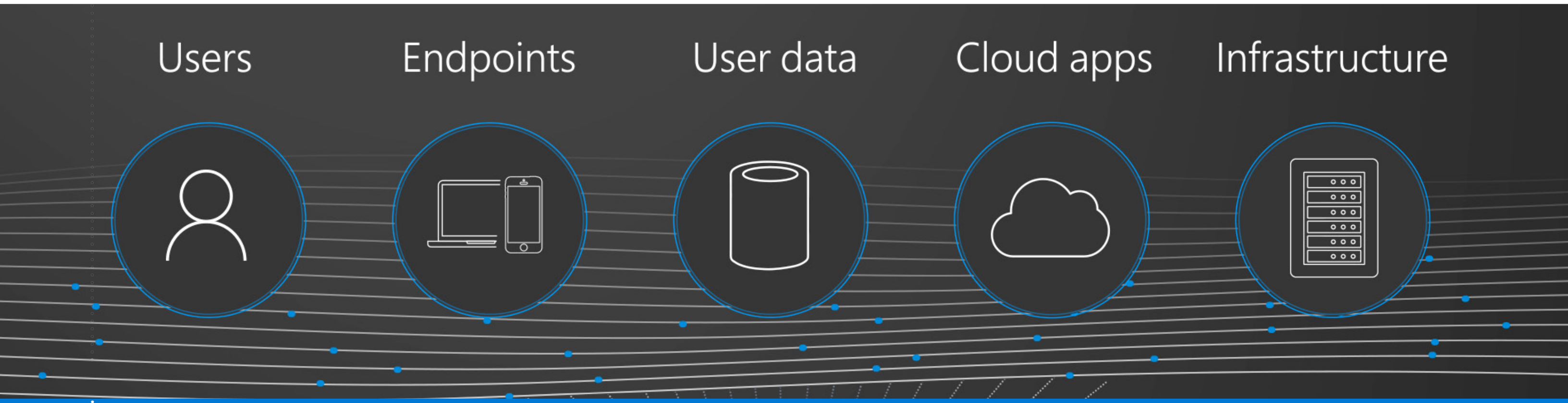
Our security teams span thousands of cyber-security experts globally and serve as a virtual extension of your own internal security teams. Utilizing signals from the Microsoft Intelligent Security Graph in conjunction with machine learning, they determine known and unknown attack vectors.

Cyber security experts at the Microsoft Cybercrime Center

The Microsoft Intelligent Security Graph, collects and analyzes an estimated 6.5 trillion signals per day from user log-ins across services, device end points, email messages and documents; Microsoft and non-Microsoft cloud apps, and our Azure public cloud infrastructure.

This scale gives Microsoft a vast window into the threat landscape, with unique insights that surpass other email protection solutions.

Importantly, exploits detected across these different sources are made known across all Microsoft services to enhance our vulnerability detection and protection capabilities across the stack.

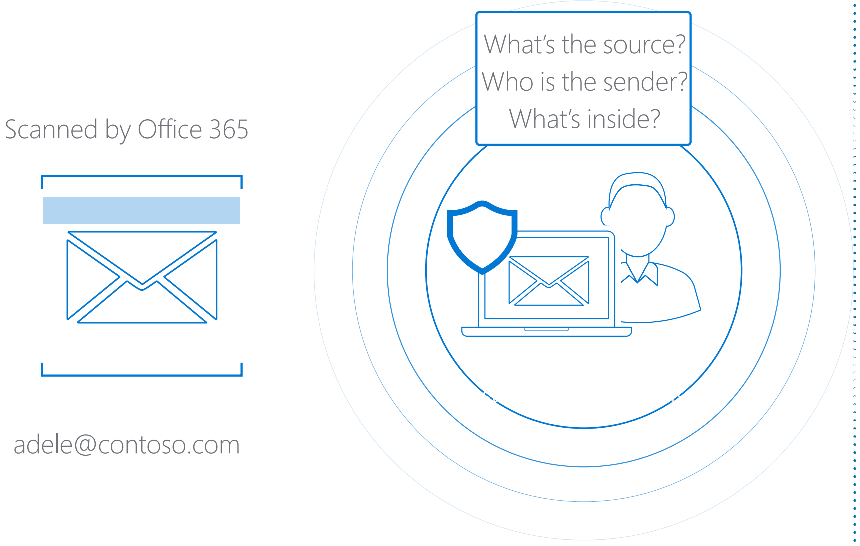


Our average malware catch rate for Office 365 email is the highest in the industry at 99.9%, and we have the lowest miss rate of phishing emails for Office 365.

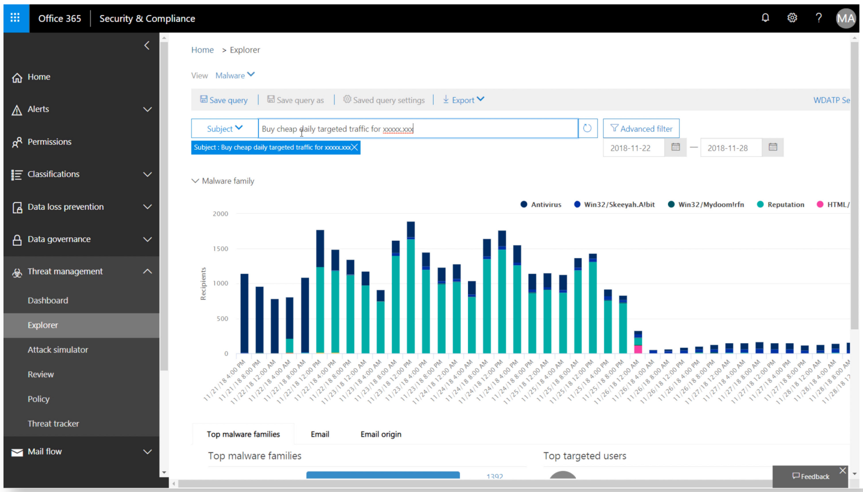
Layered defense-in-depth approach

Office 365 Advanced Threat Protection catches threats before they disrupt your organization by applying a systematic defense-in-depth approach that analyzes and protects against threats from the point at which an email is received by Office 365 to when it is delivered. This starts by identifying:

- Where the email is coming from by understanding the source
- Who the sender is and if the person, brand and or domain is authentic
- What's inside the email that could be compromising
- What post-delivery protections need to be put in place once the email is delivered to the recipient



Advanced Threat Protection in Office 365 provides best of breed capabilities for each defense layer



Subject: Buy cheap daily targeted traffic for xxxxx.xxx

Subject : Buy cheap daily targeted traffic for xxxxx.xxx

2018-11-22 — 2018-11-28

At any point in time, as an admin you can further harden your security posture against threats through near real-time reports, so that you can investigate and then respond to threats with built-in customer controls.

Who is the source?

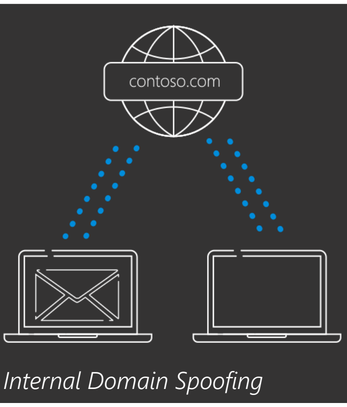
Before an email is delivered to an inbox, around 25% of all malicious messages received are blocked immediately at the edge. We look at the reputation of IP addresses by referencing our constantly updated block list of millions of domains and IPs. If the source is a known perpetrator of malicious messages, we will block it. Equally, machine learning models running on the edge determine email traffic patterns for your domain, blocking anomalous email traffic as necessary.

Who is the sender?

Next, we check that the sender really is who they appear to be by authenticating the source to prevent against spoofing, another common phishing technique. Here we are looking for evidence of spoofed domains, brands and people.

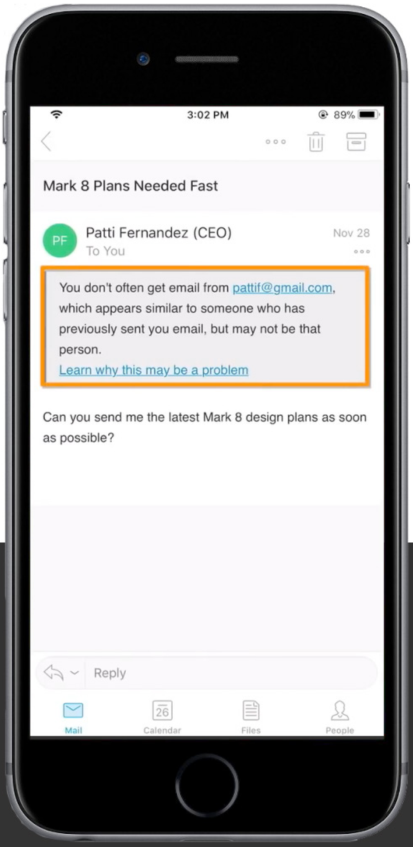
Spoofed emails look like they come from someone or something that you know or trust. The premise is that you are more likely to trust an email from someone of importance or a brand entity that you know.

Anti-phishing policies in Office 365 will verify the authenticity of the domain source against standard frameworks like Sender Policy Framework (SPF); Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication (DMARC) and also apply additional measures to detect the spoofing of internal or external domains.



Internal Domain Spoofing

In cases where emails are sent between domains that your organization owns, our anti-spoof technology will validate the origin of a message to make sure that it truly originated in your organization.



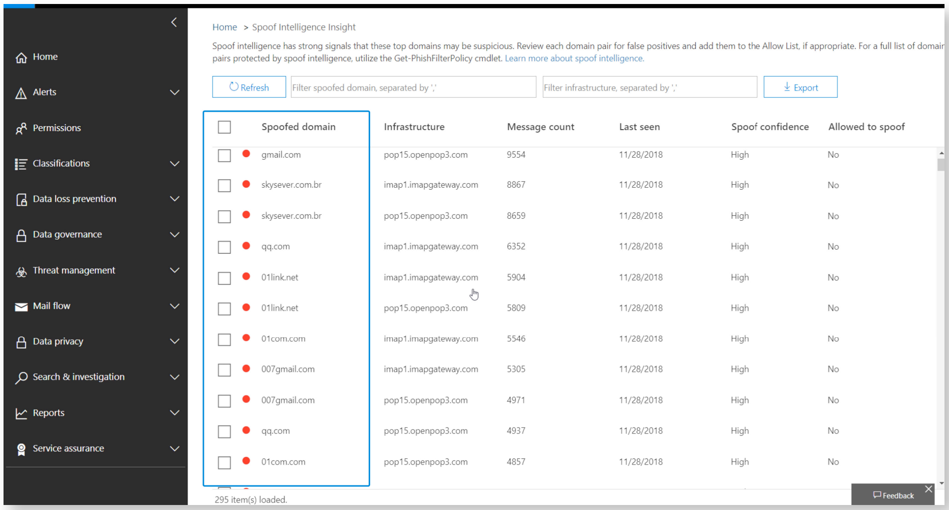
Mark 8 Plans Needed Fast

PF Patti Fernandez (CEO) Nov 28
To You

You don't often get email from pattif@gmail.com, which appears similar to someone who has previously sent you email, but may not be that person.
Learn why this may be a problem

Can you send me the latest Mark 8 design plans as soon as possible?

User and brand impersonation detected by Office 365



Home > Spoof Intelligence Insight

Spoof intelligence has strong signals that these top domains may be suspicious. Review each domain pair for false positives and add them to the Allow List, if appropriate. For a full list of domain pairs protected by spoof intelligence, utilize the Get-PhishFilterPolicy cmdlet. Learn more about spoof intelligence.

□	Spoofed domain	Infrastructure	Message count	Last seen	Spoof confidence	Allowed to spoof
□	● gmail.com	pop15.openpop3.com	9554	11/28/2018	High	No
□	● skysever.com.br	imap1.imapgateway.com	8867	11/28/2018	High	No
□	● skysever.com.br	pop15.openpop3.com	8659	11/28/2018	High	No
□	● qq.com	imap1.imapgateway.com	6352	11/28/2018	High	No
□	● 01link.net	imap1.imapgateway.com	5904	11/28/2018	High	No
□	● 01link.net	pop15.openpop3.com	5809	11/28/2018	High	No
□	● 01com.com	imap1.imapgateway.com	5546	11/28/2018	High	No
□	● 007gmail.com	imap1.imapgateway.com	5305	11/28/2018	High	No
□	● 007gmail.com	pop15.openpop3.com	4971	11/28/2018	High	No
□	● qq.com	pop15.openpop3.com	4937	11/28/2018	High	No
□	● 01com.com	pop15.openpop3.com	4857	11/28/2018	High	No

295 item(s) loaded.

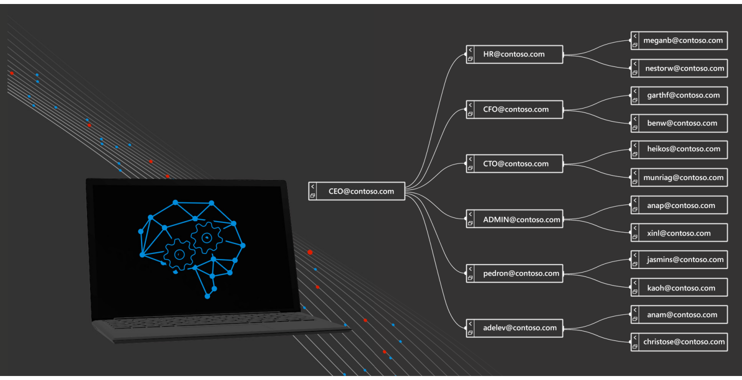
Spoofed domains detected by Office 365

For external domains, within or outside of our Office 365 ecosystem, our spoof intelligence first checks to see if the domain has been set up according to SPF, DKIM and DMAC standards. Then if not, it will observe and learn message sending patterns from the domain to identify when a message has been spoofed.

As an admin, you can access spoof intelligence under the antispam policy report to monitor suspected spoofing activity and influence the filter by forming an approved list of legitimate internal and external domains for your organization.

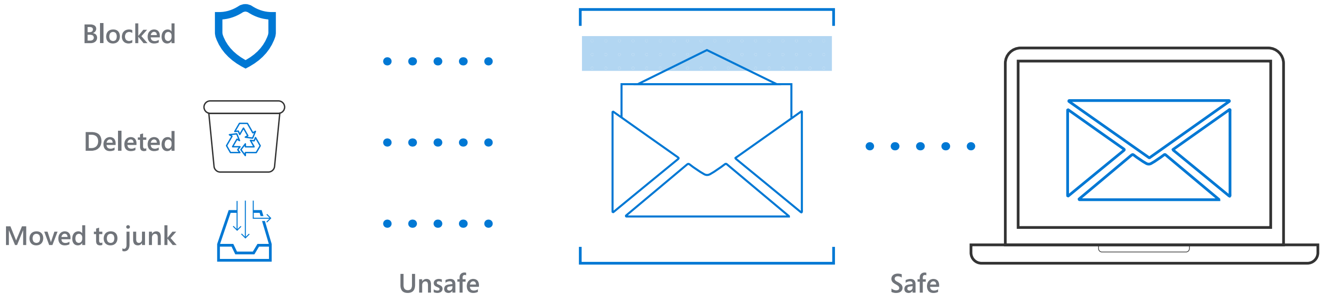
User impersonation

To protect against impersonation of your high-profile users, mailbox intelligence in Office 365 applies a machine learning model to form a contact graph of whom they are normally in contact with. This provides a strong signal for Office 365 to decipher anomalous and good behavior and to detect impersonation attempts of trusted individuals in your organization.



What's inside the message

To determine what's inside the message, we utilize a number of standard anti-virus and anti-malware engines to detect malicious content, combined with our Safe Attachment and Safe Links capabilities.



Attachments and links are detonated with actions taken according to the policies you have in place

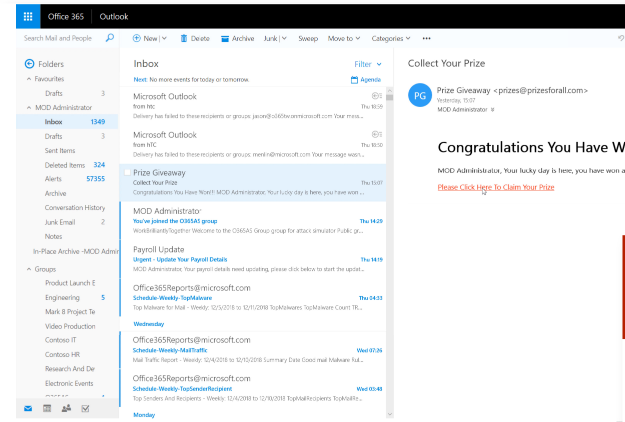
Attachments or links in the email are opened inside a sandbox environment where the content is meticulously analyzed by our machine learning models that check for malicious signals and apply deep link inspection. This allows for zero-day malicious attachments and links to be detected.

Each month we detonate around 1 billion items in our sandbox and the telemetry feeds back into the Microsoft Intelligent Security Graph to help our machine learning stay current with new and emerging techniques.

Even if the message passes through detonations, the content is analyzed further by multiple machine learning models. These examine the full message and we take actions based on what you have configured as policy.

Post-delivery protections

Sophisticated attackers will plan to ensure links pass through the first round of security filters. They do this by making the links benign, only to weaponize them after the message is delivered, altering the destination of the links to a malicious site.



Next: No more events for today or tomorrow.

Microsoft Outlook
from htc — Thu 18:59
Delivery has failed to these recipients or groups: jason@o365tw.onmicrosoft.com Your mess...

Microsoft Outlook
from hTC — Thu 18:50
Delivery has failed to these recipients or groups: menlin@microsoft.com Your message wasn...

Prize Giveaway
Collect Your Prize — Thu 15:07
Congratulations You Have Won!!! MOD Administrator, Your lucky day is here, you have won ...

MOD Administrator
You've joined the O365AS group — Thu 14:29
WorkBrilliantlyTogether Welcome to the O365AS Group group for attack simulator Public gr...

Payroll Update
Urgent - Update Your Payroll Details — Thu 14:19
MOD Administrator, Your payroll details need updating, please click below to start the updat...

Office365Reports@microsoft.com
Schedule-Weekly-TopMalware — Thu 04:33
Top Malware for Mail - Weekly: 12/5/2018 to 12/11/2018 TopMalwares TopMalware Count TR...

Wednesday

Office365Reports@microsoft.com
Schedule-Weekly-MailTraffic — Wed 07:26
Mail Traffic Report - Weekly: 12/4/2018 to 12/10/2018 Summary Date Good mail Malware Rul...

Office365Reports@microsoft.com
Schedule-Weekly-TopSenderRecipient — Wed 03:48
Top Senders And Recipients - Weekly: 12/4/2018 to 12/10/2018 TopMailRecipients TopMailRe...

Monday

Collect Your Prize

Prize Giveaway <prizes@prizesforall.com>
Yesterday, 15:07
MOD Administrator

Congratulations You Have Won!!!

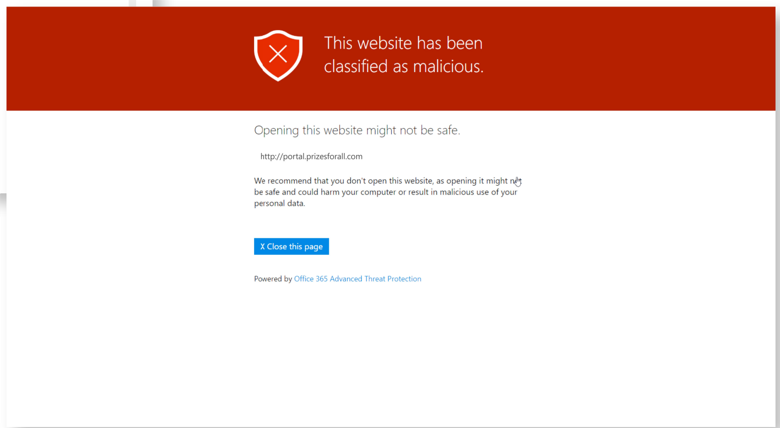
MOD Administrator, Your lucky day is here, you have won a free prize in our annual giveaway

Please Click Here To Claim Your Prize

Safe Links protects users at the point of click

With Safe Links, we are able to protect users right at the point of click by checking the link for reputation and triggering detonation if necessary.

20% of all clicks happen within 5 minutes from when an email is received.



This website has been classified as malicious.

Opening this website might not be safe.

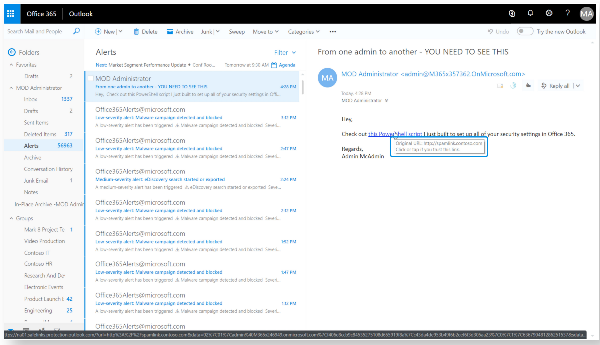
http://portal.prizesforall.com

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

Powered by Office 365 Advanced Threat Protection

Weaponized links are detonated by Safe Links and the recipient warned

Safe Links protection also extends to internal only emails. Unlike other email solutions, we are able to scan and isolate threats without routing these emails outside of Office 365.



Next: Market Segment Performance Update • Conf Roo... Tomorrow at 9:30 AM

MOD Administrator
From one admin to another - YOU NEED TO SEE THIS — 4:28 PM
Hey, Check out this PowerShell script I just built to set up all of your security settings in Offi...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 3:12 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 2:47 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com
Medium-severity alert: eDiscovery search started or exported — 2:24 PM
A medium-severity alert has been triggered ⚠ eDiscovery search started or exported Seve...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 2:12 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 1:52 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 1:47 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com
Low-severity alert: Malware campaign detected and blocked — 1:12 PM
A low-severity alert has been triggered ⚠ Malware campaign detected and blocked Severi...

Office365Alerts@microsoft.com

From one admin to another - YOU NEED TO SEE THIS

MOD Administrator <admin@M365x357362.OnMicrosoft.com>
Today, 4:28 PM
MOD Administrator

Hey,

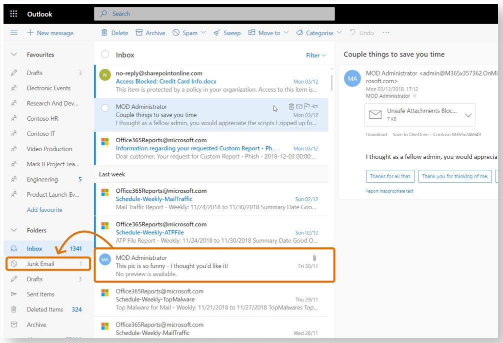
Check out this PowerShell script I just built to set up all of your security settings in Office 365.

Original URL: http://spamlink.contoso.com
Click or tap if you trust this link.

Regards,
Admin McAdmin

ttps://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fspamlink.contoso.com&data=02%7C01%7Cadmin%40M365x246949.onmicrosoft.com%7Cf406e8ccb9c84535275108d655919f8a%7Cc43da4de953b49f6b2eef6f3d305aa23%7C0%7C1%7C636790481286251537&sdata...

Real destination address of link revealed on hover to inform of potential threat



no-reply@sharepointonline.com
Access Blocked: Credit Card Info.docx — Mon 03/12
This item is protected by a policy in your organization. Access to this item is...

MOD Administrator
Couple things to save you time — Mon 03/12
I thought as a fellow admin, you would appreciate the scripts I zipped up fo...

Office365Reports@microsoft.com
Information regarding your requested Custom Report - Ph... — Mon 03/12
Dear customer, Your request for Custom Report - Phish - 2018-12-03 00:00:...

Last week

Office365Reports@microsoft.com
Schedule-Weekly-MailTraffic — Sun 02/12
Mail Traffic Report - Weekly: 11/24/2018 to 11/30/2018 Summary Date Goo...

Office365Reports@microsoft.com
Schedule-Weekly-ATPFile — Sun 02/12
ATP File Report - Weekly: 11/24/2018 to 11/30/2018 Summary Date Good O...

MOD Administrator
This pic is so funny - I thought you'd like it! — Fri 30/11
No preview is available.

Office365Reports@microsoft.com
Schedule-Weekly-TopMalware — Thu 29/11
Top Malware for Mail - Weekly: 11/21/2018 to 11/27/2018 TopMalwares Top...

Office365Reports@microsoft.com
Schedule-Weekly-MailTraffic — Wed 28/11

Couple things to save you time

MOD Administrator <admin@M365x357362.OnMicrosoft.com>
Mon 03/12/2018, 17:12
MOD Administrator

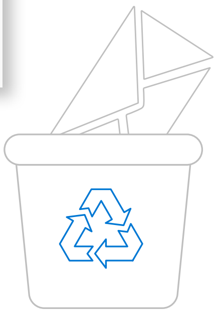
Unsafe Attachments Bloc... 7 KB

I thought as a fellow admin, you would apprecia

Malware infected email moved to Junk folder

Users are also made aware of the site they will be directed to as they hover over the link using native link rendering.

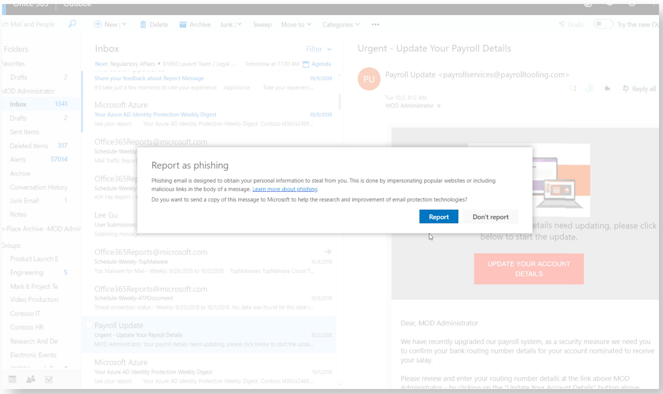
The service continues to scan email content for multiple days, leveraging new intelligence to move newly discovered malware or phish, by design, to the junk folder through a capability called zero-hour auto purge.



Zero-hour auto purge moves weaponized content to the junk folder

User self-reporting

Of course, while protections are automated in the background, we also encourage email recipients to be vigilant in identifying messages that appear suspicious. By enabling the report a message capability in your tenant, users can self-report suspect emails for validation by Microsoft and your security teams.



Next: Regulartory Affairs • X1050 Launch Team / Legal ... Tomorrow at 11:30 AM Agenda

Share your feedback about Report Message 10/9/2018
It'll take just a few moments to rate your experience. AppSource Rate your experienc...

Microsoft Azure
Your Azure AD Identity Protection Weekly Digest 10/8/2018
See your report. Your Azure AD Identity Protection Weekly Digest Contoso M365x2469...

Office365Reports@microsoft.com
Schedule-Weekly-
Mail Traffic Report

Office365Rep
Schedule-Weekly-
ATP File Report -

Lee Gu
User Submission:
Sidelining message

Office365Reports@microsoft.com
Schedule-Weekly-TopMalware 10/4/2018
Top Malware for Mail - Weekly: 9/26/2018 to 10/2/2018 TopMalwares TopMalware Count T...

Office365Reports@microsoft.com
Schedule-Weekly-ATPDocument 10/3/2018
Threat protection status - Weekly: 9/25/2018 to 10/1/2018 No data was found for this date r...

Payroll Update
Urgent - Update Your Payroll Details 10/2/2018
MOD Administrator, Your payroll details need updating, please click below to start the upda...

Microsoft Azure
Your Azure AD Identity Protection Weekly Digest 10/1/2018
See your report. Your Azure AD Identity Protection Weekly Digest Contoso M365x2469...

Urgent - Update Your Payroll Details

PU Payroll Update <payrollservices@payrolltooling.com>
Tue 10/2, 8:12 AM
MOD Administrator

...etails need updating, please click below to start the update.

UPDATE YOUR ACCOUNT DETAILS

Dear, MOD Administrator

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salay.

Please review and enter your routing number details at the link above MOD Administrator - by clicking on the "Update Your Account Details" button above

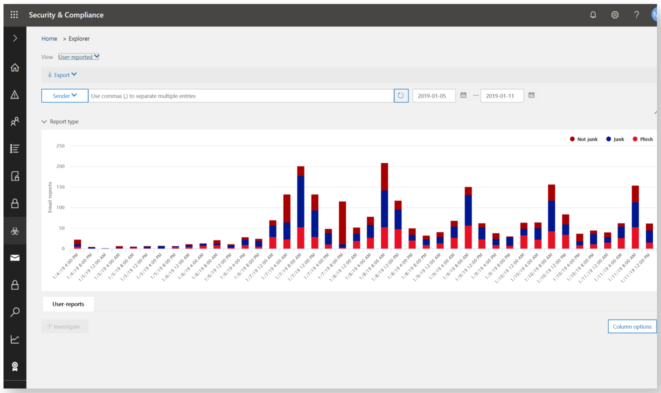
Report as phishing

Phishing email is designed to obtain your personal information to steal from you. This is done by impersonating popular websites or including malicious links in the body of a message. Learn more about phishing

Do you want to send a copy of this message to Microsoft to help the research and improvement of email protection technologies?

Report Don't report

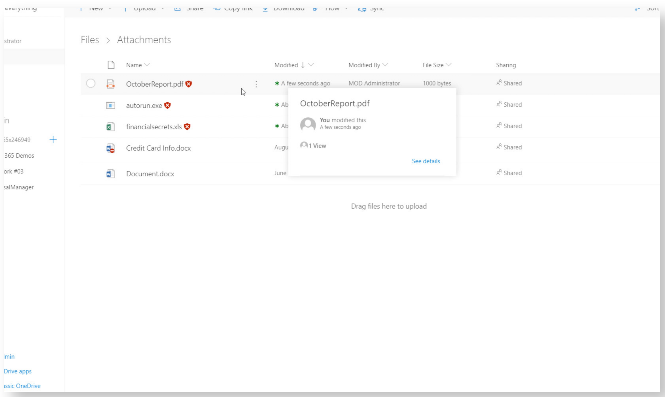
Users are able to self-report suspicious emails



Admin view of user, self-reported threats

Protections beyond email

Outside email it's important to ensure protections extend to malware infected content that may have been taken from email and placed on a share. Advanced Threat Protection in Office 365 uniquely extends protections beyond email. If malicious files or links are uploaded to SharePoint or OneDrive and shared, even via Microsoft Teams, our protection layers will detect it, block it, and contain the threat by preventing the file from being opened or shared in the future.



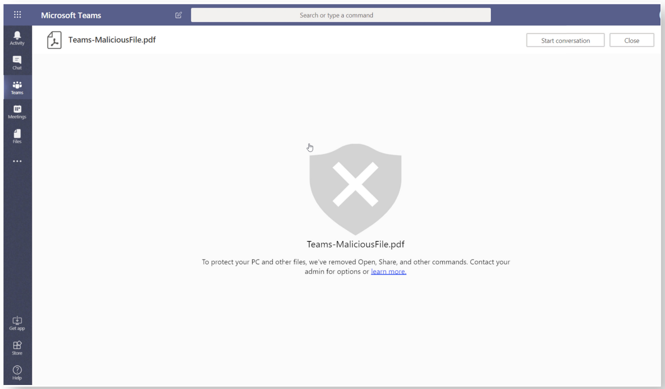
Files > Attachments

Name	Modified	Modified By	File Size	Sharing
OctoberReport.pdf	A few seconds ago	MOD Administrator	1000 bytes	Shared
autorun.exe	Ab			Shared
financialsecrets.xls	Ab			Shared
Credit Card Info.docx	Augu			Shared
Document.docx	June			Shared

OctoberReport.pdf
You modified this
A few seconds ago
1 View
See details

Drag files here to upload

Malicious links blocked in OneDrive



Teams-MaliciousFile.pdf

Teams-MaliciousFile.pdf

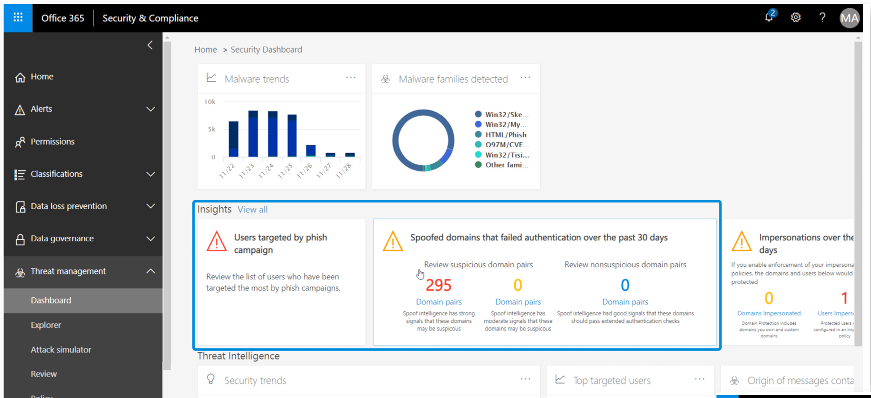
To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or learn more.

Malicious links blocked in Microsoft Teams

Review and respond

We give you near real-time reports to allow you to see emails within your organization and how they were handled by Office 365. This includes messages flagged by users as potential threats. Office 365 will additionally proactively surface insights and recommendations which you can use to determine what additional policies and protections you need to consider within your environment.

In the Security and Compliance Center, you can set up your phishing policies, define impersonation settings, investigate threats, review quarantined messages and how often they were sent, review detonations and get details on the nature of the threat and why it was detected. For example, under threat management you can drill in to see the top malware types and top targeted users.



Users targeted by phish campaign

Review the list of users who have been targeted the most by phish campaigns.

Spoofed domains that failed authentication over the past 30 days

Review suspicious domain pairs: 295 Domain pairs — Spoof intelligence has strong signals that these domains may be suspicous; 0 Domain pairs — Spoof intelligence has moderate signals that these domains may be suspicous

Review nonsuspicious domain pairs: 0 Domain pairs — Spoof intelligence had good signals that these domains should pass extended authentication checks

Impersonations over the days

If you enable enforcement of your impersona policies, the domains and users below would protected

0 Domains Impersonated — Domain Protection includes domains you own and custom domains

1 Users Impers — Protected users configured in an imp policy

Trojan Downloader Scripts
Trojan downloader scripts leverage scripting files to download other...

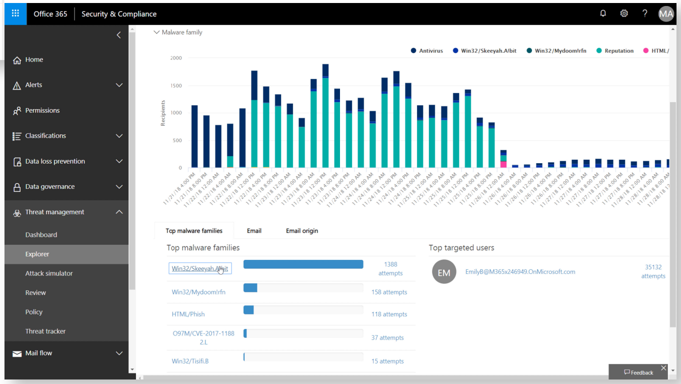
Nemucod
Nemucod is Microsoft's name for a script-based malware family that...

Emily Braun 35126

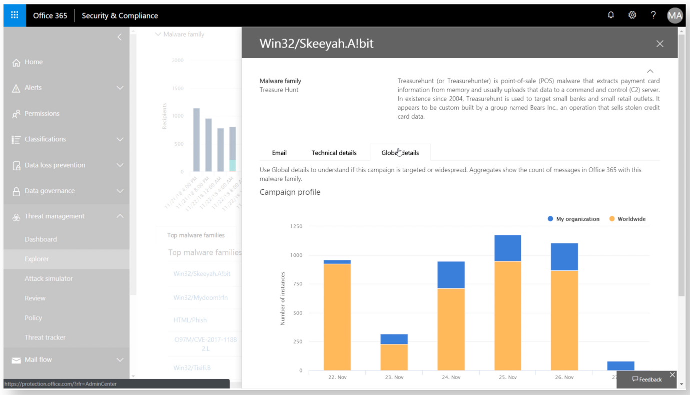
Threat intelligence dashboard view

Office 365 ATP blocked 5 billion phish emails in 2018

Within "Threat Explorer", malicious emails can be quickly identified with options to filter on sender, recipient and subject or other metadata in the message. Filtering on sender helps you to see all the emails sent from a unique sender address used for a phishing campaign. You can then investigate these emails further and take actions such as purging a malicious email campaign entirely from all mailboxes in your organization at once.



Drill down of top malware types and top targeted users



Malware family
Treasure Hunt

Treasurehunt (or Treasurehunter) is point-of-sale (POS) malware that extracts payment card information from memory and usually uploads that data to a command and control (C2) server. In existence since 2004, Treasurehunt is used to target small banks and small retail outlets. It appears to be custom built by a group named Bears Inc., an operation that sells stolen credit card data.

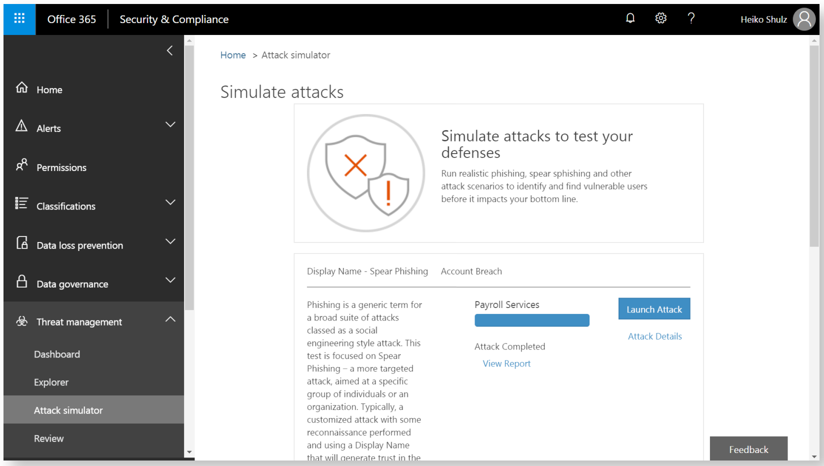
Use Global details to understand if this campaign is targeted or widespread. Aggregates show the count of messages in Office 365 with this malware family.

Incident investigation in Office 365

Investigation into an incident can also be separately delegated to your security investigation team, leaving it you your security admins to take the final actions. Also, because we know that there are common security issues that you will want to check over time, whether that's reviewing events, getting alerts, or determining threat trends, the threat tracker in our threat intelligence service enables ongoing supervision of your security tasks.

Educating and protecting users

Using services such as Attack Simulator in Office 365, we help you to broadly educate your users and augment your internal penetration testing capabilities by simulating phishing attacks in your organization to raise awareness of what to look for in a phishing campaign.



Simulate attacks

Simulate attacks to test your defenses

Run realistic phishing, spear sphishing and other attack scenarios to identify and find vulnerable users before it impacts your bottom line.

Phishing is a generic term for a broad suite of attacks classed as a social engineering style attack. This test is focused on Spear Phishing – a more targeted attack, aimed at a specific group of individuals or an organization. Typically, a customized attack with some reconnaissance performed and using a Display Name that will generate trust in the

Attack Simulator in Office 365, is designed to help you to penetration test your environment and educate users

Of course, there are other measures that you can put in place to protect your user identities. Microsoft is on a path to help the elimination of passwords altogether through password-less sign-in. We estimate that just by enabling multi-factor authentication in your organization, you can reduce your risk of attacks by 99.99%.

82% of all security breaches occur due to stolen passwords

Continued Learning

In Office 365, we give you built-in, proactive protections with Advanced Threat Protection. These protections extend to your collaboration services, such as SharePoint, OneDrive, and Microsoft Teams, in additions to your email services to mitigate malicious content. From:

- Intelligent and continuously evolving threat detection
- Visibility into threats, including real-time reporting to help you to investigate, remediate and respond to threats
- Advanced controls you set to harden your environment
- And tools to educate your users on phishing campaigns.

To learn more and try out Office 365 Advance Threat Protection capabilities for yourself, by visiting aka.ms/E5Trial today. Also watch our essentials video on Advanced Threat Protection in Office 365 here for more detail.