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.

The Microsoft Intelligent Security Graph, collects and analyzes an estimated 6.5 trillion signals per day from user log-ins across services, device endpoints, 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

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.

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.

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 DMARC 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 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.

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

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.

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.

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

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.
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.

![Users are able to self-report suspicious emails](image1.png)

![Admin view of user, self-reported threats](image2.png)

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.

![Malicious links blocked in OneDrive](image3.png)

![Malicious links blocked in Microsoft Teams](image4.png)
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.

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.

Office 365 ATP blocked 5 billion phish emails in 2018
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.

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.