Microsoft thwarts phishing attacks with Office 365

Microsoft processes more than 450 billion emails a month and blocks 10 million spam messages a minute to help protect people from malicious email, spam, and malware. Together, Microsoft Office 365, Exchange Online Protection (EOP) and Office 365 Advanced Threat Protection (Office 365 ATP) help defend against cyberthreats and guard data and intellectual property in real time—while enabling your organization to remain productive. EOP and Office 365 ATP are part of the broader, holistic Microsoft security platform, which includes security capabilities in Office 365 and in Microsoft technologies like Windows Defender ATP, Windows 10 (Device Guard and Credential Guard), Intune, and Azure Security Center.

These services all help protect against cyberthreats and use powerful machine learning algorithms partly built from signals that we get from emails and attachments. We also study patterns and anomalies that help detect malicious email, spam, and malware.

What is phishing?

One common form of unwanted email that EOP and Office 365 ATP help address is *phishing* email—a type of online identity theft. *Threat actors*—or attackers—try to trick you into opening a link or attachment, replying to an email, wiring money, or taking other action. They may also try to coax you into giving corporate or personal information like account details, passwords, or credit card numbers. Attackers try to lure you with seemingly legitimate email, text messages, websites, or phone calls, and use the information for financial gain, espionage, or other nefarious purposes. Attackers often use fake websites, issue threats, pose as a legitimate company, or pretend to be someone you know.

Let's take a closer look at some typical phishing attacks. Considering these common tactics, we'll show:

- How EOP and Office 365 ATP help improve protection against large volumes of complex phishing attacks.
- How our Core Services and Engineering organization (formerly Microsoft IT) at Microsoft—which handles more than 15 billion security events per day—uses EOP and Office 365 ATP to learn about attacks, investigate and respond to attacks faster, and be more proactive.

Phishing attempts are increasingly sophisticated

Phishing attempts are constant, and attackers' tactics are constantly evolving. Organizations must get ahead of these attempts—armed with awareness and technologies that constantly evolve to help protect against malware and viruses. This is especially true given ever more sophisticated attacks. For example:

- In the past, phishing emails—sent at mass volume—weren't as carefully constructed or as targeted. Today, there's a vast industry dedicated to phishing cyberattacks. Perpetrators include professional criminals, organized crime, and nation-states. There are companies that employ criminals, with their own research and surveillance teams. Threat actors pay close attention to spoofing a company or person and making a message look legit.
- Because of the proprietary information that they have, executives are a common high-profile target in phishing attacks known as *whaling*.
- *Spear-phishing* poses a special challenge. Whereas phishing casts a wide net, spear-phishing targets specific people. Emails appear to come from a company you do business with or someone you know and trust, like your boss or colleagues. Spear-phishers seem familiar with how your organization operates or what your interests are.
- From an overall industry standpoint, 91 percent of security breaches begin as phishing or spear-phishing. Verizon's 2017 Data Breach Investigations Report states that 1 in 14 people clicked a link or opened an attachment in a phishing message; 25 percent of these people fell victim more than once.

- Rather than setting up special domains for a campaign—only to have security mechanisms identify them as fake and block the content—a growing trend is for some attackers to compromise trusted websites and insert a page with phishing content.
- Today's life cycle of phishing attacks is shorter, which makes it harder for antiphishing technologies to keep pace.

Common types of phishing

Although there are many types of phishing, common ones include:

- **Stealing credentials.** To get inside information, an attacker obtains a person's user name and password—for example, credentials that an employee uses to access company resources.
- **Identity theft.** With the credentials and information, an attacker impersonates a user or company.
- **Stealing personal information.** An attacker goes after personal account details, passwords, credit card numbers, or other sensitive information.

Here's an example of a phishing scenario:

1. An attacker targets a broad set of people (or a subset, in the case of spear-phishing) by sending email from what seems to be a legitimate online service, retailer, or financial institution.
2. The email has a link that directs people to a malicious website or webpage, or it has an attachment.
3. If the email recipient clicks the link or opens the attachment, malware is downloaded to their computer, and the attacker gains access to their network. Other malware can be used to steal information (cyberespionage) or encrypt files for ransom (ransomware). The malware often steals credentials used for multiple apps and the attacker can use the credentials for further attacks, such as signing in to banking or retail websites.

EOP and Office 365 ATP help address volume and sophistication

Although phishing tricks and tactics never cease, awareness and antiphishing technologies go a long way in thwarting them. No one solution can stop all phishing campaigns. However, EOP and Office 365 ATP—part of the Microsoft Office 365 threat protection stack—help organizations defend against the volume and sophisticated nature of today's email-based phishing attacks:

- **EOP for known threats.** EOP is an email filtering service that helps protect against the volume of attacks by filtering *known* spam, viruses, and malware.
- **Office 365 ATP for unknown threats.** Like EOP, Office 365 ATP is an email filtering service, and the two are closely integrated. Office 365 ATP helps protect against *unknown* threats—including help stopping sophisticated, zero-day advanced threats.

EOP and Office 365 ATP—along with security capabilities in products and services like Windows 10, Windows Defender ATP, Threat explorer in Office 365 Threat Intelligence, which helps you detect and analyze threats, and Azure Security Center—are key parts of our robust antiphishing strategy.

How EOP helps protect against phishing

Integrated with Office 365 ATP, EOP is available for all Office 365 mailboxes. EOP capabilities include:

- **Protection that keeps evolving.** EOP helps protect against known viruses, spam, phishing, malware, and spoofing. Antimalware scan engines detect and block early-stage threats before they infiltrate network devices.
- **Inbound and outbound email filtering.** EOP captures more than 99 percent of spam emails and viruses. To block spam, it uses filtering, IP address block/allow lists, malicious URL block lists, and machine learning.

- **Zero-hour auto purge.** From constant monitoring and updates to Office 365 antispam and antimalware signatures, zero-hour auto purge detects delivered messages with spam or malware. If the messages are unread and flagged as malicious, it moves them to the Junk mail folder.
- **Safety tips in Microsoft Outlook.** Suspicious and phishing emails are flagged with tips stating that the email is from an untrusted source, and a red bar appears at the top of the email.
- **Filtering for common malicious attachment types.** Email administrators can filter out unwanted and suspicious attachments by file type within the Malware Policy.
- **Phishing reporting.** Users can report phishing through the **Report Message** feature in Outlook and Outlook.com.
- **Protection against insider spoofing, which has led to 500-percent stronger counterfeit detection.** Suppose a phisher impersonates an executive from the same company as an email recipient, by spoofing the email domain. EOP antispoofing capabilities use reputation filters to block email from low-reputation IP addresses, domains, and senders, and vigorously check authentication.

How Office 365 ATP helps protect against phishing

Office 365 ATP is available as part of Office 365 Enterprise E5 and as a standalone component. It addresses evolving threats like phishing attacks, at scale, with:

- **Safe attachments.** This helps to protect against unknown malware and viruses with behavior analysis, and machine learning algorithms.
- **Safe links.** This helps to protect against malicious URLs at time-of-click.
- **URL detonation.** This helps to protect users against files that are linked to in the body of an emails, combining the capabilities of Safe attachments and Safe links.
- **Reporting and tracing.** This provides URL trace and reports on advanced threats.
- **Office 365 ATP enhanced reporting.** This shows malware and spam trends in an organization.

Safe attachments helps protect against zero-day exploits and other dangers

Safe attachments helps detect new, malicious attachments before new antivirus signatures are made available to block them. Consider the following scenario:

1. An attacker targets an organization with a new malicious attachment. EOP uses filtering techniques such as looking at the sender's IP address or other email headers. Antivirus signatures help thwart attacks, and antispam filters remove spam.
2. If the email message or attachment doesn't yet have an antivirus/antimalware signature that can block the attack, it goes to a sandbox environment. Safe attachments detonates attachments such as PDFs, Office documents, or executable files. We use behavioral analysis and machine learning to see if the content is malicious.
3. With Dynamic Delivery, the body of an email is delivered while Safe attachments scans the attachment. The email recipient can still read/respond to the email while the attachment is being analyzed. After the attachment is scanned, if it's legitimate, it's delivered to the person's mailbox. If it's malicious, the attachment is filtered out.

Safe links helps protect against malicious URLs

When people click a link in an email, Safe links protects them by preventing them from going to a malicious site. Safe links blocks the malicious link at the time of click, while allowing people to access legitimate links.

With Safe Links, when someone clicks a link, the link is checked against a list of malicious URLs at the time of click. Consider the following scenario:

1. An attacker compromises a site sends an email that contains the URL that looks like a safe site, and thus passes by the initial reputation check of EOP filters. Because the website seems trustworthy, the URL passes through our filtering pipeline.
2. A few minutes later, the original URL morphs into a malicious website, potentially a phishing site. At this point, the email has already gone through the filtering pipeline.
3. If you enable Safe links, the URL is rewritten so that it redirects to EOP web servers. You can modify Safe links behavior by adding URLs to a list of good/bad URLs. If someone clicks the link, before going to the URL, the link is checked against the latest good/bad URLs. If the link is bad, a warning states that the website is malicious.

Figure 1 shows how EOP, Office 365 ATP, Safe attachments, and Safe links help fight attacks.

Figure 1. How EOP, Office 365 ATP, Safe attachments, and Safe links help fight attacks

URL detonation checks links in a safe environment

URL detonation combines the capabilities of Safe Attachments and Safe Links. When an email contains a linked-to file, URL detonation will examine the linked-to file using our sandboxing technology to determine if the file is malicious. If the file is found to be malicious, at the time of click, a user will be blocked from accessing the malicious linked-to file.

Reporting and tracing give details on actions taken, messages, and links

- Safe attachments reports show actions that are taken on files (for example, blocked or replaced), file types, date, sender, recipient, subject, and other details).
- To help with quick remediation, Safe links reports show who clicked a malicious link.
- URL tracing tracks malicious links, shows who in the organization is targeted, and shows the types of attacks.
- Reporting and message tracing help with investigating messages that are blocked because of a virus or malware.

Office 365 ATP enhanced reporting shows malware and spam trends

The Office 365 Security & Compliance Center provides security reports that show trends in your organization—for example, malware and spam that were sent or received, and advanced threats that Office 365 detected and stopped.

Phishing scenario: Technologies help protect and defend against threats

In the bigger picture, EOP and Office 365 ATP capabilities are an essential part of our broader security platform. This platform includes security capabilities in Office 365 and other Microsoft technologies like Windows Defender ATP, Windows Defender SmartScreen, Windows 10 (Device Guard and Credential Guard), Intune, and Azure Security Center. Figure 2 shows how these technologies help defend against threats and malware in a phishing campaign that targets an organization. The top of the figure shows the threats, and the bottom shows the technology capabilities.

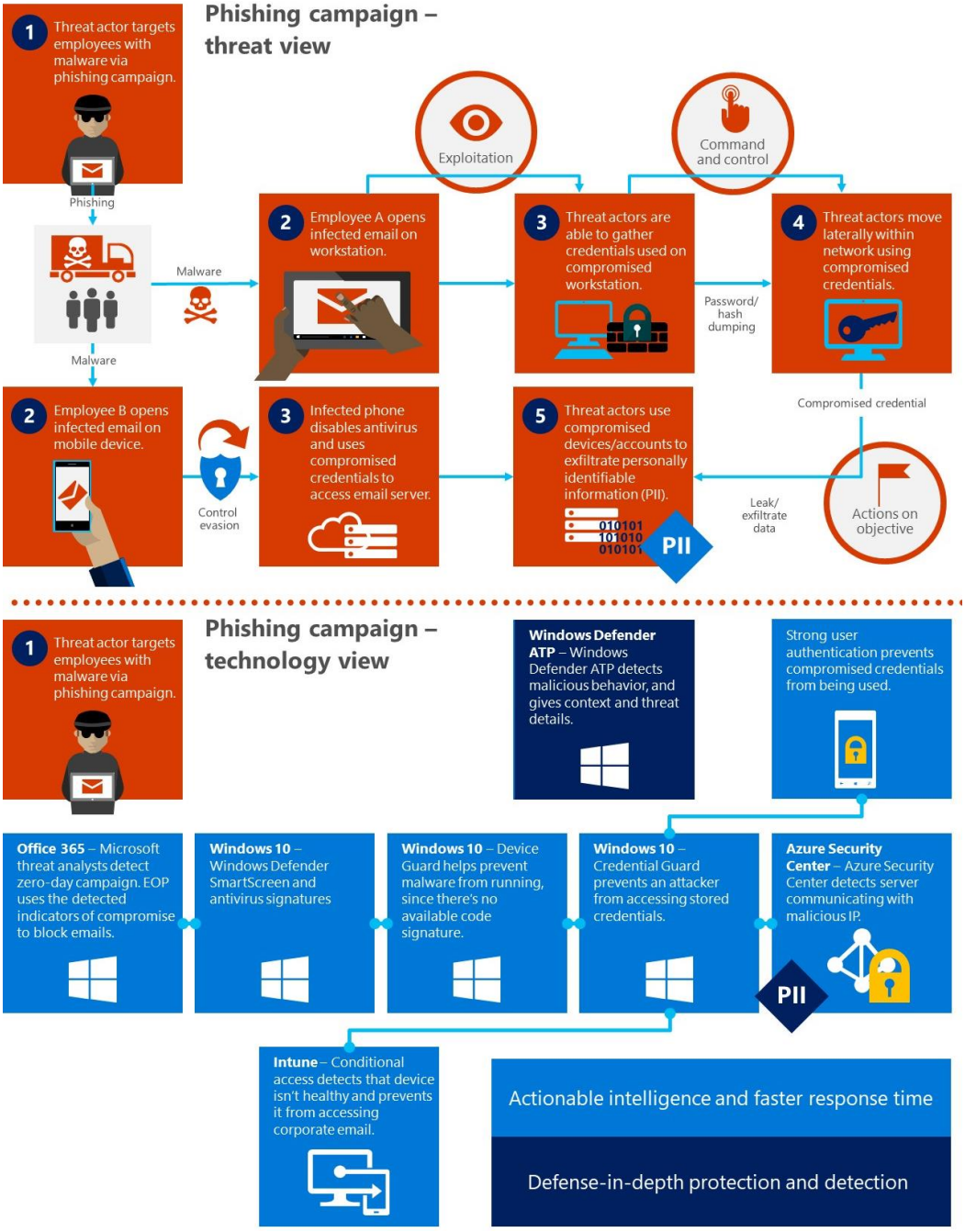

Figure 2. Office 365, Windows Defender ATP, Azure Security Center, and other technologies combat phishing attacks

How Microsoft is enhancing antiphishing technology

At Microsoft, we're continuously advancing how we combat phishing. For example, we use:

- Optimized machine learning algorithms that detect phishing signals in the email body, headers, and URL. To enhance Office 365 ATP and EOP, we extract signals from URLs and attachments. To detect phishing in websites and in attachments such as PDFs, we feed these signals into machine learning models.
- Enhanced clustering, patterns, and anomalies associated with phishing, malware, and spoofing.
- Enhanced real-time reputation lists of domains, IP addresses, senders, and URLs. We also incorporate knowledge from industry-leading feeds.

Case study: How the Core Services and Engineering organization at Microsoft fights phishing

At Core Services and Engineering—and in our Digital Security and Risk Engineering (DSRE) team at Microsoft—we fight today's complex phishing attacks with a multipronged approach. The DSRE team was developed to help ensure that all company information and services are protected, secured, and available for appropriate use through innovation and a robust risk prevention framework. Across our organization and throughout the company, DSRE constantly evolves the security strategy and protects our assets and our customers' data.

Our antiphishing approach combines people and technologies

As part of our process, we combine information from employees, product groups, alerts, and other sources with antiphishing capabilities in technologies like EOP and Office 365 ATP—which are part of the Office 365 security stack. Using this approach, we proactively defend against phishing, advanced threats, malware, and zero-day attacks.

From a strategy perspective, these methods give us added visibility into phishing campaigns. Educating employees about phishing and encouraging the mentality of "when in doubt, report it out" provide network defenders with additional telemetry for detecting large-scale phishing campaigns—including sophisticated and targeted spear-phishing attempts.

How employees report phishing

Methods for gathering phishing information include Microsoft employee reporting and other sources:

- They can report phishing emails or any cybersecurity incident through an internal website.
- They can use the **Report Message** feature in Outlook.

What DSRE does after phishing information is reported

After the information is reported:

- In DSRE, from the reports we receive in the group mailbox, we analyze the message, attachments, and links. They are triaged, prioritized, and escalated for proper mitigation of the email threat.
- We also get information about phishing activities from our security information and event management (SIEM) system. Our reporting channels and SIEM help us investigate and respond—for example, by flagging phishing sites.

We set up our SIEM to:

- Detect malware infection and compromised accounts.
- Monitor and respond to trojans that steal passwords.
- Get alerts on credential theft.

- Additionally, in DSRE, we use signals and intelligence from a variety of products and product teams, such as Windows Defender ATP and Office 365 ATP.

Antiphishing capabilities help DSRE protect against advanced threats

Some of the technologies and capabilities we use in DSRE include:

- EOP to help protect against spoofing, known viruses, and 99 percent of spam.
- Office 365 ATP to detect malicious links and attachments, and to track blocked messages and malicious links with Safe links, Safe attachments, URL trace, and Message Trace.
- In the Office 365 Security & Compliance Center, we use Threat explorer to:
  - Search emails and malware, analyze headers in malicious email, and see the impact of phishing and malware.
  - Take action—such as move email to Junk, so that recipients don't open it, click a link, or open an attachment.
  - Get details such as who was affected, the sender and recipient addresses, and what actions were taken.
- Also available in the Office 365 Security & Compliance Center, we use Content Search to see the body of malicious email and get full context for further analysis. For example, we could see if there's an unsafe link in the message.

How EOP and Office 365 ATP help us

EOP and Office 365 ATP are crucial parts of our overall strategy. For example, we use them to:

- **Take advantage of antispoofing protection in EOP.** Suppose a person in business group A of a company gets an email with a link and attachment from someone in business group B. The latter person requests inside information or personally identifiable information. In this case, the attacker has spoofed the identity of the employee in business group B, but neither employee knows it. The employee in group A might not recognize the sender or may think the request is suspicious, and they report the email.

  As a result, we can see if others got emails from that address, and check if others clicked a link or opened an attachment. EOP can detect something that's spoofed and, at the top of the email, indicate that it's a fraudulent message. We can also have the Exchange team create a rule so that any emails that go to the unsafe address are redirected to our mailbox. We prevent those emails from going to the attacker and can see who's being phished.
- **Help us proactively defend against attacks by checking links and attachments.** Email with unsafe links and attachments can carry advanced threats like zero-day attacks and advanced phishing campaigns. We enable Safe links, for time-of-click protection against malicious URLs. Malicious links are blocked while good links can be accessed. We also enable Safe attachments. Potentially malicious files without a known virus/malware signature are opened in an isolated environment. If no suspicious activity is found, the message is delivered. From the visibility we get, we apply security policies in organizations across Microsoft.
- **Get reporting, message tracing, and URL tracing.** We investigate messages blocked because of a virus or malware. We search on sender, recipient, subject line, and other criteria. With URL trace—based on Safe links—we track malicious links that are clicked. We see how many emails had the link and how many people clicked.

Benefits of our antiphishing strategy

The technologies and processes that form our broad threat detection strategy help us in many ways:

- **We have better visibility on phishing and get more context about threats.** This helps us to be more proactive. With telemetry from EOP, Threat explorer in Office 365 Threat Intelligence, and antivirus detection on

malicious files, we can see who the business groups and other recipients were and we can spot trends without having to rely on other teams for this information. To be even more proactive, we're working on targeted alerting and clustering, based on specific business groups that receive a suspicious email.

- **We save time and respond faster.** We can search and purge emails on our own—again, without having to rely on other teams as much. In the past, depending on the size of the phishing campaign, searching for malicious emails, and then purging them from email stores, could take days. Now, with Office 365, we can:
  - Search for malicious email ourselves.
  - Use EOP and Office 365 ATP to determine the status of an email or attachment.
  - Delete malicious attachments or move email to the Junk folder to prevent people from interacting with the malicious email.

  For example, even when we faced the large DocuSign phishing campaign, we were able to understand the breadth of the campaign and remediate it within an hour by using Threat explorer, EOP, and Office 365 ATP. In the past, it would have taken days to remove the emails from people's inboxes.

  Plus, from the time we save, we can respond more quickly to threats.
- **We have fewer manual processes.** There used to be much more manual investigation to see who was targeted. Now, we get telemetry up front, which removes a lot of the manual work.
- **For email investigations, we've reduced the number of tools required.** The integration between Threat explorer and Office 365 ATP means fewer places to look for details on a threat and to triage an event.
- Because of integration between technologies in our security platform**, we have good context about what happened before, during, and after an attack.** One example is the integration between Windows Defender ATP and Office 365 services like Threat explorer. Suppose that we're investigating a malware infection. We can see what happened before the infection, such as an email with an attachment that was saved from Outlook. We can use Threat explorer to investigate the email and attachment and determine if that attachment caused the infection. For example, when one email recipient got an alert from Windows Defender ATP about a ransomware infection, we were able to track the malware back to a downloaded file from Outlook.

Summary

To help protect against increasingly sophisticated phishing attempts, spam, and malware, Microsoft keeps advancing its security capabilities. No one solution can stop all phishing campaigns. However, Office 365 services and capabilities like EOP, Office 365 ATP, Safe links, Safe attachments, and antispoofing—along with other technologies in the broader Microsoft security platform—provide robust defense against phishing, malware, zero-day attacks, and advanced threats. Our technologies evolve as phishing campaigns and other attacks evolve. Antiphishing algorithms, machine learning, clustering, and pattern/anomaly detection further strengthen our security framework for quick detection, enhanced prevention, and targeted response.

For more information

Microsoft IT Showcase

microsoft.com/ITShowcase

Microsoft Office 365