Whitepaper

Mastering Email Security

Author: Richard Diver | Cloud Security Architect – Insight Security Team

Introduction

The use of email continues to be a critical part of the core communications between, and within, every organization in the world. Currently the majority of attacks and successful breaches that impact companies of all sizes can be attributed to email-based attacks as the starting point.

A successful phishing attack is when an email is created with malicious intent, delivered to the end user, and they unwittingly carry out the unwanted behavior, such as activating malware or disclosing sensitive information. There are similar attacks such as spear phishing and whaling, which both refer to attacks that are targeted at high-value individuals for specific outcomes. Spoofing and impersonation are common compromises that plague our email systems, playing on the social engineering techniques that defy many modern defenses and de facto trust in others.

IT teams will deploy multiple security solutions and approaches in an attempt to secure their organization against these email-based attacks, including email gateways, anti-malware, and end-user awareness training. Unfortunately, the attacks continue to succeed, at an alarming frequency and with devastating financial, reputational, and privacy impacts.

This whitepaper will cover the key scenarios, risks, and threats that are inherent with every email system. Due to the popularity of the platform, the information provided will reference Office 365® and Exchange Online as an example. However, the guidance is transferrable to any other email platform you may use to manage email for your organization today. The same is true for other components of the email solution, such as the device, operating system, browsers, and applications used to interact with email.

Sections

This whitepaper should be read in sequential order, however, you can jump to the chapter that most interests you.

Attacks | Risks | Solutions | Recommendations

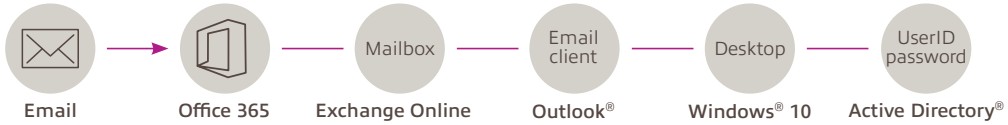
Five types of attack

Email overview

Email is a standard form of official communication between organizations, and to or from their customers. Although not its original design or intention, organizations now rely on email as one of the primary means for sharing sensitive information and especially links to useful websites.

The choice of email platform is open to a range of options, with Microsoft® Office 365 currently the main contender and Google G Suite as another popular choice. Whichever platform your organization chooses, the risks, attacks, and solutions will apply to them all.

As with all email systems, the full attack chain includes the platform, mailbox, applications and browsers used to connect to the mailbox, operating system of the end-user device, as well as the identities used to gain access to the information.

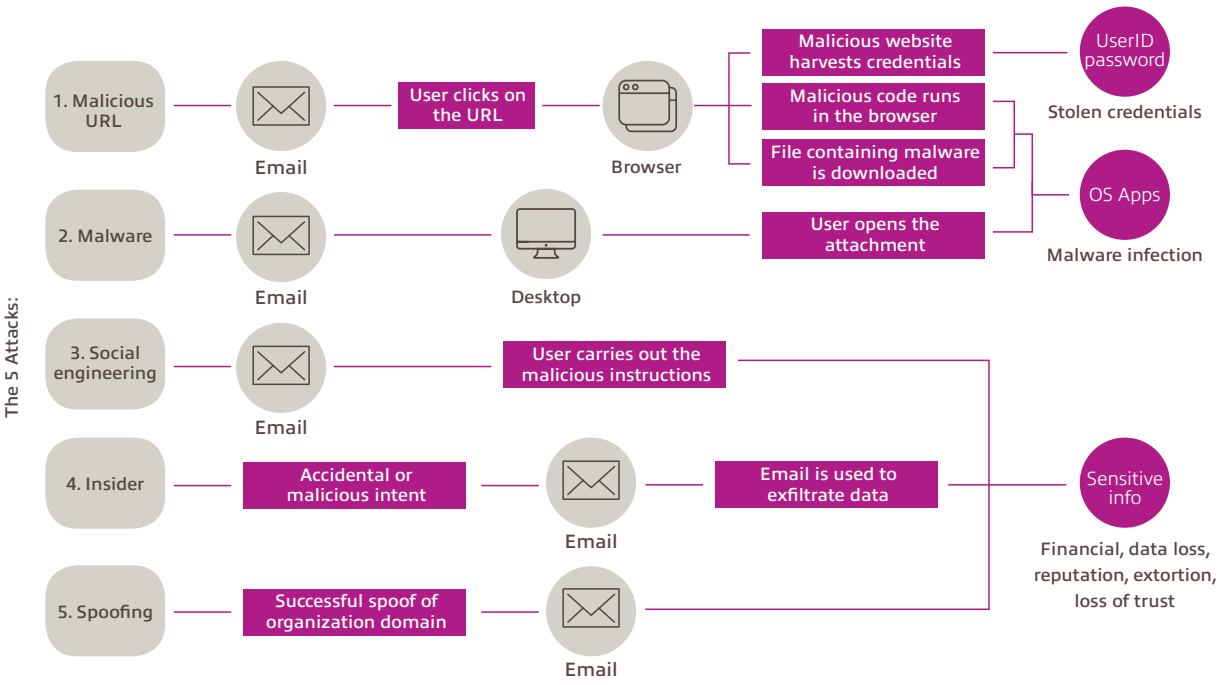


Five key attacks

This diagram represents the five attack types that are most common and successful in today's email systems. Other attack types are a variant of these, and the underlying problems and solutions are the same.

Each attack type may be combined and the results may have additional impacts, such as reputation and financial damage, following the success of stolen credentials.

This section will walk through each of these attacks in more detail. Whilst these are not the only attack methods, they do convey the majority of successful attacks over the last decade.

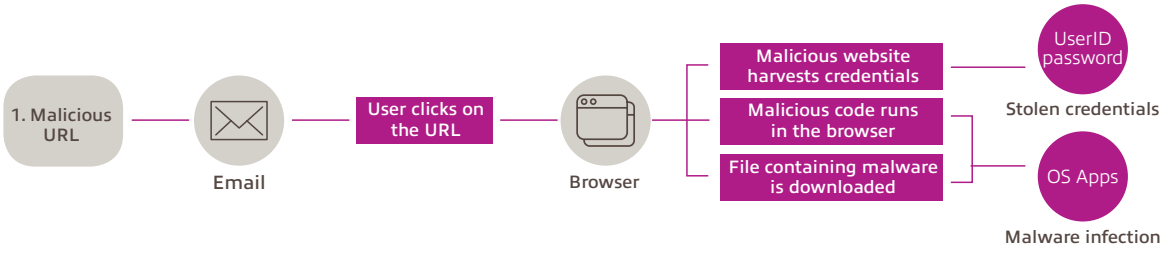


Attack 1 — Malicious URL

In this scenario, the attacker has crafted an email with a malicious URL embedded in the document. It may be masked as a link to an official site, or embedded in an image. The URL may also be within a document containing relevant information to the reader — anything to entice them to click on the link and visit the malicious webpage.

Once the URL is clicked, the browser will launch and present the malicious site to the end user. Depending on the nature of the site, the user may be duped into believing it is an official site from a well-known brand, prompting for a sign-in. Browsers may alert to certificate errors, or they may not.

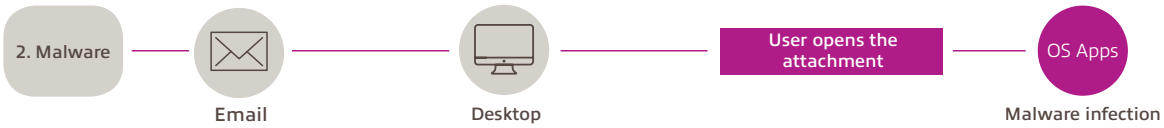
If the end user does enter their user ID and password, these are captured by the malicious site for reuse, and may then take the user to the legitimate site and sign them in, masking any malicious activity.



Attack 2 — Malware

In this scenario, the attacker has added an attachment to the email which contains malware. When the attachment is opened, the malware will exploit vulnerabilities in the application, browser, or operating system in use at the time. New variants of malware will also run within the context of the current user, without any exploits or elevated privileges, acting on behalf of the user to encrypt documents, send further emails, and spread itself across the infected system and connected networks, storage, and other mailboxes.

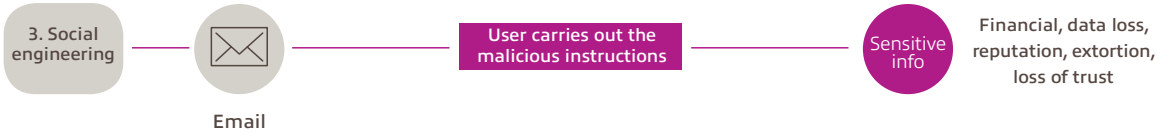
The effects can be immediate, and may also be silent. The end user may be unaware anything nefarious has occurred, and carry on with the usual activities whilst the malware hides in the background.



Attack 3 — Social engineering

This may also be seen as a "malware-less attack" — any scenario where the attacker will attempt to use persuasive techniques to encourage the end user to carry out a task that is beneficial to the attacker. Examples of this include offering a prize or reward, suggested promises of a job interview, providing useful information, or otherwise pretending to be someone else the end user trusts (spoofing or impersonation). This may occur outside of the business email channel, such as using personal email, social media, phone calls, and other forms of communication.

Unfortunately, exploitation of human trust will always be the weakness of any security system. Social engineering techniques continue to bypass many security controls because the end user is interactive in the process and unaware the actions they are taking may lead to malicious activity. When the end user carries out the activity, it is difficult to tell if it was their intention to carry out this activity willingly, or if they were duped into doing so through trust in the instructions given.

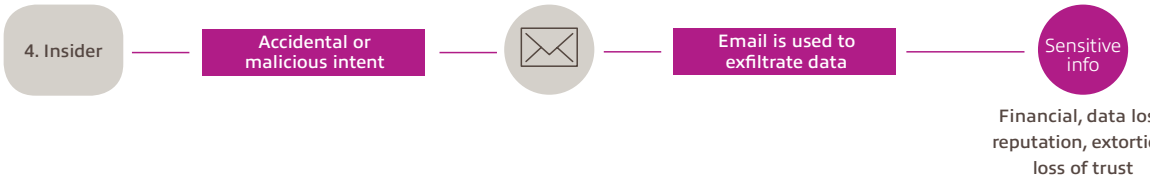


Attack 4 — Insider compromise

This attack type comes in two key methods, with the result being very similar:

1. Compromise of the identity, device, or application; in order to act on behalf of a legitimate user, without their knowledge or consent (a key result of attack types 1 and 2).
2. Compromise of the end user's integrity; the human is actively intent on causing malicious harm to the organization and will use their internal trust in order to carry out their attack.

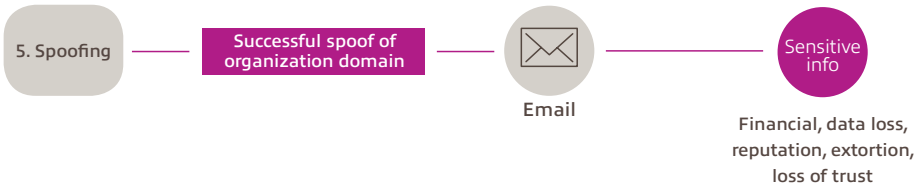
With either method, the potential for loss through email is primarily data exfiltration, but could also result in system modification or sending malicious instructions to others inside or outside of the organization.



Attack 5 — Brand/reputation

In this scenario, the attacker is using your organization's brand in order to carry out attacks against other organizations, your partners, or your customers. By impersonating your organization, they can influence other people to believe they are acting on your behalf, and therefore carry out the instructions that have been sent to them via email.

One of the most successful, and financially damaging attacks of this kind, is when an email is sent to request the change of payment information, usually for the next invoice that is due to your organization from a customer or partner. Not only does your organization not receive the invoice on time, but the loss of funds and the effort required to investigate and recover those funds causes additional loss to the customer or partner impacted.



Attack summary

There are many variants to these five attack types, including attacks that originate outside of email. Each attack will use an element of these examples, and the results are generally the same:

- Compromise of the user identity, leading to unauthorized access to multiple systems across the organization
- Compromise of the device/application, leading to persistent threats against all systems and data access on that device, application, and the other systems they are connected to
- Loss of integrity and confidentiality, leading to the loss of financials, brand reputation, and customer loyalty

In the next section we will look at the inherent risks of any email system by exploring the key components and provide a thorough understanding of the multiple points of attack that can lead to a compromise.

Inherent risks of email systems

Email system

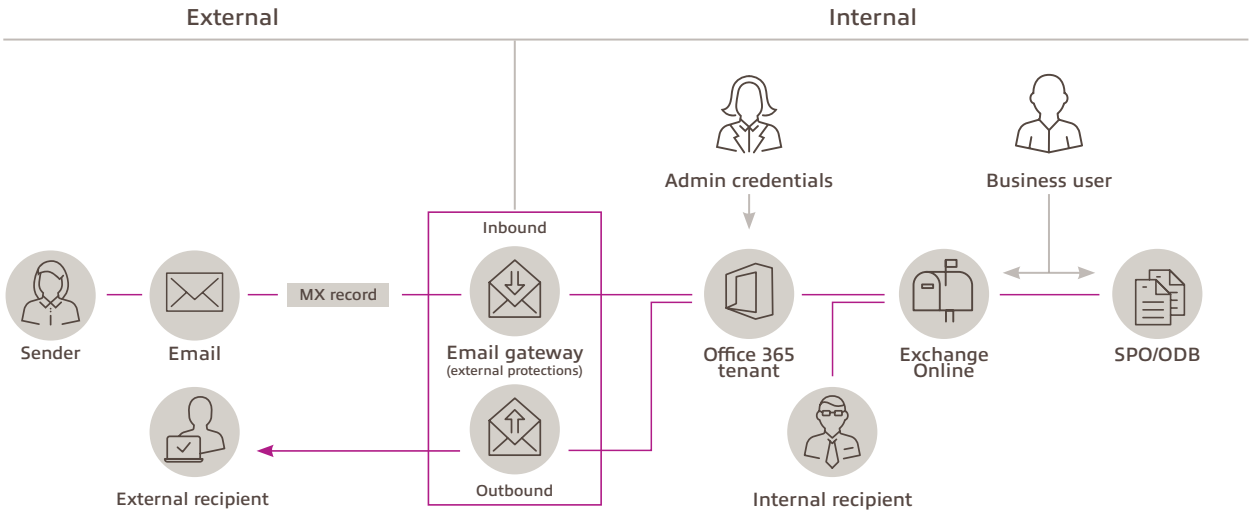
In order to understand the risks, we need to explore the key components of every email system.

This diagram provides a high-level view that will be referenced throughout this document.

For the external components, every email has a sender and a recipient. This information can be inspected to ensure domain reputation and authoritative source details.

The DNS MX record is also a key component for the correct routing of email to the inbound gateway of the organization's email system.

The email gateway is the first line of defense for all inbound email and should also scan for malicious activity for any outbound email.

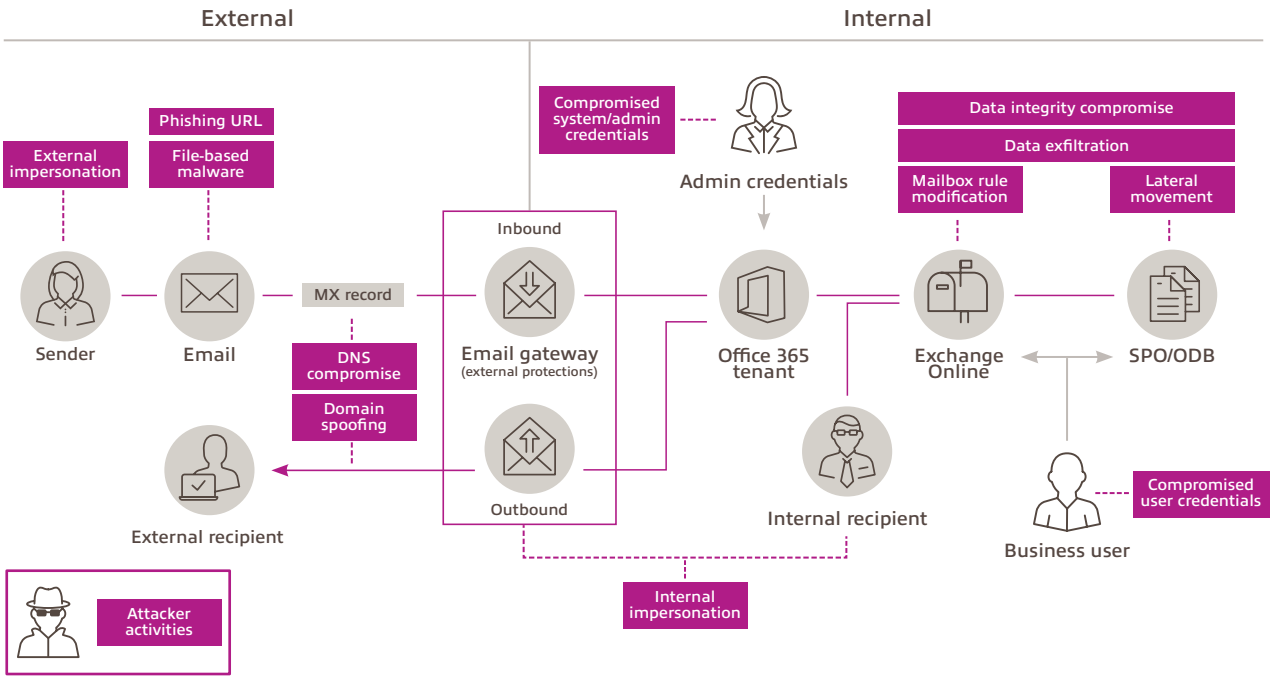


The internal components consist of an email exchange solution that provides routing information and storage for the email and attachments. Identity and access management is critical here to ensure the appropriate authentication and authorization for access to the email exchange system, via the mailbox.

Inherent risks

Addressing each component in the system allows identification of risks at each stage, to understand the potential threats and mitigations.

These threats and risks will be further explored in the following pages of this section.



External threats and risks

External impersonation | Phishing URL | File-based malware | DNS compromise | Domain reputation | Domain spoofing | Propagation of attack | Damage to brand/trust

Email-based attacks are an issue for organizations of all sizes, and even the most advanced defenses can be circumvented by tricking a user through social engineering. Training remains a critical part of the solution, ensuring your people can identify and report suspicious activity and potential compromises.

The phishing URL and file-based malware attacks are the most common and successful, but also have the widest range of solutions available to combat this well-known attack vector. Impersonation and spoofing attempts are becoming more sophisticated and realistic, but can be detected and mitigated before they reach the mailbox, or very soon after. The hardest attack to thwart is when the email is sent from a legitimate mailbox at a trusted domain.

DNS compromise is less common, but more devastating. If an attacker can modify your MX records, they could redirect all inbound and outbound email to their own servers for inspection and manipulation.

Reputational attacks, such as domain spoofing, may occur with no visibility to your organization as it does not rely on malware to attack your systems. You will not see the impact of attack until you are made aware of it by your customers and business partners. They may have had weak email security and been successfully phished by an email that they believe came from your domain. This usually results in financial loss for that organization, and has the potential to interrupt your business workflow as they attempt to recover their losses and repair the damage.

If the breach results in email being sent out from your legitimate domain, to your partners and customers, then the attack can be extended to their email systems. Any damage extended to them will likely cause damage to your brand reputation and trusted partnership. Domain reputation damage (such as blacklisting) could also occur if the domain is reported for adversarial activities.

Internal threats and risks

Internal impersonation | Compromised system/ admin credentials | Compromised user credentials | Data integrity compromise | Data exfiltration | Mailbox rule modification | Lateral movement | Damage to brand/trust

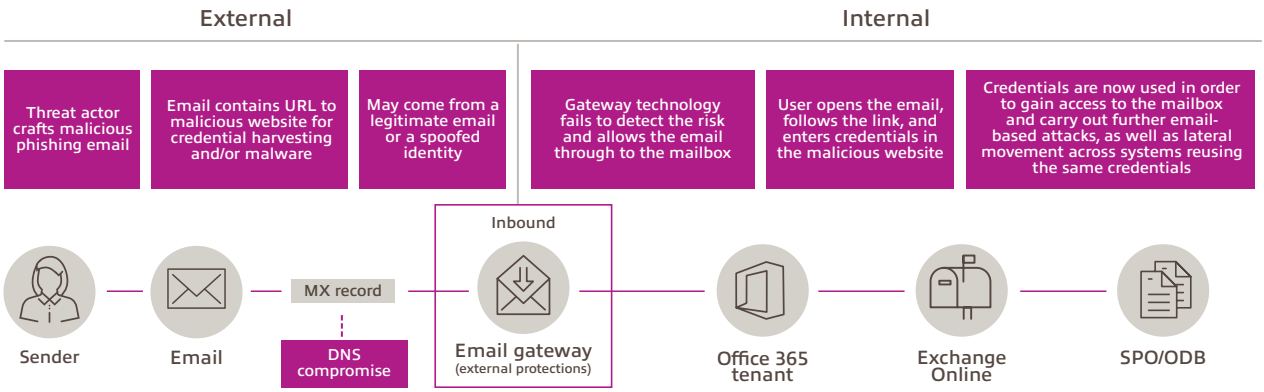
These attacks follow from the initial successful compromise of the email system, or may have originated from another source, and directly impact the user's credentials (identity), device and operating system, or applications (malware). An attack can be further propagated through the email system or connected storage solutions and other trusted systems.

The impact of a successful breach may be felt immediately, or may go unnoticed for a long period of time, whilst the attacker carries out surveillance and reconnaissance to collect and exfiltrate your data. By the time the malicious actions are taken, the attacker may have been inside and breached the system for several months.

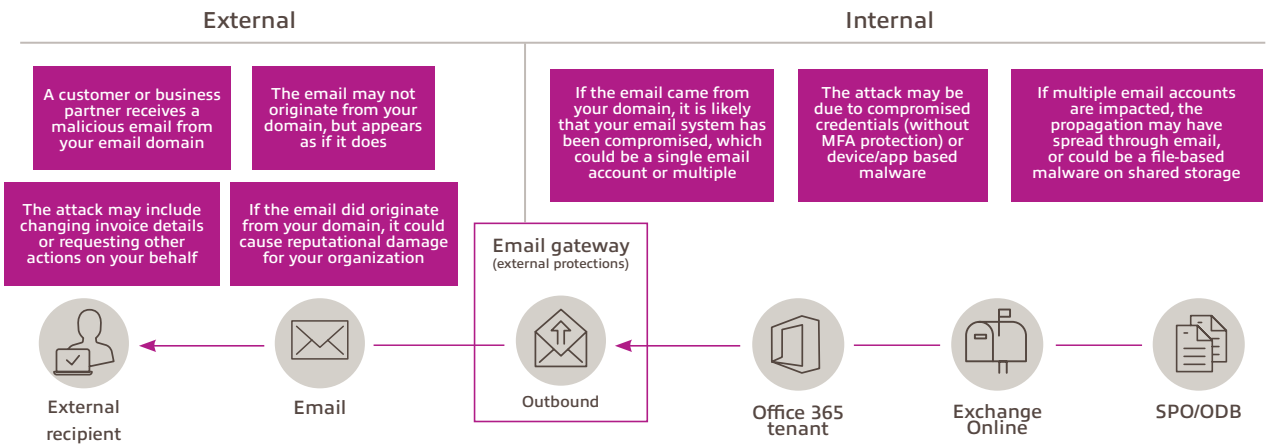
One technique used to remain undetected is the use of mailbox rules to divert incoming email to a hidden folder, instead of the inbox folder, to allow the attacker to view the email before they place it back into the inbox folder (or delete it). Email sent from the compromised mailbox can also be hidden from the legitimate end user by intercepting any responses and deleting any evidence of the conversation thread.

Gaining any level of access to the systems internal to your organization, the likely outcome is exfiltration of sensitive information or ransom demands. Gaining access to privileged access accounts, such as system or delegated admin, enables the attacker to gain full control of the target environment and do a lot more damage.

Example 1: Inbound email



Example 2: Outbound email



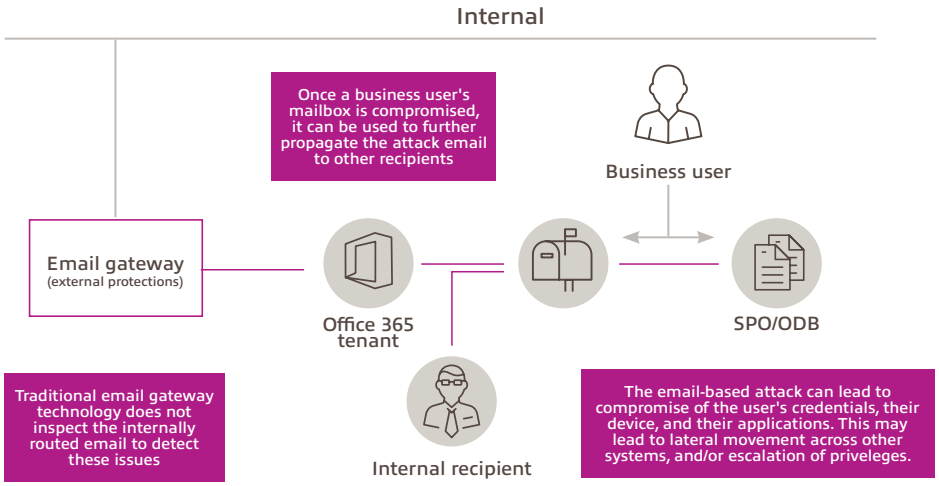
Example 3: Internal email

Internal threats may come in many forms, and are usually the result of a successful attack through inbound email.

Detection, isolation, and eradication of these threats need to be planned for and tested on a regular basis to minimize the impact and reduce the potential exposure of any successful compromise.

Additional components that need to be protected, not shown here, include the devices, operating systems, browsers, and applications used to interact with email.

A fully layered defense strategy will incorporate these components to prevent them from becoming additional threat vectors, and minimize the potential for malware to compromise them, should all other layers of email defense fail to prevent the malware getting through the email system.



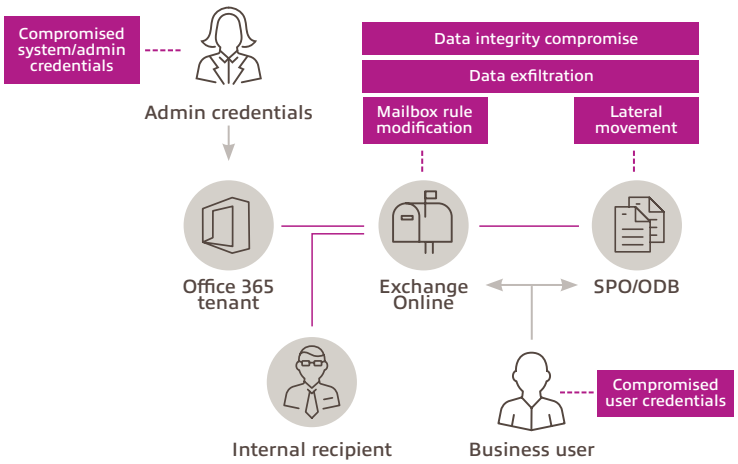
Other scenarios

These scenarios show some of the risks following a successful breach through any of the other scenarios, or from other types of compromise.

Email isn't the only way of getting into an organization's systems, but it is the most successful. Email is also a target for finding sensitive information that may otherwise be protected, and to launch attacks internally and externally.

Once compromised, the attacker may learn more about your networks, systems, processes, and organization structure, in order to move laterally between systems and potentially escalate privileges into other organizations.

In the next section we will explore the solutions and strategies required in order to protect, detect, and respond to these types of threats.



Strategies and solutions

Email security strategy

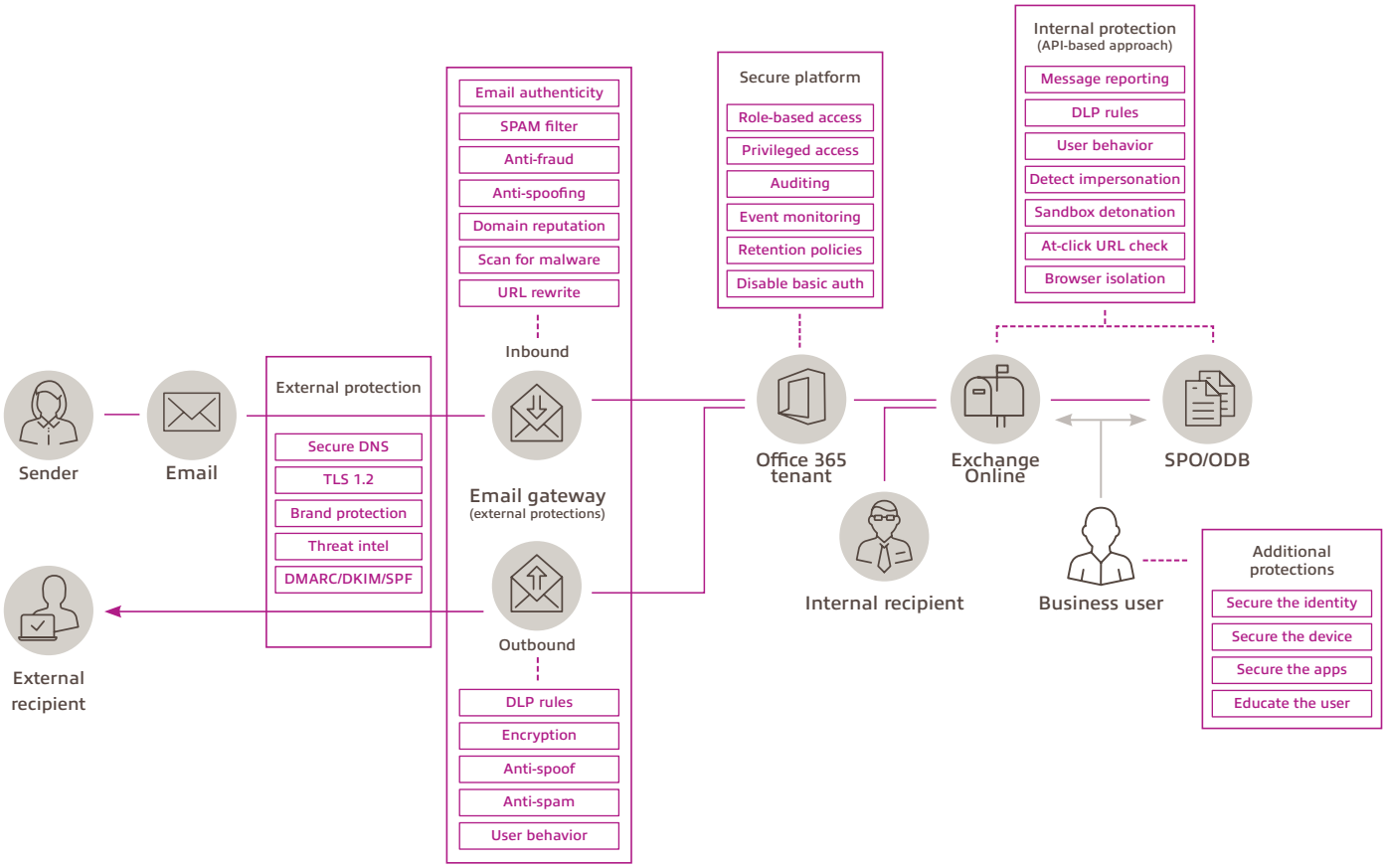
This section will explore the multiple layers of defense available to mitigate the threats and risks that have been discussed previously in this document. The intent is not to encourage you to purchase more solutions, but to use this information to assess your current security strategy against today's threats, then carry out a gap analysis for your deployed solutions and processes. You may use this information to review potential solutions in order to make investments in future technologies and strategies that will make a real difference to your security posture.

The best approach is to apply controls and defenses at each layer of the email system, to protect from all attack vectors:

- Let's say you decide to focus all efforts on just one specific solution, such as identity, and fully deploy multifactor authentication. Your system will remain vulnerable to other threats that can circumvent these controls. For example, if the device has malware installed and the user carries out multifactor authentication, the malware could use the authenticated token for malicious intent without the system or user noticing any suspicious activities (such as mailbox rule manipulation and sensitive data exfiltration).
- Scanning for malicious intent is the first line of defense for email-based threats, followed by isolation of the execution environment to protect from the eventuality that something is likely to get through all the other layers of defense (a posture of assume breach).
- Monitoring the logs and carrying out user behavior analytics, is fast becoming the de facto standard approach to hunting threats that may already exist in your infrastructure.

Layered protection

The solutions can be divided into logical groups based on the focus of the area of attack. These will be explored in the following pages.



External protections

It is important to ensure your domain(s) are protected from threats that may impact your brand reputation. These are some of the fundamental email security steps and best practices that can be deployed to ensure protection against common attacks even before an email is sent to, or from, your domain:

- Securing access to your public facing and internal DNS records will mitigate any unauthorized modifications and domain ownership issues.
- Understanding and implementing standards, such as DMARC, DKIM, and SPF, is key to enabling greater trust between legitimate email domains, but can only be as good as how well they are adopted from all parties.
- Require/enforce Transport Layer Security (TLS) between partner organizations to disable opportunistic TLS. This mitigates the risk of any plain text communication sent to and received from external email partners.
- Services are available to carry out investigations for dark net credential and compromise research, to ensure vulnerability scanning for configuration and health status, and for intelligence about potential malicious intent targeting or evidence of brand spoofing attempts against your customers.
- Define communication policies with your customers and partners to ensure the potential of a rogue email (spoof/impersonation) does not lead to modification or release of sensitive information. If email cannot be secured end to end (both parties have responsibility here), then you must have alternative methods for sharing critical changes, such as the modification of invoice/bank account details or the provision of PHI/PII.

Boundary protection

The first line of defense against email-based attacks for your organization is to implement boundary protection services that focus on scanning every email, using threat intelligence, and advanced heuristics to prevent the threats being sent or received.

These defense technologies may be built into the server or email service by default, or they may be provided by a third-party solution such as an email gateway. Below are some of the key capabilities of these services:

Inbound email

- Only accept email from trusted sources
  - DKIM/DMARC/SPF/TLS
- Check inbound email for authenticity/trust
  - Domain validation/certificates
  - Detect spoof and impersonation attempts
- Content filtering for SPAM and malicious content
  - Detonate URLs and scan for malicious intent
  - Rewrite URLs to enable scan-on-click
  - Detonate attachments in a sandbox environment
- Validate content sensitivity and apply appropriate controls

Outbound email

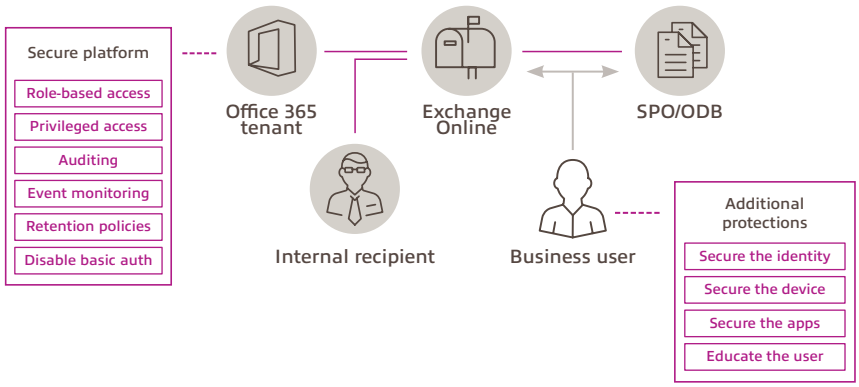
- Prevent outbound SPAM by limiting send rate
- Prevent spoofing and fraud attempts
- Use Data Loss Prevention (DLP) rules to abide by content sharing policies
- Use behavior analytics to detect unusual activity
- Ensure encryption is enforced for all sensitive communications (or apply to all communications)

Secure configurations

Securing the email platform is a fundamental step to reduce the risk of compromise at the system level, including privileged access to modify controls or gain unauthorized access to sensitive information.

Each platform will have a variety of control options, which should be enhanced with any additional services offered by the provider, or by third-party solutions, especially for Privileged Access Management (PAM) and alerting for unauthorized modifications:

- Review all permissions granted at system and per-mailbox level
- Enable auditing for all system and mailbox activity
- Enable retention and deletion policies to ensure integrity of information
- Govern all user access to their mailbox with strong controls:
  - Enforce strong authentication practices and policies
  - Ensure the security and compliance of the device and applications used to gain access
- Limit system administrator access based on the most restrictive policy:
  - Identity — using strong authentication practices and policies
  - Devices — only use trusted, managed, and compliant devices
  - Networks — restrict based on trusted locations (known IP address, VPN clients)
  - Applications — ensure secure protocols and authentication methods are used



Internal protections

Human error will always be a factor to consider in any IT system; a simple error can lead to devastating consequences. For advanced email protections we need to look at ways of detecting unwanted behaviors or suspicious activities. All activities are recorded in the logs of each component in the email system, which can be interrogated and compared to known attack types or searched for pattern-based heuristics that can assist with hunting for unknown threats. These solutions may apply checks to the emails before they enter the inbox, or afterwards. Automated remediation ensures new threats can be detected in existing email, as well as new, and removed.

As a final layer of protection against malicious websites and attachments, that have evaded all other detections and are still able to launch, there are now solutions available to provide an isolation platform which will allow them to be launched remotely and only send back safe content to the client browser. This type of protection will prevent a user from entering their credentials into phishing sites, or allowing malicious code to execute on the client device for malware infection or system modification and compromise.

To protect business critical information, implement information protection solutions that will identify sensitive information and apply protections automatically, such as DLP rules and file-level encryption. This will prevent information being sent outside of authorized boundaries, and if the information is leaked, the encryption stays with the file and can prevent unauthorized access regardless of where the data is stored.

Training and awareness

With social engineering still favored as an entry point past many security systems, it is imperative that we educate everyone on the risks of falling for this type of attack, and how to identify it.

Identify procedures where it might be possible for a single person to carry out a change to procedure, or modification to a system, without the oversight of governing controls to prevent both accidental and malicious activity:

- Example: If email is used to request funds be transferred to a new account, ensure the account details have been verified by someone other than the requestor. This would prevent the common attack where a spoofing email is sent and the recipient doesn't challenge the request by talking directly to the real person, or validate the information through a secondary process before carrying out the action (too much trust in the email alone).

Social engineering attacks won't only be sent via email, they can originate from telephone calls, social media, messaging apps, and even direct influence from real people that have made their way into a place of trust. More advanced attacks will include multiple methods to further trick the person into believing it is a legitimate request and navigating them to carry out malicious actions directly.

One successful way of increasing organization-wide awareness is to carry out self testing with professional security experts that will help identify weaknesses in physical security as well as social engineering, and systems access testing. Let your people know that it is okay to challenge and verify anything they find even slightly suspicious.

Review and recommendations

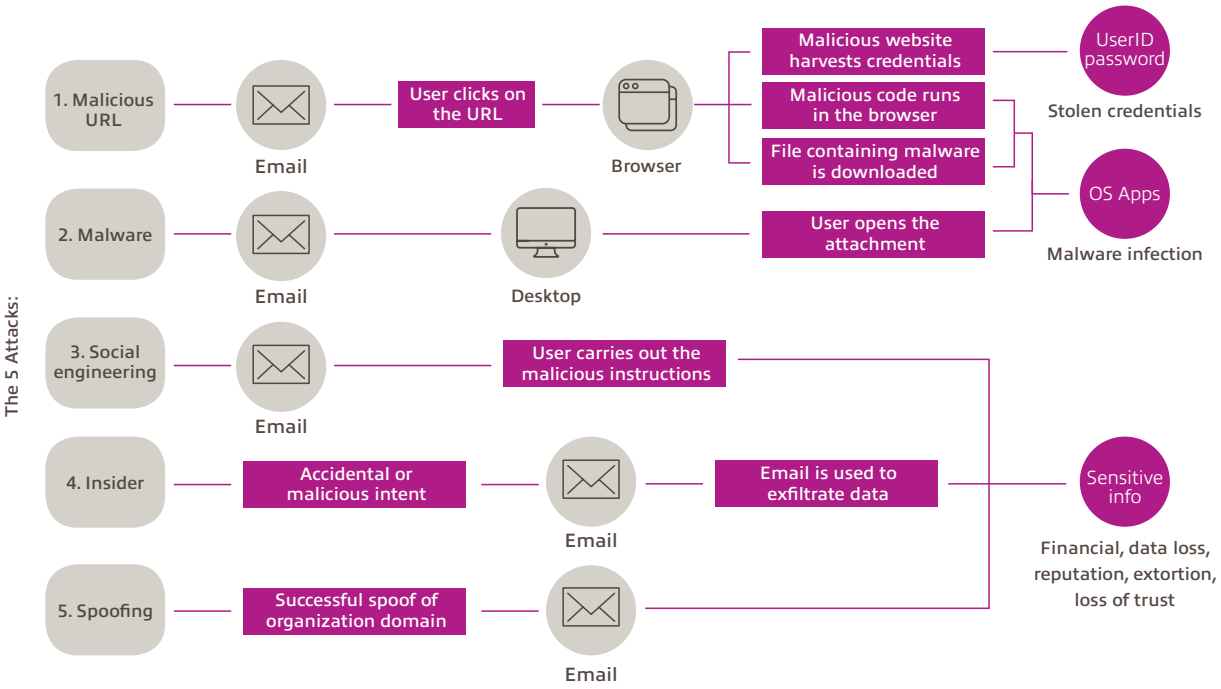
Although email security is a technical topic, this really is a key business risk that must be addressed by the whole organization. A combination of education, awareness, and vigilance, supported by advanced security technologies, can mitigate and reduce the impact of a successful email-based attack.

In terms of the types of attacks, many phishing attempts are generic enough to try to fool anyone and are not targeted specifically at your organization or users. The rate of success is staggering, however, once detected they can be quickly isolated and mitigated; if you have planned for the event and react quickly enough.

Targeted attacks, using social engineering, whaling, and insider attacks, are the ones that lead to the greatest financial loss. The costs come from a range of issues that follow the immediate impact: productivity impact due to systems outage, loss of customer loyalty, fines and payouts, cost of implementing urgent security solutions, and recovering from any damages (including legal and reputational).

This section provides a summary of the attacks and the corresponding strategies and solutions you need to deploy in order to protect, detect, respond, and recover from email-based attacks. Use this information to ensure you are able to prevent this kind of devastating impact to your organization and recover quickly should a successful breach occur.

Over the next few pages we will review the five attack types from Section 1, and show how each type of attack can have multiple layers of defense and detection.

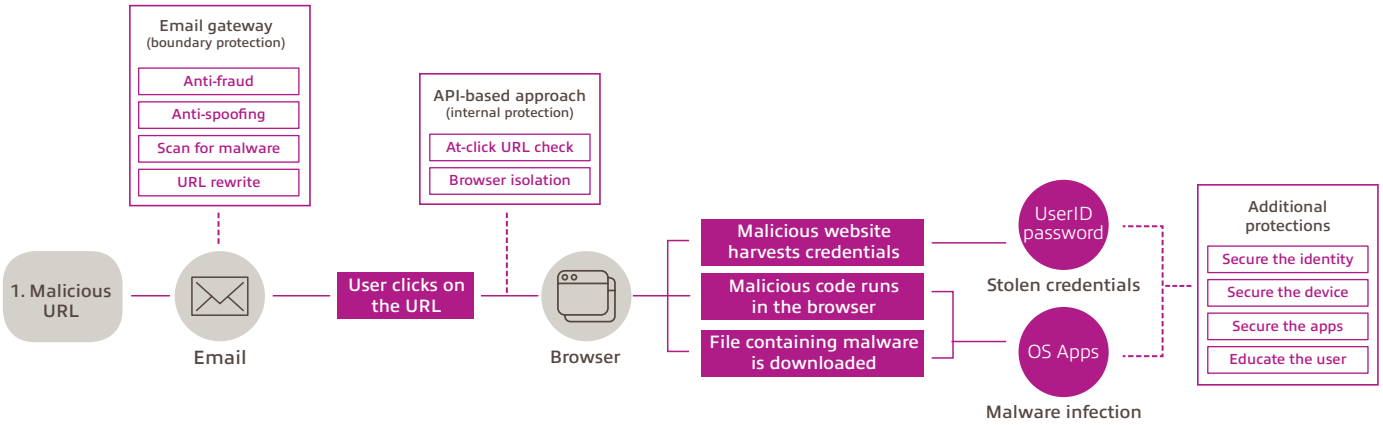


Attack 1 — Malicious URL

Standard email hygiene solutions will check all inbound email for the potential of fraud, spoofing, and malware, as well as rewriting the URLs to redirect the browser to a security service for validation prior to forwarding on to the legitimate website (at-click protection). Malicious URLs are constantly evolving to evade detection, and may even come from a legitimate website that has been compromised, so there is a need to apply additional layers of protection to combat this eventuality.

As it is likely that some will make it through the gateway defenses, or the user may end up on the malicious site via other means (look up watering-hole attack), it is very important to also protect the user identity, the device, and the applications that are allowed to gain access to the email system. Advanced identity protection solutions will detect the misuse of credentials and reduce the attack surface by disabling legacy authentication and protocols, such as IMAP and POP.

The last line of defense is to use a browser-isolation service. This will ensure all potentially malicious sites are run in a safe environment, preventing the user from entering their credentials and other sensitive information, or allowing scripts and other threats to run on the local device.

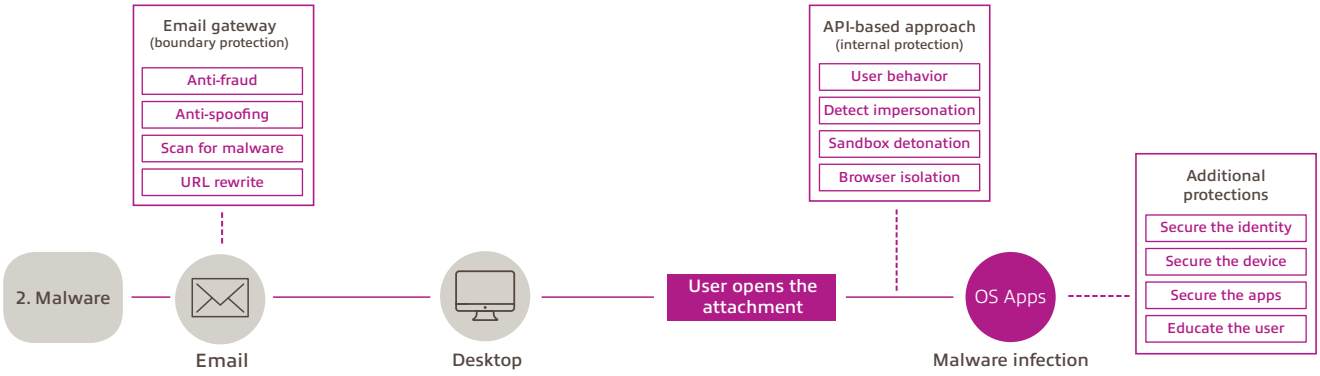


Attack 2 — Malware

Standard email hygiene solutions will check all inbound email for the potential of malware using a variety of approaches such as signature detection (known attacks) and sandbox detonation (unusual behavior detection).

Malware is constantly evolving to evade detection, and when combined with social engineering, it is very likely an attachment will be the cause of device/application compromise, so there is a need to apply additional layers of protection to combat this eventuality.

As it is likely that some will make it through the gateway defenses, or the user may end up executing malware from other sources (USB, cloud storage, social media, etc.), it is very important that we also protect the user identity, the device, and the applications that are allowed to gain access to the email system. Sandbox and containerized services can ensure all potentially malicious attachments are run in a safe environment, preventing the scripts and other threats running on the local device.



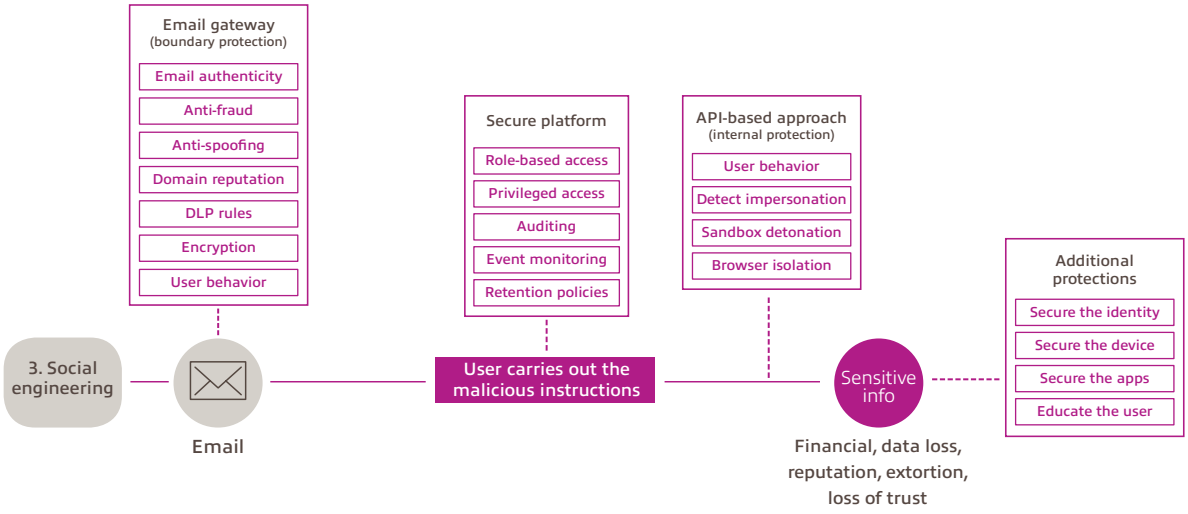
Attack 3 — Social engineering

Security awareness training is critical to ensure your people know how to spot a potential attack. This investment will not only protect your organization, but also provide defenses against attacks in their personal lives.

Prevention is the first stage of defense; email security solutions need to analyze email to detect multiple types of behavior that can lead to compromise based on social engineering techniques. However, this is a hard problem to solve and will eventually lead to compromise, so we must be vigilant in applying the other layers of protection to mitigate the impact of a user falling for a social engineering attempt, which may include follow-up attack techniques such as a phone call or social media request.

Consider implementing email encryption policies to protect sensitive information exchanges between trusted parties.

Also, review procedures to ensure email isn't a single point of failure in the authentication and authorization of major business transactions.

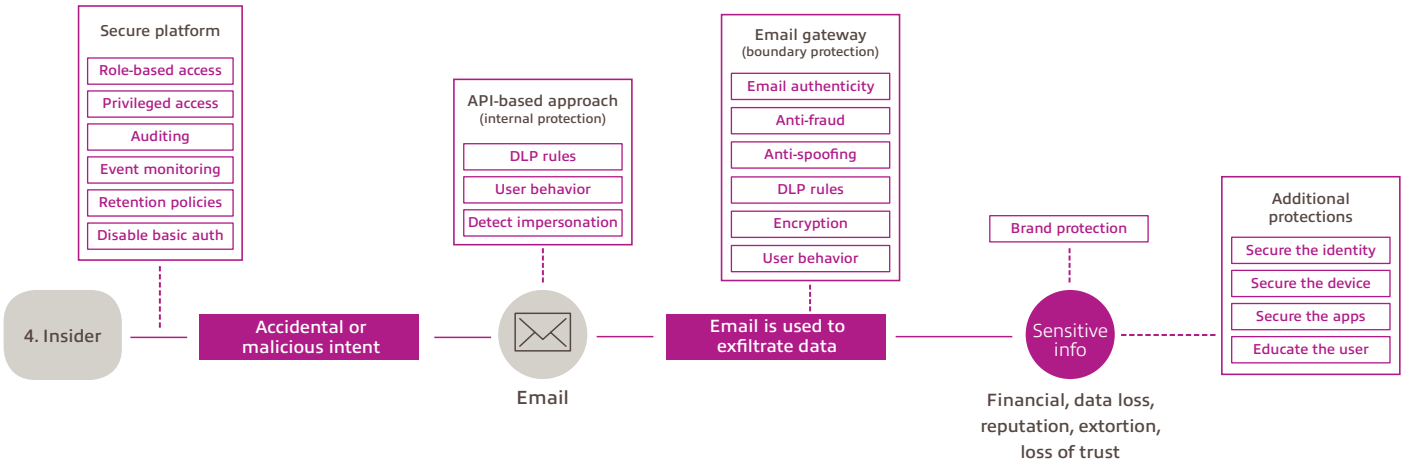


Attack 4 — Insider compromise

This attack may be the result of one of the first three attack types; leading to compromised credentials and/or malware infection. In a worse-case scenario, it could be a legitimate insider attack (imposter/infiltration).

Detection is based on monitoring user behavior to detect changes against a baseline standard, or known techniques (such as the creation of new mailbox rules). Looking at the way a user interacts with the systems, by accessing information that is not relevant to their job role, or roaming between multiple systems until they find the sensitive information they are looking for and then exfiltrating and/or destroying it.

Damage can be limited by implementing role-based access, data retention and deletion policies, DLP rules to control information flow, and encryption to prevent unauthorized sharing and exfiltration.



Attack 5 — Brand/reputation

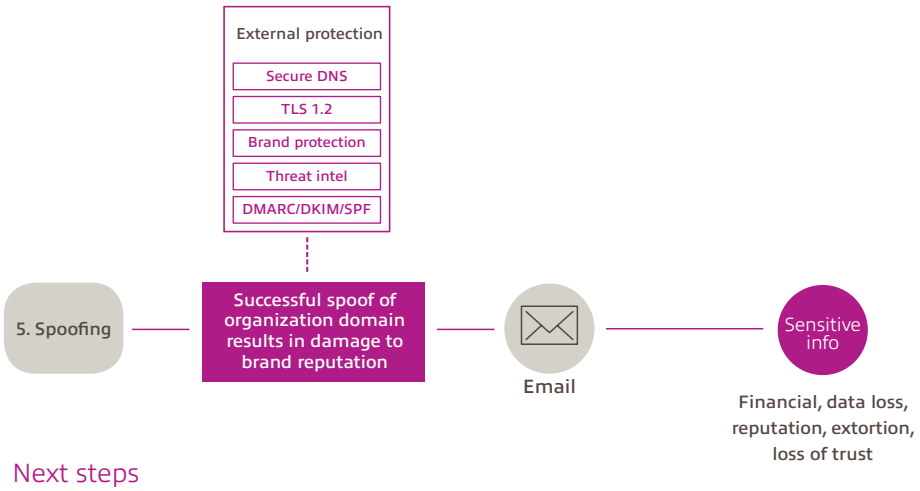
This attack type may used as part of social engineering, or a supply chain attack, and is possibly one of the most difficult to protect from, detect occurrence of, and respond effectively to.

Implementing email domain security solutions, such as look-a-like domain scanning, is a starting point, as well as enabling secure communications through OME, TLS, or S/MIME. Advanced protections include information rights management for email/attachment encryption.

For proactive protection consider the use of services that will use threat intelligence to discover activities that may make your organization a target, or provide evidence of active attacks using your brand. Responding to identified attacks requires a strong communications plan that ensures you can contact all your customers quickly and effectively to mitigate the potential damage.

If your organization is impacted due to an attack of this nature, you may need to work with specialists that will help resolve the issues faster and reduce the potential loss.

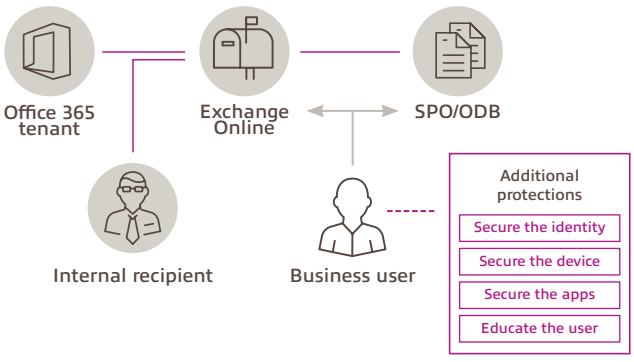
It is better to plan for this attack upfront, instead of reacting at the last moment.



Next steps

There are many ways to evaluate solutions to ensure you are gaining value and efficacy. Use the information in this document to really evaluate what the new solution or methodology is solving for, and where the gaps are.

- Look for holistic platform solutions that span email, endpoint, and web protection:
  - How effective is the solution at solving the problems (ask for a real-life demonstration scenarios)
  - What integrations do they offer, and how easy are they to deploy and operate
  - Look at the company's history in security; are they just building a product, or do they have extensive security credentials
  - What is the source of their threat intelligence, and can you subscribe to additional feeds (bring your own)
  - The best solution for your needs might not appear on the industry reports (such as Gartner and Forrester)
- Don't forget about defense in depth:
  - Securing the user identity is a critical step in mitigating lost credentials
  - Implement MFA as a matter of urgency
  - If the device is compromised, and allowed access to the mailbox,all bets are off
  - Control which methods of access are acceptable, and where your organization's data can be stored or sent
  - Constant education, awareness, and a security culture will go a long way towards defending from future attack types we haven't seen yet



Summary

The following recommendations are a good starting point for improving your security posture for email-based attacks. Many of these defenses will help extend to other types of attacks:

- Enforce conditional access policies for all users, including enforced multifactor authentication for sensitive access
- Disable access based on legacy authentication protocols and old email clients (IMAP and POP)
- Look for system weakness, such as default open relay connectors and the misuse of mailbox rules
- Review the security solutions you have already deployed, assess the maturity, plan for improvements
- Enable continuous monitoring of the email system to detect anomalous behaviors
- Run a free scan, offered by one of our partners, to see if any existing threats exist in your system
- Review the incident response readiness program to account for these types of attacks and impacts
- Assess and remediate process failures, prevent email being a successful attack point for social engineering
- Develop/improve awareness training, create your own phishing campaigns, help people identify this in their home lives as well as at work

If you need help implementing any of these solutions, please reach out to Insight for:

- Mastering Email Security Workshop
- Microsoft Office 365 Security Health Check
- Cloud Security Consultation
- Free email health-check scans

We hope this information was useful, thank you for taking the time to read it, and we welcome your feedback to improve future versions.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com