Whitepaper

mimecast

Danger within: email and security awareness training strategies for effective account takeover protection

Inbound malware, phishing and impersonation attacks are often the primary focus for IT security teams, but organizations also require an inside-the-perimeter strategy for rapid remediation of internal threats.

Executive summary

It's a common misconception that email-borne attacks come only from outside the organization. While most attacks start from the outside, attackers will typically look to land and expand once they are inside. One way they gain this foothold is to use account takeover, compromising a user account to send internal emails, spreading the attack laterally to others in the organization, or even outbound to trusted external contacts.

Meanwhile, the attack surface of organizations is increasingly expanding to the cloud. Cloud email services, notably Exchange Online in Microsoft 365 (Office 365) and G Suite are becoming the de facto choices for organizations of all sizes. The global pandemic is accelerating this adoption as organizations are forced to make pragmatic decisions about business transformation, cost and risk.

Many employees are now also working from home, often for the first time, and cloud tools are a readymade option to keep workers productive and looking after customers. Cybercriminals are also refocusing their phishing, impersonation and ransomware attacks from office networks to the cloud services remote employees use from home.

In most cases, without their knowledge or understanding, employees play an integral role in attacks by sending an attacker's emails to others in the organization. However, malicious insiders do exist, and many of the same techniques can be used to detect and limit their ability to cause harm.

Human error lies at the heart of most successful attacks, but data or financial loss rarely occurs immediately with a single click. Business Email Compromise (BEC) scams most often comprise of a series of emails as confidential "Crown Jewels" data is often guarded by a series of gatekeepers. Supply chain attacks depend on first penetrating one organization to then expand and land into another.

For these reasons it's clear there is a need for a strategy that combines email security and awareness training for effective account takeover protection. By bringing together defenses and intelligence across multiple security layers, organizations can overcome the lack of visibility of internal and outbound email threats, detecting attacks that are underway and take action to stop them before completion, or educate users to prevent compromised accounts in the first place.

Email remains the single easiest way for an attacker to break into your network and it's vital that organizations prioritize adding more security layers on top of cloud email services like Microsoft 365 or G Suite. This paper will explore the threat in more detail and suggest a comprehensive email security strategy to address both the human and technical risk areas.

Ask Yourself

How susceptible are your employees at discerning an impersonation email or email attack using a legitimate internal account?

What open and click rate would your organization expect?

Email security threat landscape

Cybercriminals and other malicious actors use phishing, social engineering and brand impersonation techniques to steal login credentials and compromise email accounts. Email account takeover allows hackers to then monitor and track activity, learning how individual employees do business and the way financial transactions are handled.

According to the **fourth annual State of Email Security report by Mimecast**, 43% of respondents said the volume of internal threats or data leaks had increased in the prior 12 months. It also found that 60% of respondents' organizations were hit by an attack spread from an infected user to other employees. Infected email attachments were the most common method with 42% of these cases, 30% were via infected links within emails and 17% via instant messaging applications

60%

Of respondents' organizations were **hit by an attack spread from an infected user** to other employees

43%

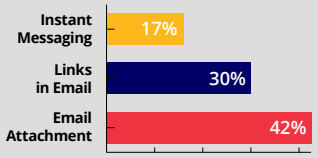
Of respondents said the volume of **internal threats or data leaks** had increased

30%

Increase of impersonation fraud in the first **100 days of COVID-19**

Internal attack patterns

Attack vector used where malicious activity has spread from one infected user to others.



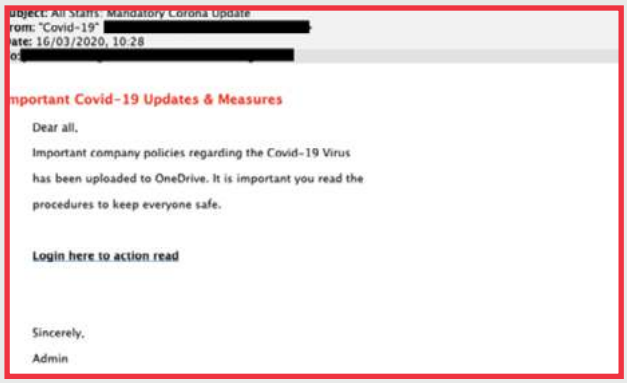
Traditional email security mechanisms focus on detecting malicious links and malware but many of these attacks evolved to simply hoodwink target employees to carry out the will of the attacker. Once compromised, attackers can launch subsequent phishing attacks inside the organization and wider supply chain, including harvesting financial information and additional login credentials for other accounts.

During the pandemic, threat actors pivoted their tradecraft using Covid-19 phishing and impersonation lures to land hits on vulnerable organizations. The Mimecast Threat Center found that impersonation fraud increased by 30% in the first **100 days of COVID-19**.

A 2019 Tech Validate survey reported, in the previous 12 months, over half of respondents had suffered from threats caused by attackers compromising their users email accounts.

"All Staffs" Mandatory COVID-19 Update Email

This sample, sent to a US recipient, attempted to steal credentials by linking to a ***OneDrive*** login page, presenting as an essential safety related policy change. Given the extent to which workforces are working from home, perhaps even for the first time, this would be a plausible and effective lure.



"All Staffs" COVID-19 Update Email

Landing Page

The availability of phishing kits and an "as a service" phishing model has democratized phishing. In a 262-day period, Microsoft was the top targeted brand with 62 kit variants found across 3,897 domains, **according to Akamai**. The result of this is highlighted in a **Microsoft study**, which reported 44 million Microsoft and Azure cloud account holders were using passwords that had been compromised in data breaches.

As 'Insider' threats increasingly feature inbound and outbound attacks on services external from the office network, organizations require a whole new model of threat detection and remediation.

Credential phishing account takeovers

Access to cloud mailboxes and other services, are controlled using credentials, most commonly a username and password. In account takeover attacks, adversaries aim to steal or guess those credentials so they can sign in as the original user and perform illicit actions. For example, once a user's Microsoft 365 credentials are compromised, the attacker can access the user's Microsoft 365 mailbox, SharePoint folders, or files in the user's OneDrive.

Once an account is compromised, an attacker often begins by monitoring email traffic to learn more about the organizational environment, individuals – ultimately looking for opportunities to steal money or confidential data. In advanced attacks, they may aim to drop (install) malware in order to gain persistent access to a user's system.

Attackers may begin sending emails as the original user to recipients both inside and outside of the organization. They may seek privileged admin users, those responsible for financial transactions or guardians of "Crown Jewel" data assets. Valuable supply chain partners may also become a key target as they extend their attack. A data breach will occur when the attacker emails confidential data to external recipients, or exfiltrates it by other means.

Consequences of an attacker obtaining access to a user's email account include:

1. Any second stage attack is more likely to succeed, internally or externally to business partners and customers, as the email came directly from a trusted sender.
2. Gateway email defenses alone have no visibility of the compromised account or internal emails that are sent from it.
3. Sensitive information can be sent by email to external recipients, resulting in data breach.

Password reuse warning

Phishing attacks are made even more dangerous by poor password policies and lack of employee training. Password reuse is all too common and results in compromised business credentials through attacks that phish for personal credentials where technical and human controls are often weaker. A **Google survey** found that 52% of people use the same password for multiple accounts . This problem could be mitigated by use of multi-factor authentication, but according to a **Microsoft blog**, less than 10% of their customers use it.

Spear-phishing usage by high-profile malicious actors

It was **revealed in July 2020** that APT29 (also known as 'the Dukes' or 'Cozy Bear') was using custom malware to target a number of organizations globally, including those involved with COVID-19 vaccine development. The UK, US and Canada's national cybersecurity agencies all assert this cyber espionage group is 'almost certainly' part of the Russian intelligence services

Alongside specific customer malware used by the group, the report highlight how "The group also uses spear-phishing to obtain authentication credentials to internet accessible login pages for target organisations."

52%

of people use the same password for multiple accounts

Cloud email account takeover

The rapid growth of cloud services, notably collaboration suites Microsoft 365 and G Suite, is fundamentally changing the organizational attack surface, creating new risks of account takeover.

Microsoft 365 (rebranded from Office 365 in April 2020) encompasses not only Microsoft Exchange, but also Teams, SharePoint, OneDrive, and other popular enterprise tools. Even through the onset of the pandemic, **Microsoft reported** strong constant currency 'Office 365' revenue growth with 27% in Jan-March and 22% in April-June 2020.

Microsoft also regularly tops the list of brands that hackers impersonate the most in phishing attack attempts. **One study** by Vade Secure's ongoing research detected an average of more than 222 unique Microsoft phishing URLs per day.

In April 2020, the FBI put out a **specific warning (pictured)** highlighting the growing risk to cloud services as threat actors have realized they are a gold mine of information. Between January 2014 and October 2019, the FBI's Internet Crime Complaint Center (IC3) received complaints totaling more than $2.1 billion in actual losses from BEC scams using 'two popular' cloud-based email services.

Some organizations try to rely on these vendor's security and data protection alone. However, the security efficacy of the cloud email providers has proved sub-optimal against advanced phishing attacks and even the most basic anti-spam management. For example, Microsoft has been rated poorly by independent analyst firms, and Mimecast testing shows that their efficacy is not comparable.

According to the SE Lab's **Email Security Services Protection report** from March 2020, both Microsoft 365 and its Advanced Threat Protection service received a 'C' security rating in its detailed testing and analysis. G Suite Enterprise received an 'A' and G Suite Business a 'B'. These are compared to a number of third-party security services scoring AA and AAA ratings.

FBI ALERT – APRIL 2020

"Cybercriminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds."

Beware the cloud security monoculture

Defense-in-depth security best practice prescribes using multiple layers of security, and architecturally these also need to be in the cloud to effectively work alongside your Microsoft 365 or G Suite service.

A new risk is also created when moving primary email systems to the cloud as adversaries can hone their attacks against a 'security monoculture.' Exchange Online is a single, large target for attack and we know cybercriminals often test their campaigns against their own tenant environment (,i.e. a mirror of your environment), before retargeting against their real victims.

A single cloud service can represent a greater risk exposure if you flatten all your protections, services and applications into one dependent system. You're also outsourcing control of that risk to Microsoft or Google.

Without additional risk mitigation, dependency on the security, availability and immutability of this single cloud data store can become your Achilles' heel.

Email Account Takeover Symptoms

Account takeover is so common that Microsoft has produced a **detailed list of symptoms** on its website for Microsoft 365.

These include:

- Suspicious activity, such as missing or deleted emails.
- Other users might receive emails from the compromised account without the corresponding email existing in the **Sent Items** folder of the sender.
- The presence of inbox rules that weren't created by the intended user or the administrator. These rules may automatically forward emails to unknown addresses or move them to the **Notes**, **Junk Email**, or **RSS Subscriptions** folders.
- The user's display name might be changed in the Global Address List.
- The user's mailbox is blocked from sending email.
- The Sent or Deleted Items folders in Microsoft Outlook or Outlook on the web (formerly known as Outlook Web App) contain common hacked-account messages, such as "I'm stuck in London, send money."
- Unusual profile changes, such as the name, the telephone number, or the postal code were updated.
- Unusual credential changes, such as multiple password changes are required.
- Mail forwarding was recently added.
- An unusual signature was recently added, such as a fake banking signature or a prescription drug signature.

Multilayered-layered email security strategy

To better respond to account takeover threats, we need to re-think how and where we deploy technical email security controls and how they integrate with procedural controls, such as employee security awareness training.

There are three core areas for email security controls:

1. **At the email perimeter –** enforcing security controls at the point of entry or exit of the organization or of the email platform. e.g. traditional secure email gateways
2. **Inside the perimeter -** security capabilities focused on applications, systems and people that are internal to the organization, including cloud/SaaS-based emails services.
3. **Beyond the perimeter –** the wider internet that is beyond direct control of an organization's IT and security teams, but where cybercriminals develop and host many of their attacks. e.g. Spoofed websites used to attack your employees, partners or customers

Controls across all three areas systems can be connected through API data integrations and automation to each other and more widely into an organization's other security systems. E.g. SIEM/SOARs. This combined approach allows organizations to overcome the lack of visibility of internal and outbound email threats, detecting attacks that are underway and take action to stop them before completion.

While this paper is focused on inside the perimeter controls, you can read more on the other areas **here**.

Inside the perimeter

Email security controls inside the perimeter can help detect abnormal behaviors, identifying compromised accounts and insider threats. Additional direct integrations with Exchange and Office 365 allows organizations to detect and automatically remove malicious, unwanted, or inappropriate emails that may be traversing internally. Employees too, play an important role as allies to your defense. Awareness training and internal business procedures should be considered of this layer.

Internal technical security controls should:

1. **Offer continuous protection** from newly detected email threats. Using the latest threat intelligence, new threats that have evaded the gateway or another security control can be contained and remediated.
2. **Mitigate the risks** associated with email account takeover. Detects and protects from malware attachments and phishing emails being sent from compromised accounts, helping to identify them, ready for remedial action.
3. **Detect internally generated malicious emails.** Stop malware propagating by email, and phishing emails being spread internally from user to user, whether from compromised accounts, devices infected by malware, or malicious users.
4. **Monitors outbound emails.** Prevents attackers using compromised accounts or computers to send malicious emails to customers and business partners to attack the supply chain.

5. **Prevents attackers and malicious or careless users** exfiltrating sensitive information.
6. **Streamline incident investigation** and reporting, response and remediation by API integration with SIEM and SOAR platforms

Why speed to email remediation matters

Email account takeover is a race for time. The longer an attacker remains within an organization's environment, the higher the risk that they access confidential data, steal funds, or observe user and network behavior to help them plant secondary malware.

Reducing these lengthy 'dwell times' requires a programmatic approach that includes measuring mean time to detection (MTTD) and Mean Time to Respond (MTTR). However, the **Exabeam 2020 State of the SOC Report** found just 22% of frontline SOC workers tracking were MTTD.

Automating internal email protection and remediation

The easiest way to speed up response and reduce MTTR times is through automation, reducing the burden on IT admins and security analysts.

Security orchestration, automation and response (SOAR) tools are used to take the intelligence from disparate systems to enable SOC teams to make quicker decisions, which lowers the MTTR when working incidents.

Organizations with existing SIEM and SOAR platforms can **streamline their email account takeover or malware outbreak** responses by using internal email security service APIs to integrate directly into existing playbooks. Remediated emails should still be retained for compliance purposes, but tagged, so that they cannot be retrieved by users.

APIs and email journal feeds from cloud-based email services like Microsoft 365 allow SOC teams to directly monitor and remediate malicious emails as if they were on an on-premise email server.

Critical SOC measures for account takeover protection

- Mean Time to Detect (MTTD): the average time it takes to discover a security threat or incident.
- Mean Time to Respond (MTTR): measures the average time it takes to control and remediate a threat.
- Dwell Time: measures the entire length of a security incident, from when an attacker first enters to the time they are removed.

Endpoint protection

Integration with endpoint security should allow for rapid and automated and any email downloaded attachments directly from the recipient's local file storage.

This technique can dramatically reduce the MTTR and help prevent users from inadvertently opening a malware infected file or having continued access to attachments containing sensitive information. It also can prevent them re-attaching a file containing malware or sensitive information to another email and sending it to internal or external recipients.

Automated defense adoption

58% of organizations say they have automated detection and removal of malicious or unwanted emails that have already landed in employees' inboxes.

While 36% either have an active project underway or planning to roll one out in the next 12 months.

(Mimecast State of Email Security, 2020)

Awareness training - from compliance to commitment

Training is a critical component of a pervasive email strategy, but many organizations have struggled to turn training programs into a demonstrable success. As previously stated, it's critical to concentrate technical controls both at and inside the perimeter. However, they can never be 100% successful when accounting for novel zero-day malware and the human element.

Additionally, attackers often bypass perimeter security by targeting employees directly through their personal email and social media accounts, even by means of social engineering in the physical world. These vectors can include USB devices, malicious websites, public WiFi hotspots and compromised devices on less protected home networks.

Once an attacker has compromised a user's device, they can use keystroke loggers or password caches to steal credentials and login to move laterally across the network. Malware can send malicious emails from one email client to internal users, business partners and customers.

For these reasons, all employees should be empowered to become a security ally, your last line of defense.

55% of businesses do not provide awareness training on a frequent basis

17% of organiazations only conduct security training once a year

(Mimecast State of Email Security, 2020)

How to build a successful secury awareness training program

Awareness training is not a new concept with **Gartner now reporting** global spend increasing over the $1B mark. However, **Forrester research** shows 44% + of employees are unenthusiastic about it. Some employees associate training as a punitive measure which impacts their productivity. More concerning is that when employees are disengaged, they won't learn good behaviors and become dismissive of security in general.

Traditional training has failed employees. To retain topical knowledge, they need a consistent, engaging cybersecurity awareness training program. **Mimecast's State of Email Security research** reported only 1 in 5 respondents (21%) offer training on a monthly basis. 17% are only trained once per year, a rate that neglects to foster a comprehensive security culture throughout the organization.

If there is not a clear cyber resilience or mitigation culture within an organization, vulnerabilities may develop that can be exploited. To be truly successful, security awareness training programs need to meet **three criteria as outlined by Forrester Research.**

With these criteria, employees can make their training stick, playing an active role in their organization's cybersecurity posture. However, the effects of infrequent or monotonous security awareness training can have far-reaching consequences.

Overall, organizations are taking security awareness training more seriously. In fact, nearly all of respondents' organizations (97%) offer some kind of training at varying frequencies and formats. About 6 in 10 offer group training sessions, while around 4 in 10 offer various other types like online tests, emailed or printed tips, or 1:1 training.

IT and security administrators need to be able to contextualize risks gathered from training data. For example, in phishing simulations, identifying who clicked, which department they work in and what was clicked. Technical and human controls can then be adapted at the specific point of risk.

Mimecast customer best practices experience highlights that organizations should train first and phish second. This helps encourages a positive learning experience. Security awareness training should not be about embarrassing employees through trickery and deception.

Three criteria to security awareness training programs.

Foster a security culture rife with empathy and encouragement, instead of obligatory (or boring!) training and testing.

Use engaging, inclusive images and messages to encourage active participation

Take a global view and make training culturally relevant to each region.

Almost all incidents have human error at the heart and if employees are not prepared for an attack, neither is your organization. Training should be about positively changing culture and closely integrated with the rest of your security controls.

Content is king

Engaging content is as critical to awareness training as it is to marketing. In fact, there's many similarities in the disciplines and security leaders would do well to imitate their marketing colleagues closely in their programs. Good training content alone will improve employee knowledge. Creating a nurture campaign with follow up supplemental materials, such as memes or flyers, will help employees retain that knowledge.

Building a rich set of engaging content in-house can be a challenge, which can lead to infrequent or inconsistent training modules. This will often include videos, animations and text guides than can also be deployed within an existing learning management system.

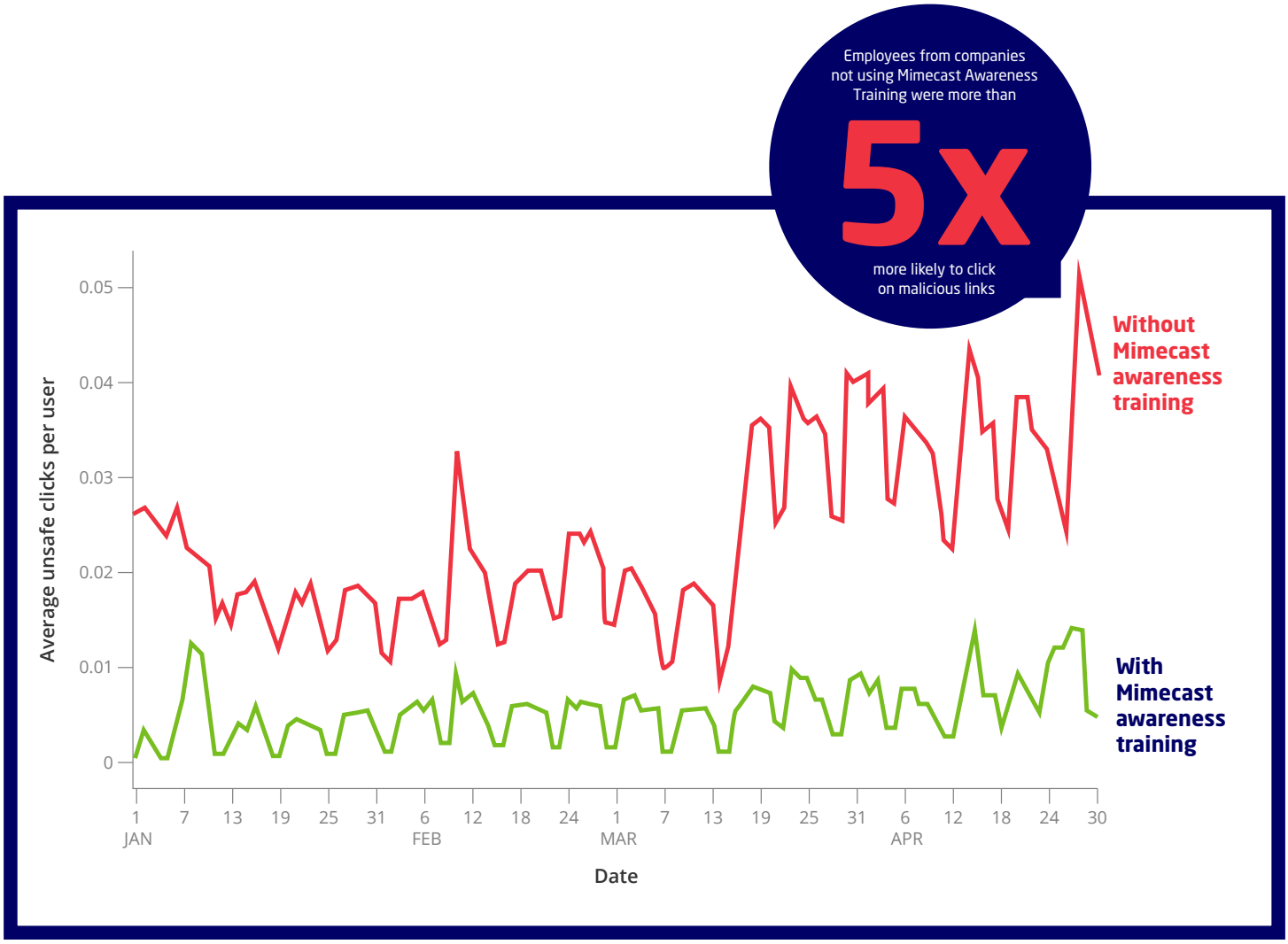
According to the recent 2020 State of Email Security research, just 23% of global organizations are using training videos, and barely 1 in 5 (18%) use a single third-party provider, although this is predicted to continue to grow.

Many security professionals struggle to accurately replicate the sophistication and variability of genuine cyberattacks for the purpose of testing and training employees. Good phishing simulations need up-to-date and adaptable templates suitable for the specific organization and high-risk departments. However, a more accurate and impactful way to identify risk is to neutralize and convert the real phishing emails targeted at the organization.

Memory test

How well can you memorize and recall a list of 10 security tips? Compare this to how you remember the last movie you watched made you feel.

Engaging story-driven content builds empathy to help change behaviors and improve memory recall.



(Mimecast State of Email Security, 2020)

Measurement is majestic

Embracing a risk scoring system allows you to evaluate the security preparedness of your indivdual employees, departments and the organization as a whole. This can be compared with industry or regional averages to get a clear point of comparison. Improving your comparitive risk allows you to asses the impact of changes, and gain actionable insights for correcting course.

Risk scoring factors (measured over time)

1. Real attack and click data by employee or department
2. Employee engagement with simulated phishing campaigns
3. Completion of security training
4. Self-graded sentiment scores, measures employee perceptions
5. Comparisons with industry or regional averages

Conclusion

Email continues to be the number one source of cyberattacks and great concentration of risk. While other internal collaboration tools (e.g. Slack, Teams) are growing in popularity, there is no evidence that internal email will disappear.

Traditional email security techniques focused on defending the network perimeter, but threats have evolved and become sophisticated in such a way that you can no longer rely on this alone. Cloud adoption (notably SaaS services) further breaks down the perimeter defense model and filtering at the gateway for spam, impersonation, malicious links, and malware is longer enough. Email security controls must also operate inside the perimeter to detect abnormal behaviors, identifying compromised accounts and insider threats, and providing tools to automatically remove malicious or unwanted emails from employee's inboxes.

Combined with these technical controls, we need to arm all employees with regularly up-to-date security awareness training and a firm belief that they play an important role in defending the organization from attacks. We need to build a culture of security commitment not one of simple compliance. Almost all incidents have human error at the heart and if employees not prepared against attack, neither is your organization.

As part of our collective response to the global pandemic-led digital transformation, it's vital that every organization's email security evolves to respond to the new threat landscape. The danger within can only be effectively mitigated by a pervasive and multi-layered security strategy.

Account takeover protection - planning priorities

1. Upgrade email security perimeter defences to detect advanced impersonation and malwareless attacks
2. Enforce strong password hygiene and multi-factor authentication use
3. Monitor internal emails for malware, phishing and suspicious user account behaviour
4. Protect and monitor your most valuable data with Data Leak Prevention (DLP) inspection
5. Share intelligence with endpoint and web security services to pinpoint malicious files on employee devices
6. Extend an API-led approach for automatic remediation of malicious emails inside the network (including cloud email providers)
7. Track mean time to detection (MTTD) and response (MTTR) in your SOC
8. Build a consistent, engaging cybersecurity awareness training program and measure its performance over time
9. Integrate DMARC monitoring and enforcement to protect the domains you own being used to spoof your employees and supply chain partners
10. Monitor and takedown web domain names similar to your own or cloned versions of your websites

Mimecast was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together.

We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.