UNDERSTANDING THE EMAIL THREAT LANDSCAPE

F-Secure Whitepaper
CONTENTS

1. Introduction ................................................................. 3
2. Email threat landscape .................................................. 4
   Social engineering ......................................................... 4
   Phishing ........................................................................ 5
   Malware .......................................................................... 6
3. Examples of business email compromises ......................... 7
   Business email compromise (BEC) .................................... 7
   Email account compromise (EAC) .................................... 9
4. Tactics, attacks and current trends .................................... 11
   Microsoft 365 ................................................................... 11
   COVID-19 ...................................................................... 13
5. Recommendations and best practice .............................. 15
1. INTRODUCTION

There is already a large number of organizations transitioning to more cost efficient cloud-based solutions as of now. According to recent research by Gartner, “by 2021, Gartner expects 70% of public and private companies to be using cloud email services.”⁶

As services evolve so do attackers’ methods. The transition from on-premise to cloud solutions has seen a parallel transition in attackers’ goals. Access to a user’s email account now often grants access to a wide range of available services, meaning attackers may only need to steal one set of credentials to have a potent effect. This is clear as there is a marked increase in number of attacks against cloud-based email services such as Microsoft 365.¹

The consequences of successful malicious email attacks are numerous – with most malware still being delivered by email. Most common threats include Business Email Compromise (BEC) scams and Email Account Compromises (EAC). The COVID-19 pandemic has also affected the email threat landscape since its outbreak. As a result, we have observed an increasing number of coronavirus-themed attacks appearing in the wild.

A multilayer approach is crucial in strengthening an organization’s security features and to keep an organization safe from email attacks. Merely because all it takes is one small act on the wrong email to compromise an entire organization.

This whitepaper discusses the common email security threats that are faced by organizations and how to keep your organization safe from these attacks.
2. EMAIL THREAT LANDSCAPE

The hazards presented by email are numerous. One small act upon the wrong email and recipients may end up as the victim of cryptomining or have their credentials stolen. They may even find themselves suddenly out of large sums of money if they fall for the wrong socially engineered scam.

Social engineering

Social engineering is a form of manipulation and deception that is crucial for a successful phishing attack. Successful phishing attacks rely heavily on the attacker’s ability to effectively deceive the target by convincing them to trust the sender as well as its content.

Phishing is conducted in order to gain as much information of the target as possible. In order to increase the effectiveness of social engineering for a successful attack, the attacker will aim to demonstrate detailed knowledge of the person or target organization, in which information is often gathered by performing open source intelligence gathering (OSINT).

This assumed credibility rests on two critical sets of information:

- Knowledge about an organization’s internal structure, processes, and software;
- Knowledge about an organization’s staff.

Many organizations keep a web presence offering a wealth of information. Knowledge about an organization’s internal structure, processes, and software often easily derived from what organizations themselves published such as job listings.

Attackers are also able to gather extensive knowledge about an organization and its staff from public channels such as Linkedin. The more intelligence obtained about a potential target, the better attack a skilled social engineer can craft.

For example, a typical job listing covers:

- **Processes**: Detailed descriptions of the task and responsibilities for a specific role;
- **Structure**: Information about whom the employee reports to or manages;
- **Software**: Desired skills and knowledge.
Phishing

Phishing represents the intersection between cybercrime and social engineering and is one of the oldest threats on the internet that hacks a person rather than a particular computer system. It is used with varied sophistication and purpose depending on the scale of the attack. Attackers can range from novices and fraudsters to serious organized criminal groups and nation states.²³ Phishing used by the majority of attackers for its ease, reliability, and potency. The goal of a phishing attack can be:

- Obtain login credentials to be used to gain access to assets – an account, a server, a network or the likes;
- Obtain sensitive information such as financial or personal data;
- Deliver malicious payload like ransomware, a keylogger or Remote Access Trojan (RAT);
- Convince victims to carry out activities that are against their self-interest, such as wiring money or sharing personal data.

The rate of phishing attempts has been increasing due to the proliferation of leaked email addresses, with the number of unique phishing sites detected being at an all-time high⁴. Phishing attacks can be categorized into two types – untargeted phishing attacks and targeted spear phishing attacks.

1. Untargeted phishing attacks
Untargeted phishing attacks are used to reach as broad an audience as possible. The main goal of this kind of attack is to trick recipients into clicking on a link, opening a malicious attachment, disclosing sensitive information, or transferring funds.

Because untargeted attacks often rely on high volume to be successful they are more easily identified and mitigated by email security filters. These filters look for existing patterns and indicators of malice found in language, type of content or domain registration information. In the grand scheme of things, untargeted phishing campaigns have become increasingly less of a threat.

2. Targeted phishing attacks
Targeted phishing attacks, on the other hand, are used to target a small set of users within a specific organization and relies heavily on social engineering. This kind of attack is much harder to detect and stop. They will be crafted using in-depth knowledge about the targets and their environment that often only an insider should possess.

Unlike untargeted phishing attacks, even a small number of successful targeted phishing attacks can lead to a much greater damage overall. Although only a small proportion of victims click on the bait, the significant danger of targeted spear phishing attacks lies in the fact that it only takes one successful attempt to compromise an entire organization.
Malware

Email remains as the primary initial access vector used by attackers – with 94% of malware being delivered via email.³

The delivery of malicious binaries used to be more prominent with .exe, Java, and Flash files attached directly to emails to trick users into opening an executable. Preventive controls have become more advanced, thus requiring attackers to change their attack tactics, technique, and procedures. Nowadays, malware is much more likely delivered through less suspicious business document attachments or URLs that are commonly sent in regular, valid email communications or through other applications.

Almost 50% of all malicious attachments are found to be office documents with hidden macros, scripts and other exploits, which upon activation, will download additional payloads, such as ransomware and RAT. The rest are commonly through Windows Apps (26%) and other, such as archives and .js files (22%).³

Ransomware attackers are now targeting companies to get better and larger income instead of mass attacking consumers. They also changed the way they operate in order to maximise their chances of receiving the ransom. Instead of an immediate deployment of ransomware or exfiltration of data following the initial breach, the attackers will spend some time in the company network in order to gain as large foothold as possible, before taking action. This is to ensure that as much data as possible is exfiltrated and as large part of the company network is encrypted, in order to maximize the chance of payout. However, the goal is not always financial as ransomware is sometimes also used to cover up a compromise.

THE INSYNQ ATTACK

In August 2019, INSYNQ’s internal network was compromised due to a successful email phishing attack that was targeted at an employee working in sales. Upon the initial compromise, the attackers spent approximately ten days rooting around the organization’s internet network before deploying a ransomware to demand for a substantial amount of ransom.

3. EXAMPLES OF BUSINESS EMAIL COMPROMISES

In this chapter, we will take a look at a few most common threats that organizations are facing. It is crucial to understand how these attacks work in order to protect your email systems from them.

Below are some of the most common compromises faced by organizations.

Business Email Compromise (BEC)

BEC scams are a form of email fraud where the attacker masquerades as a senior employee and attempts to coerce the recipient into performing their business function for an illegitimate purpose, such as wiring money.

Attackers might carry out these scams through:

- Email or website spoofing – imitating a legitimate email or website
- Sending spear phishing emails
- Deploying malware

According to the Europol, they are also becoming alarmingly more professional and convincing. BEC attacks have quickly gained the status of being a top priority for European law enforcement as the threat landscape continues to evolve at tremendous speed.

Most malware is still delivered by email
Four common BEC scams

Here are four basic BEC scams to watch out for:

1. **Fake Invoice Scam**
   This type of attack typically involves the impersonation of a company’s trusted supplier. The impersonation relies on social engineering and is often achieved using spoofed email. The scam is then carried out with a request for funds to be wired for an invoice payment into a fraudulent account instead of a legitimate account for that supplier. Last year, Google and Facebook made headlines for falling victim to such a scam and ended up losing approximately $100m.⁹

2. **Wire Fraud Scam:**
   Attackers in a wire fraud scam typically impersonate and identify themselves as higher-level executives such as CEO, CFO or COO of the targeted company who appear to be handling urgent and confidential matters through spoofing. These matters are accompanied by a request to wire a transfer to an account within their control, e.g. a mule’s account. In some cases, these requests are made directly to the company’s financial institution insisting funds to be wired urgently.

3. **Fake Lawyer Scam**
   In this scam the attacker reaches out to employees or the targeted company while pretending to be a lawyer with either the Corporate Counsel or another law firm. Similar to above mentioned scams, they often claim to be handling confidential and time-sensitive matters that require the employee to handle a transfer of funds. The request may reference matters which are occurring at the company like a merger or acquisition thus making it more believable. It is typically timed closer to the end of a business day when employees are tired and more vulnerable to mistakes i.e. falling victim to the scam.

4. **Human Resources Scam**
   Here, the attacker poses as someone from a specific functional area in the company such as Human Resources. However, unlike the previous scams, they ask for personally-identifiable information (PII) instead of money. This request is even more damaging to a company as the information received can be used to make money or be used for a larger attack.

The bad news with BEC scams is that they work. BEC scams are even more believable when they are carried out from compromised email accounts.
According to the Internet Crime Complaint Center (IC3), there were U.S. $1.7 billion in losses in 2019 alone due to BEC scams. Below is a list of incidents that have made it past the news threshold. Some Examples of BEC at work in the past five years:

2015 – 17 different Dallas firms were scammed out of $600,000 in total by a sophisticated CEO impersonation BEC scam. The basis of the scam was the use of spear-phishing emails, which were used to compromise email accounts.

2015 – Xoom: A full $30.8 million was lost to employee impersonation where a number of spoof emails were sent making requests to the finance department to pay invoices.

2015 – Mattel: The toymaker handed over $3 million USD during a BEC attack. The spoof email was part of a CEO impersonation scam.

2016 – Crelan: A total of 70 million euros was lost due to CEO impersonation.

2016 – Austrian company FACC Operations GmbH: This was a case of CEO impersonation. Walter Stephan, the CEO of the Austrian company, was sacked after the organization lost $47 million due to a BEC scam.

2019 – Toyota: Toyota Group subsidiary announced in September 2019 that they were the victim of a BEC scam with an expected financial loss of over $37 million.

2019 – Nikkei: Another BEC attack affecting Nikkei, one of the largest media groups in the world, costing the company around $29 million in October 2019.

Email Account Compromise (EAC)

EAC is a sophisticated attack in which attackers use various tactics, techniques, and procedures to compromise a user’s email account in order to gain access to their legitimate accounts. While it is similar to BEC, the difference between EAC and BEC lies in whether the email system has been compromised.

- **BEC: Impersonates you, has not compromised the email system**
  BEC attackers typically use identity deception tactics such as domain spoofing, display name spoofing, and lookalike domains to trick targets into making payments to fraudulent accounts

- **EAC: Impersonates you, has compromised the email system, uses your actual email account**
  EAC attackers take control of your account which allows them to bypass email filters and authentication controls. This is a very effective way to conduct email fraud internally or with your customers using phishing emails because they are “trusted”.

Both EAC and BEC rely heavily on social engineering and are targeted at specific people. These two kinds of compromises are so intertwined that the the US Federal Bureau of Investigation (FBI) has been tracking these scams as a single crime type since 2017.
EAC attacks launched from compromised email accounts are difficult to detect. These attacks may be targeted at other users within the target organization or externals such as clients and partners. An EAC attack is a serious risk for the account's legitimate owner and the companies involved because it doesn't only give attackers the ability to impersonate the account's owner but it also provides full access to the person's contacts, ongoing email conversations, and email archives.

That means that attackers can now leverage hacked company email accounts to craft new scams that are extraordinarily personalized and effective based on the information they have. Among them are:

1. Launching large phishing campaigns from the compromised account. In most cases, the 'good reputation' of the account and the company email server makes these campaigns successful.

2. Sending more targeted and elaborate emails to employees who are authorized to pay bogus invoices, if the account owner is a senior figure within the organization.

3. Inserting themselves into organizational conversations that are centered around payments to inform recipients that they need to wire money to a different account on this occasion, and the theft is done.

Due to the increase in credential theft used to hack cloud-based email services and to conduct a BEC or an EAC, it is crucial to ensure the security of business credentials and their use. Organizations can keep their businesses safe by implementing a multilayer approach to their security, including usage of Multi-factor authentication (MFA), User and Entity Behavior Analytics (UEBA), and password managers. It is also essential to conduct organization-wide security awareness training against credential theft so that employees can assist in the detection of social engineering attacks instead of falling for them. Other kind of attacks such as malware and network intrusion will, however, require a different type of response.

Over 80% of compromises is driven and enabled by credential theft!
4. TACTICS, ATTACKS AND CURRENT TRENDS

Attackers are constantly looking for opportunities to refine their social engineering to make their attacks more believable. They are conscious of world trends and seasonality and will use this to advance their attacks. In this chapter, we will take a brief look at how attackers adapt their tactics to two recent trends – Migration to cloud email services and COVID-19.

**Microsoft 365**

Email solutions, whether on premise or cloud, are vulnerable to phishing attacks, credential thefts, and exploitation of configuration errors. Criminals simply shift their focus and adapt their tactics to locate and steal the data they find to be of most valuable depending on the target organization’s IT infrastructure.

According to recent research by Gartner, “by 2021, Gartner expects 70% of public and private companies to be using cloud email services.”⁶ There is already an increasing number of organizations transitioning to the more cost-efficient cloud-based solutions such as Microsoft 365.

Along with this transition is a parallel uptick in attackers seeking to compromise a user’s email account as the organizations’ emails and other valuable data migrate along with them. To date, over 80% of compromises is driven and enabled by credential theft.¹

The most recent examples include:

- The distribution of TrickBot, an information-stealing trojan, via a fake website.¹¹
- A phishing campaign that sends fake alerts with the intent to take over the accounts of email domain administrators.¹⁰
- The phishing campaign using Microsoft Sway.¹²

However, Microsoft 365 isn’t the only target. Similar phishing attacks have been observed against other cloud-based email services such as Google’s cloud email offering, Gmail and G-Suite. A newly discovered cybercrime group, Exaggerated Lion, reported to prefers targeting G-Suite when conducting BEC attacks.¹³ Given the prevalence of Google accounts, and how they are leveraged across the Internet to log into various websites, it’s no surprise that attackers have created phishing sites in this arena as well.

¹¹
¹²
¹⁰
⁶
¹
The threat of these attacks against cloud email services such as Microsoft 365 is so severe that the FBI issued a warning on threat actors abusing Microsoft 365 and Google G Suite as part of BEC attacks.¹⁴

*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,* the FBI said in a Private Industry Notification (PIN) from March 3.

**Types of Microsoft 365 attacks**

**Failure of delivery emails**

When you try to send an email to either a full or non-existent inbox, you’ll get a non-delivery or failure of delivery email in return. Because cybercriminals know these are hard for you to ignore, they use this to their advantage.

**Alert for hitting storage limits**

This Microsoft 365 phishing email also pretends to be from Microsoft. If you use this subscription service often, it’s not hard to believe that you’ve reached your account storage limits. Scammers send out fake emails notifying you that you must activate “Quota” to resolve your storage issues. In actuality, “Quota” is malware, just like with the fake non-delivery emails.

**Requests for reactivation**

Microsoft 365 phishing attacks are highly successful because they prey on fear and knee-jerk reactions. Spoofed reactivation requests do precisely that. They tell the recipients that their accounts have been deactivated. In order to reactivate their accounts, they have to use the attached malicious link. It leads to a spoofed login site, where their credentials are sent to the cybercriminals responsible for the attack.

**Update your password**

This Microsoft 365 phishing email pretends to be from Microsoft (you see the trend here?). It leads to a spoofed login site, where the user can change their password, after which their credentials are sent to the cybercriminals responsible for the attack.

Phishing campaigns targeting Microsoft 365 often leverage Microsoft’s own legitimate tools to conduct the attack. The attack itself can be very sophisticated and believable with very little effort; attackers can simply buy phish kits for as low as USD 999 from the dark web.

The tricky part about these campaigns, also the hardest part to catch, is that the message and its links are completely safe which makes it easy to bypass existing security filters. However, they lead the target towards carrying out harmful action which will compromise both the email account and the company (Read earlier chapter on EAC).

Phishing campaigns that are targeting Microsoft 365 are also incredibly effective because the end-users are accustomed to receiving many notifications from the email service itself. Therefore, they aren’t nearly as cautious with the links, emails, and notification they receive – especially if it is part of the organization’s software infrastructure. After all, it is “just normal, expected, and filtered everyday emails” coming from the service and not some strange Nigerian prince who wants to donate his lottery money to the user.

Traditionally, phishing attacks have been crafted to trick end users. If successful, the attacker will gain access to the system and information they need. However, this compromise is still limited only to the victim’s email and to the areas and services where they had permissions. Hence, we are also seeing an increase in cyber criminals launching targeted spear phishing attacks against Microsoft 365 administrators – a move that would allow them to gain full administrative control over an organization’s Microsoft 365 domain and accounts, if the attack was successful.

Phishing campaigns that are targeting Microsoft 365 often leverage Microsoft’s own legitimate tools to conduct the attack. The attack itself can be very sophisticated and believable with very little effort; attackers can simply buy phish kits for as low as USD 999 from the dark web.

The tricky part about these campaigns, also the hardest part to catch, is that the message and its links are completely safe which makes it easy to bypass existing security filters. However, they lead the target towards carrying out harmful action which will compromise both the email account and the company (Read earlier chapter on EAC).

Phishing campaigns that are targeting Microsoft 365 are also incredibly effective because the end-users are accustomed to receiving many notifications from the email service itself. Therefore, they aren’t nearly as cautious with the links, emails, and notification they receive – especially if it is part of the organization’s software infrastructure. After all, it is “just normal, expected, and filtered everyday emails” coming from the service and not some strange Nigerian prince who wants to donate his lottery money to the user.

Traditionally, phishing attacks have been crafted to trick end users. If successful, the attacker will gain access to the system and information they need. However, this compromise is still limited only to the victim’s email and to the areas and services where they had permissions. Hence, we are also seeing an increase in cyber criminals launching targeted spear phishing attacks against Microsoft 365 administrators – a move that would allow them to gain full administrative control over an organization’s Microsoft 365 domain and accounts, if the attack was successful.

Phishing campaigns targeting Microsoft 365 often leverage Microsoft’s own legitimate tools to conduct the attack. The attack itself can be very sophisticated and believable with very little effort; attackers can simply buy phish kits for as low as USD 999 from the dark web.

The tricky part about these campaigns, also the hardest part to catch, is that the message and its links are completely safe which makes it easy to bypass existing security filters. However, they lead the target towards carrying out harmful action which will compromise both the email account and the company (Read earlier chapter on EAC).

Phishing campaigns that are targeting Microsoft 365 are also incredibly effective because the end-users are accustomed to receiving many notifications from the email service itself. Therefore, they aren’t nearly as cautious with the links, emails, and notification they receive – especially if it is part of the organization’s software infrastructure. After all, it is “just normal, expected, and filtered everyday emails” coming from the service and not some strange Nigerian prince who wants to donate his lottery money to the user.

Traditionally, phishing attacks have been crafted to trick end users. If successful, the attacker will gain access to the system and information they need. However, this compromise is still limited only to the victim’s email and to the areas and services where they had permissions. Hence, we are also seeing an increase in cyber criminals launching targeted spear phishing attacks against Microsoft 365 administrators – a move that would allow them to gain full administrative control over an organization’s Microsoft 365 domain and accounts, if the attack was successful.
Threat actors target administrative credentials for several reasons. Amongst them:

- Microsoft 365 admins have administrative control over all email accounts on a domain. A compromised admin account may enable retrieval of user emails or a complete takeover of other email accounts on the domain.
- Microsoft 365 admins, most often, have elevated privileges on other systems within an organization. A compromised admin account potentially allows further compromises to take place via password reset attempts or abusing single sign-on systems.
- Microsoft 365 admins can create new accounts within the organization. A compromised admin account allows attackers to do so and abuse single sign-on systems or to leverage the reputation of the compromised domain to send out a new wave of attacks.

One of the more recent examples of phishing attacks against Microsoft 365 Administrators was a Fake Alert phishing campaign.

In this particular campaign, the fake alerts are well-crafted and include the actual Microsoft 365 logo which is meant to portray a sense of familiarity alongside the urgency that the administrator needs to deal with time-sensitive concerns. For example, a notification that company’s licenses have expired and require immediate action to reactive them. These fake alert emails typically include links that prompt the administrator to log into their account and fix the issue that was brought up in the email. Needless to say, the links lead to a phishing website that asks the target user to enter their Microsoft credentials and, voila! The attack is done.

COVID-19

As people across the globe have restricted their movements in hope of curbing the spread of the coronavirus, spammers and phishers are out in full force to take advantage of the online demand for information about the pandemic. Since its outbreak, we have observed an increasing number of coronavirus-themed attacks appearing in the wild through:

- Malspam campaigns where attackers deploy malwares through what appears to look like links to sites with more news and information on the coronavirus.
- Mask scams where attackers capitalize on the widespread shortage of masks. They entice the recipients to pay but the criminals send them nothing.
Think twice before you click

In this case, cyber criminals know that you are expecting emails relating to COVID-19. Criminals can increase the effectiveness of their email attacks by mimicking a familiar authority, using urgency and exploiting the globally felt fear due to the current situation.

Malicious actors may use existing, real, materials as bait to encourage people to perform a risky action such as click a link or open an attachment. A favourite tactic is to hide executables in archive files attached to emails. It is critical that users look at the sender of an email and examine any links contained within it before taking action. If at all unsure, users should report it. By mid April 2020, Google reported an average of 18 million COVID-19 phishing emails that were sent out via Gmail in a day.

Some of the recent examples for COVID-19 related phishing campaigns targeted attacks towards medicare groups and organizations. The criminals carried out the attacks by using a faux World Health Organization email address with the subject line “COVID-19 supplier notice” and attaching a malicious Word document hosting a ransomware payload that takes advantage of computers that have not been patched. Medicare groups and organizations are extremely vulnerable in delicate times like these when they are scrambling for supplies to handle the situation – which makes it harder to practice extra caution with their emails when actual lives are at stake.

MALWARE THAT’S BEEN EMPLOYED IN THESE CAMPAIGNS INCLUDE:

- Emotet and Trickbot – modular threats that deliver different payloads to different targets. Emotet was originally a banking trojan that was updated/upgraded to include new capabilities, such as infostealing and malware delivery. It is known to deliver Trickbot, which then delivers Ryuk ransomware.
- Formbook – an infostealer that collects victim's sensitive information, such as passwords/credentials from browsers.
- Lokibot – an infostealer that collects email credentials and passwords from browsers, FTP clients and CryptoCoin wallets.
- Agent Tesla – an infostealer that has keylogging capabilities for stealing email credentials and passwords from browsers.
- Remcos RAT – a remote access tool used by cyber criminals that allows attacker to control a victim's system remotely, and execute commands.
5. RECOMMENDATIONS AND BEST PRACTICE

Not all is lost even if attackers are becoming alarmingly professional and believable in their approaches. As in the past, a layered approach to security is incredibly critical in defending an organization from email-based attacks.

There are several tried and tested email security capabilities that still matter today:

- Leverage purpose-build email security that provides anti-malware and URL blocking capabilities are vital to block malware, spear phishing, ransomware, and cryptomining in attachments, along with URL intelligence to combat malicious links in emails.

- Integrated sandboxing should happen automatically in the background for new files arriving in email to quickly understand if they are malicious. There’s no way to guarantee against falling for email based attacks, but there are many things

- Train your end-users:
  - don’t click on links or attachments from senders that you don’t recognise
  - don’t provide sensitive personal information (like usernames and passwords) over email
  - watch for email senders that use suspicious or misleading domain names (where the email address originated from). Is the email name and domain name real? Hovering over the ‘From’ column is a simple way to check if an email is legitimate or not.
  - inspect hyperlinks carefully to make sure they’re legitimate and not directing you to imposter sites. To do this hover over the link to see if it matches the URL that is displayed.
  - don’t try to open any attachments that you’re not expecting to receive
  - use a different password for each application/website
  - check if your credentials have been compromised [https://haveibeenpwned.com/](https://haveibeenpwned.com/)

- Have processes in place
  - Payment requests, regardless of source, are verified F2F/on-the-phone before they are processed.
USE CASE: BEST PRACTICE RESPONSE TO MICROSOFT 365 PHISHING ATTEMPT

The following steps are recommended to help secure the Microsoft 365 environment and rectify any potentially impacted accounts:

1. Preserve Tenant activity logs and include the following:

2. Investigate Microsoft 365 Tenant and other IT infrastructure, including a review of all Tenant settings, user accounts, and the per-user configuration settings for possible modification. Check for indicators of methods of persistence, as well as indicators an intruder may have leveraged an initial foothold to get VPN credentials, or access to other organizational resources.

3. Review delegate permissions and mail forwarding rules for all your mailboxes. The following PowerShell script can help do this here: [http://aka.ms/delegateforwardrules](http://aka.ms/delegateforwardrules)


5. Enable multi-factor authentication for all users. Setup instructions can be seen here: [http://aka.ms/MFAuth](http://aka.ms/MFAuth)


7. For every identified impacted account, automatically perform the following remediation steps by running the script located here: [http://aka.ms/remediate](http://aka.ms/remediate)
   a. Reset password (this secures the account and kills active sessions).
   b. Remove mailbox delegates.
   c. Disable mail forwarding rules to external domains.
   d. Remove global mail forwarding property on mailbox.
   e. Enable MFA on the user’s account.
   f. Set password complexity on the account to be high.
   g. Enable mailbox auditing.
   h. Produce Audit Log for the admin to review.

8. As part of your investigation, consider whether you should or must notify government authorities, including law enforcement.

In addition, it is recommended you:

- Read and implement our guidance on addressing unusual activity here: [http://aka.ms/fixaccount](http://aka.ms/fixaccount)
- Enable the audit pipeline to help you to analyze the activity on your tenancy here: [http://aka.ms/improvesecurity](http://aka.ms/improvesecurity). Once complete, your audit store will start populating with all activity logs and you’ll be able to leverage the ‘Security and Compliance Center’s Search and Investigation’ feature seen here: [http://aka.ms/sccsearch](http://aka.ms/sccsearch)

Deliver or reinforce phishing/cybersecurity training for your employees.

Built to complement the native email security capabilities of Microsoft 365, our new cloud solution brings you a comprehensive protection against the most sophisticated phishing, malicious content, and targeted attacks.

Get your FREE trial

About F-Secure Phishd
Phishd forms part of the F-Secure Consultancy business. In Phishd we aim to solve the threat of Phishing. This is done through a managed awareness service, and the simplification of reporting malicious emails to security teams. Importantly, Phishd’s suite of Informer products performs initial triage of reported phishing emails, providing the users with an analysis report, as well as a dashboard where the security team can view and investigate pre-triaged phishing emails.
REFERENCES

5. 2019 Data Breach Investigations Report
ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We’re closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry’s best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world’s most potent threats.

Together with our network of the top channel partners and over 200 service providers, we’re on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business  |  twitter.com/fsecure  |  linkedin.com/f-secure