CISA's recommendations to

Recognize and avoid email scams

ManageEngine
Exchange Reporter Plus

Table of contents

Introduction

Email has always been the most popular tool used for business communications. Unfortunately, it is also one of the weakest links in an organization's security strategy. 94 percent of all cybersecurity incidents originate from emails.

As organizations all over the world have adopted remote work at an unprecedented rate, the dependence on email has also increased simultaneously. This has made email one of the most favorite and lucrative attack vectors among cybercriminals.

According to an UN official, there has been a 600 percent increase in malicious emails amid the COVID-19 crisis.

Various scam campaigns involving spear phishing, impersonation attacks, and account takeovers, to steal money, intellectual property, or other forms of sensitive data belonging to an organization have been growing rampant.

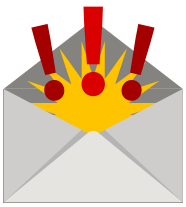
In this e-book, we will look at the reason behind the increase in email-based attacks, how you can implement the Cybersecurity and Infrastructure Security Agency's (CISA) recommendations to mitigate them— using Exchange Reporter Plus, a comprehensive web-based analysis and reporting solution to keep an eye on all key aspects of Exchange Servers and Exchange Online.

Recognizing email scams

Combating email scams is an ongoing security concern for organizations of all sizes. This is mainly because email-borne cyberattacks are relatively unsophisticated and easy to carry out when compared to other types of cyberattacks. This, coupled with the capability of reaching thousands of people at once, makes it highly challenging for IT teams to protect their employees from inadvertently divulging sensitive organizational data to the attackers.

Understanding the anatomy of such scams and how the attackers manage to successfully deceive employees helps a lot in spotting them as quick as possible rather than enabling or engaging with them accidentally. The following are some of the most common types of emails that are more likely to be used for scamming employees.

Emails that evoke a sense of urgency



Scam emails are almost always drafted to create a sense of urgency. For example, the attacker can impersonate a C-suite executive to deceive employees or partners into sending money or personally identifiable information (PII) such as Social Security numbers, credit card numbers, login credentials, and so on.

Some of the most commonly used subject lines are as follows:

- NOTIFICATION OF PAYMENT RECEIVED
- YOUR RECEIPT FROM APPLE
- USPS: Your digital receipt is ready
- PASSWORD CHECK REQUIRED IMMEDIATELY
- Would you mind taking a look at this invoice?
- FedEx: Correct address needed for your package delivery on [date]
- PAYMENT DUE [date]

Sources: The FBI's Internet Crime Report (ICR), KnowBe4's top-clicked phishing report.

Attackers use this tactic to prey on the employees' natural curiosity and their willingness to trust. This is primarily because attackers usually operate under the presumption that it is easier to exploit the vulnerabilities of human behavioral traits, such as trust, than software vulnerabilities—and they're often right.

Emails that contain links that do not match legitimate URLs

As convincing as it may seem, not all emails that appear to be coming from a reputed brand or institution are genuine. Some emails contain links that do not match the legitimate URL, and a gullible employee might click the link thinking it will take them to a genuine website.

These emails attempt to lure employees into visiting a bogus site to either inject malware into the employee's computer (or other malicious programs that could compromise their computer) or steal their Microsoft 365 login credentials.

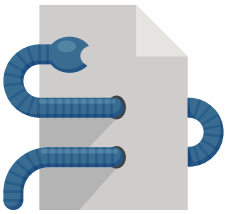
According to a survey conducted by Osterman Research on 300 companies with more than 5,000 employees in the US and the UK, 40 percent of enterprises reported that Microsoft 365 login credentials of their employees have been compromised in the past, and over a quarter of those said it happened 10 or more times.

For example, an attacker might masquerade as an IT administrator to send emails to employees saying that their mailbox storage is full and urge them to add more mailbox storage to avoid not being able to send or receive emails. This message will also contain a "Sign in to the Microsoft 365 Admin center" link.

Once an employee clicks the link, they will be taken to a spoofed Microsoft 365 login page—which looks remarkably similar to a legitimate one—where they will give up their login credentials unwittingly.

With these stolen credentials, attackers can further orchestrate various other malicious activities within the organization. It is a huge bonus for the attackers if the stolen credentials are from an account with admin privileges offering them a complete control over all the email accounts of that domain. They can also go on to create a backdoor user account to launch a new wave of attacks.

Emails with attachments having executable files



Email attachments are one of the most common ways attackers try to sneak viruses onto an employee's computer. This is why it's imperative to treat email attachments with caution. Especially if it's from an external email ID in the form of executable files or scripts.

Some of the most commonly used file extensions to inject viruses are as follows:

- .exe
- .dot
- .com
- .dll
- .pif
- .scr
- .js
- .xls
- .doc
- .xlt

According to the CISA, if a malicious file (sneaked in through a screamingly innocuous email attachment) gets executed, it can:

- Create a security vulnerability on the computer in which the file was executed.
- Open a "backdoor" for the attacker by allowing illicit access to the computer.
- Install fraudulent software that logs the employee's keystrokes and sends the logs to the attacker. The attacker can then rummage through those logs and find out the employee's passwords and other important information.
- Gain access to the employee's files and monitor the employee's online activities and transaction details
- Turn the employee's computer into a “bot” that the attacker can use to send spam, launch denial-of-service attacks, or spread the virus to other computers on the network.

CISA's recommendations to help combat email-based scams

The following are a few recommendations by the CISA to help IT administrators keep their organization safe from email-based scams.

Educate employees

No matter how strong an organization's email security is, it only takes one unsuspecting employee to click a malicious link and put the entire organization's network and data at risk.

90 percent to 95 percent of successful cyberattacks start by phishing scams, while 37.9 percent of untrained employees will fail a phishing test.

Hence, one of the most sensible things for organizations to do would be to evaluate the level of understanding employees have over email-borne cyberattacks and educate them on the risks associated with negligent email use.

This is crucial, especially for small businesses, because they are often handicapped by limited resources to have adequate fail-safe mechanisms to recover from cybersecurity incidents. Fortunately, the cost of educating employees is far less than the average cost of a data breach.

According to Ponemon research, an average-performing cybersecurity program results in a 37-fold return on investment, while even the least effective training programs have a 7-fold return on investment.

Be vigilant about spam messages

If a particular employee is receiving an unusual number of spam messages, this might indicate that the employee is being targeted by an attacker. In worst cases, the employee might be a victim of email bombing. Email bombing is when an attacker sends huge volumes of emails to a target address in an attempt to crash the employee's email account or the mail server itself. If multiple accounts of an email server falls victim, this might even have a denial-of-service impact.

Due to the sheer volume of the emails the employee receives, some emails might even bypass the spam filters and get to the emloyee's inbox folder. Once this happens, it's only a matter of time until the employee opens the mail and walks right into the trap set by the attacker. In such cases, the IT administrator must quickly notify the employee(s) about the anomaly and block the domain by configuring the router to deny all the packets that originate from the attacker as a preventive measure.

To do this, the IT administrator must be able to have maximum visibility over spam messages that enter and leave the organization's mailboxes.

Using Exchange Reporter Plus' Mail Traffic reports, IT administrators can increases their visibility over the spam messages by:

- Viewing the list of top spam recipients over a specified period.
- Detecting malicious emails and listing the sender and recipient names, times emails are received, and more.
- Viewing details about spam messages such as sender, recipient, and more.

Regard unsolicited email with suspicion

A higher degree of caution must be exercised for unsolicited emails coming from external email IDs, as they have a higher chance of containing fraudulent links.

Subject lines with keywords traditionally used for fraudulent communications—such as secret, transfer, urgent, immediate, attention, payment, and so on—are most likely to be coming from a perpetrator. This is why it's crucial to screen the subject lines of all inbound emails.

Exchange Reporter Plus offers comprehensive Mailbox Content Reports report that help IT administrators to keep tabs on mailboxes that receive emails with subject lines containing commonly used keyword baits. These reports can also be scheduled to run at desired intervals so that suspicious emails do not slip under the radar of the IT administrator.

Treat email attachments with caution

If an employee clicks a malicious attachment and executes the file, the employee's computer will be compromised. The attacker can now use this compromised computer to gain an initial foothold and laterally move through the organization's network to further attack and abuse other computers in the network.

This is why it's important to spot these emails at the earliest and take proactive remedial measures before it snowballs in to security disasters.

With Exchange Reporter Plus, IT administrators can set up filters to inspect emails containing attachments with executable file extensions. Once configured, all the mailboxes that contain such attachments can be viewed in the "Attachments By File Extension Keyword," report which can be scheduled to run at desired intervals. This report also has information on the attachment file name, its extension and size, date it was received, and more.