ManageEngine
M365 Manager Plus

# How to protect your C-suite from **whale phishing attacks.**

www.microsoft365managerplus.com

# Introduction

According to Gartner research,[1] on average, one out of every 4,500 emails is a phishing attack. Phishing attacks involve campaigns attacking a large number of mostly low-yield targets, similar to shooting a large number of arrows and hoping one hits any target. Scammers deploy various phishing methods to penetrate an organization, such as gathering credentials using fake login pages and spreading ransomware or malware.

Over time, phishing campaigns have developed new methods, including spear phishing and whale phishing (also known as whaling); these strategies incorporate focused targeting and reconnaissance. Scammers now have access to emails harvested from data breaches or commercial lead generation sites, and can supplement this data with information gathered from various social media platforms to make their campaigns highly effective.

This increased sophistication, combined with the rapid increase in the number of phishing campaigns, is causing huge damage to organizations across the globe. According to Check Point Research's 2018 Security Report,[2] 64 percent of organizations have experienced a phishing attack in the past year. According to Forbes,[3] scammed C-level executives in the United States, UK, and Europe have sent more than $12 billion to attackers since 2013.

This e-book will focus on a type of targeted phishing campaign known as whale phishing. We'll discuss what whale phishing is and how it's accomplished, and outline the strategy of a whale phishing attack through a recent case study. Plus, we'll address how you can protect your C-suite from whale phishing.

# What is whale phishing and why does it work?

TechTarget[4] defines whale phishing as, "*a specific type of phishing attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company, as those that hold higher positions within the company typically have complete access to sensitive data. In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.*"

To understand whale phishing, we need to understand spear phishing. Spear phishing is a type of attack that uses scare tactics and urgency in emails to manipulate victims into sharing sensitive information. Whale phishing is similar, except the target is a whale, a very important executive in the organization with access to critical business data and documents.

For example, a high ranking official at Snapchat fell victim to a whaling attack in 2016. The attacker disguised the emails as if they were sent by the CEO, and the employee fell victim and disclosed the company's payroll data.

## Why do these attacks work?

Because they appear credible.
Whaling attacks are highly personalized and sophisticated. The phishing emails and credential harvesting websites are professionally designed to project a legitimate appearance. To bolster the legitimacy of these attack tools further, scammers also use the logos and contact information of actual companies or government organizations.

Scammers spend lots of time collecting information about their targets, especially from social media platforms such as LinkedIn, Facebook, and Twitter. By uncovering the maximum amount of information on the target's background, attackers are able to make the phishing campaign appear very authentic.

## How whale phishing works

The first step in whale phishing is identifying a high-profile target. Most C-level executives are active on various social media platforms. Scammers use multiple LinkedIn scraping tools, such as Inspy, to fetch the email addresses of these executives.

After the targets are identified, the attacker profiles them. Conducting extensive research, they use social media and readily available information from the internet to gather as much information as possible. This might include the target's phone number, information about their company and role, industry information and details about company conversations, the organizational hierarchy, and anything else that will make them seem legitimate.

Then comes the spoofing part. The attackers carefully construct bogus websites and spoofed email addresses that are tailor-made to fool their particular target. These websites and email addresses are convincing enough that even a cautious person might be deceived. The bogus websites may even get redirected to the authentic website after the necessary information is obtained, and the email addresses will be almost identical to the original ones with just minute changes, such as replacing the letter "o" with the number "0."

Once everything is prepared for the attack, personalized emails are sent to their respective targets. The emails might use various methods to attempt to extract information.

One common tactic is to use fear to pressure victims into performing a certain action. For example, the emails might say, "Your account password has been compromised. Reset your password now to stay safe!" Or, they might disguise the emails as coming from an insurance company by stating, "Your insurance policy has expired! Log in now to renew your insurance!" These types of emails might impose a time constraint to exert additional pressure on the target.

Another common tactic is to pretend that the email is from the CEO or another high ranking official at the target's company. These emails may request an immediate transfer of large amounts of money or highly sensitive information about the company, and state a seemingly legitimate reason.

Leveraging the popularity of SaaS, another successful strategy is creating fake login webpages to popular software services like Dropbox or Google Drive to gain the target's user credentials. Once the credentials have been obtained, the fake webpage may redirect to the organization's authentic website. This way, targets may not even realize they have been compromised.

## A recent case study

Obinwanne Okeke from Nigeria is the founder of Invictus Group, a business with interests in the oil and gas, telecommunication, construction, real estate, and agriculture industries. Okeke's business success landed him a place on Forbes' list of "Africa's 30 under 30" in 2016. In 2019, a US District Court issued an arrest warrant for Okeke for allegedly committing business email compromise (BEC) fraud to the tune of millions of dollars. One of Okeke's high-profile victims was the CFO of Unatrac Holding Limited, a global distributor of Caterpillar industrial and farming equipment.

How did Okeke manage to scam this C-suite employee?
According to the FBI, Okeke and his partners were involved in BEC scams starting in 2016. They created phishing webpages for various online services regularly used by businesses in the US. In April 2018, a phishing email was sent to the CFO of Unatrac Ltd. The malicious link directed the CFO to a spoofed Microsoft 365 login page. The CFO provided the requested credentials on the fake webpage, and those credentials were then captured by the attackers. Over a span of two weeks, the scammers accessed the CFO's account 464 times from Nigeria and initiated fund transfers from the company's internal finance team.

Their modus operandi involved sending fake invoices with Unatrac logos from external addresses to the CFO's account, and then forwarding those messages to unsuspecting employees on the payments team. To avoid the CFO's attention, the scammers marked the replies to these emails as read and then moved them to a different folder. In this manner, Unatrac ended up sending $11 million overseas, most of which couldn't be traced.

## How to protect your C-suite from whale phishing

To comprehensively secure C-level executives from falling prey to constant attacks from scammers, IT admins must implement a mix of technical and non-technical measures. These include:

## Creating awareness among employees.

Organizations must train the members of their C-suite to have a security-oriented mindset. Upon opening every email, executives should be concerned with the email content as well as validate the legitimacy of the email itself. They should always check the correctness of the email address before replying. If there are any urgent payment requests, especially involving huge sums, they should call to verify the legitimacy of the request before processing the transaction.

## Promoting the cautious use of social media.

Social media serves as a goldmine for information about C-suite members. Scammers often conduct detailed reconnaissance before initiating any attack, and they can uncover volumes of information about a C-level executive from various social media platforms. C-suite executives should enable privacy restrictions on their social media accounts.


## Monitoring logons, especially logon failures.

If a logon has occurred from an unusual IP or location, or at an unusual time, this could indicate the account in question has been compromised. IT admins should keep an eye out for such anomalous logon events and check for any spike in logon failures for any C-suite account.

Using M365 Manager Plus, ManageEngine's comprehensive Microsoft 365 reporting, auditing, monitoring, management, and alerting tool, IT admins can view details such as the IP from which a user logged on and whether the logon was performed during non-business hours. IT admins can receive details of logon failures due to incorrect credentials to keep track of brute-force attacks. They can also check the daily logon count per user to monitor an unusual spike in logons, as seen in the Unatrac attack.

## Enabling MFA for C-suite accounts.

Multi-factor authentication (MFA) is a crucial component to ensure secure access to an organization's network by protecting user identities and verifying that users are actually who they claim to be. By implementing MFA for all user accounts, and especially for accounts with privileged roles, organizations can prevent scammers from gaining access to critical devices and data, even if accounts have their credentials compromised.

While Microsoft 365 provides the option to implement MFA, IT admins need to work between different tabs to select users and configure necessary settings. M365 Manager Plus, on the other hand, simplifies this task by allowing admins to configure MFA for multiple users from a single console in just a few clicks.

## Monitoring inbox rules.

By setting up inbox rules, scammers can perform specific actions on the emails that arrive in a C-suite executive's inbox without their knowledge. For example, scammers can automatically move the spoofed emails and the replies to such emails to other folders, or delete them based on certain conditions.

M365 Manager Plus' Inbox Rules report provides the ability to generate the list of inbox rules created by any user. IT admins can then investigate if any new inbox rules have been created and whether they are legitimate requirements.

## Monitoring activity on sensitive files.

An organization's sensitive data, including plans for new ventures, information on mergers and acquisitions, and intellectual property, is a prime target for scammers. IT admins need to closely track and send alerts about suspicious activities on sensitive files to prevent any data loss.

IT admins can receive a comprehensive overview of all user activity on files in their OneDrive for Business environment with M365 Manager Plus' preconfigured File Operations report. Admins can also set alert profiles to help mitigate security breaches by providing notifications on critical changes to confidential files and folders in their OneDrive for Business environment, including information on files that have been deleted, moved, copied, renamed, and restored.

## Monitoring external emails sent to C-suite accounts.

IT admins must keep an eye on all emails from external email addresses that arrive in C-suite members' inboxes, especially messages containing payment requests.

M365 Manager Plus' content search feature helps IT admins achieve this. Using this feature, admins can quickly and easily find emails sent from external addresses. This helps verify the validity of the sender, and ensures IT admins are notified even if the scammers delete or move the emails.

Security professionals must have a deep understanding of business processes so they can devise the best techniques to protect their organization. Both user education and implementation of secure processes must go hand in hand to narrow the surface area of attack opportunities for scammers.

[1] https://www.apptio.com/emerge/trends/phishing-patterns-ai

[2] https://research.checkpoint.com/check-points-2018-security-report/

[3]https://www.forbes.com/sites/dantedisparte/2018/12/06/whaling-wars-a-12-billion-financial-dragnet-targeting-cfos/#3e494f687e52

[4]https://searchsecurity.techtarget.com/definition/whaling