25% of 'over-the-counter' phishing emails are the default security of Office 365

A recent report showed that as many as 25% of all phishing emails were found after researchers conducted a series of 55 million emails that had previously been Office 365 Exchange Online. Protection (EOP) - Office 365's default security program is marked as' clean 'and of course has been reached by users' inboxes, while another 5.3% is whitelisted. instead of being blocked by administrators.

A recent report showed that as many as 25% of all phishing emails were found after researchers conducted a series of 55 million emails that had previously been Office 365 Exchange Online. Protection (EOP) - Office 365's default security program is marked as 'clean' and of course has reached the user's inbox, while another 5.3% is whitelisted. instead of being blocked by administrators.

The rest of 69.7% of these fraudulent emails were blocked by Office 365 EOP, with 49% of them being marked as spam, and 20.7% tagged as "phishing."

1. The hyperlink test command is being used by hackers to perform DDoS

Overall, Avanan's Global Phish Report (2019 Global Phish Report) shows that for every 99 emails, one of them is malicious email used as part of phishing attacks. on how to send malicious attachments or links as a mainstream attack. This statistical result is also particularly interesting in the context that phishing attacks are considered to be a more serious security threat than malware.

To get these results, Avanan had to analyze about 55.5 million emails sent to organizations with between 20 and 100,000 employees using the Office 365 email platform and G Suite.

	EMAILS ANALYZED	PHISHING EMAILS	PERCENTAGE PHISHING
Office 365	52,379,886	546,247	1.04%
G Suite	3,120,114	15,700	0.5%
TOTAL	55,500,000	561,947	1.01%

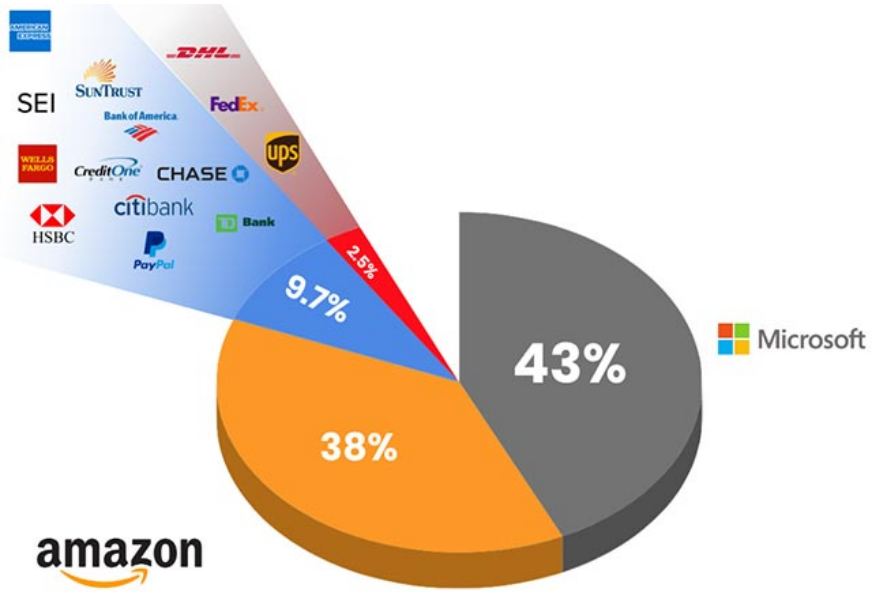
1. Danger: Hackers can target medical devices, change medical examination and treatment results

For Office 365, 546,247 out of a total of 52,379,886 emails tested were found to be part of phishing campaigns, accounting for about 1.04% of the total number of checked messages. On the other hand, the analysis also shows that about 0.5% of the 3,120,114 emails that G Suite users receive are phishing messages.

All emails analyzed by Avanan have previously gone through 'strict' rounds of default security tools on the platform.

"Our software connects through the API inside the cloud, creating a tighter inspection advantage than the usual solutions in default email security, which are only deployed in the outer ring (for example, like email gateways. For this reason, it can detect and analyze phishing attacks that have previously been compromised by default on Office 365 and Gmail, 'Avanan said.

In addition, malware scams are identified as the attack method used in 50.7% of 561,947 phishing emails, followed by collecting authentication information (40.9%), extortion (8%) and spearphishing (0.4%).



1. Reveal personal data of more than 1.3 million people from a vulnerability in web application

Besides, Avanan has also successfully excavated information that is quite interesting considering the indicators that can be used to detect phishing attacks, with 98% of emails containing electrical wallet addresses. (cryptowallet), and 35% of emails with links to WordPress websites are part of a scam plan.

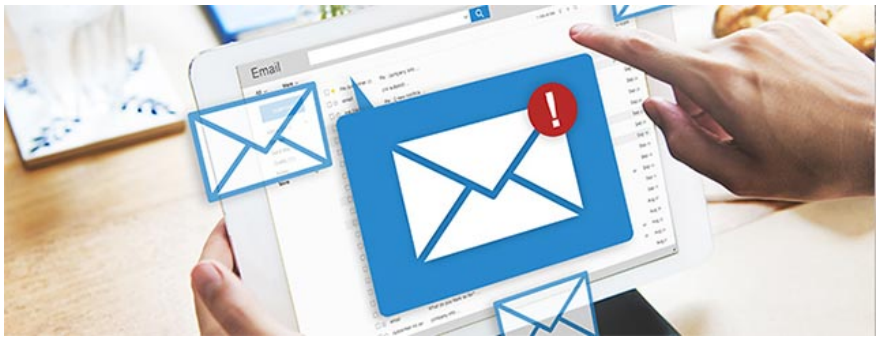
Brand fraud is also a commonly used form to disguise phishing emails coming from a variety of trusted brands. Specifically, the Microsoft brand has been used in 43% of phishing attacks and, for Amazon's case, about 38%.

Phishing attacks are often used by malicious agents to trick their victims into accessing the websites they control and design to collect confidential information, download attachments that contain parts malicious software, or entice the victim to click the redirect link to malicious websites and thereby infect the malicious code to their computer.

"Although it offers undeniable benefits, Cloud-based Email is also showing signs of becoming one of the main factors contributing to the start of a new era in phishing attacks, tricks and The nature of the cloud is much more flexible, the flexibility of operation as well as service delivery, and this inadvertently provides hackers with more attacks, copper it also gave them wider access to important data warehouses when a phishing attack was successfully implemented, 'said the top security analyst of Avanan Yoav Nathaniel.

1. [Infographic] 4 types of Phishing are easy to trap users

Payment data and login information are the top targeted factors



In some related news, Doctor Web researchers have also revealed a new scam approach discovered yesterday 11.4, disguised as a service to subscribe to newsletters from websites. of many trusted international brands, being used by crooks to effectively scam phishing emails as if they were completely reliable registration messages.

Last week, ProofPoint illustrated how phishing campaigns are actively targeting many tax agencies with the help of phishing emails that look real, combined with malicious attachments.

In addition, the March 2007 Microsoft Office 365 Threat Research team also found that customers of Netflix and American Express (AMEX) were targeted by two other phishing campaigns with the help of code. It is intended to steal credit card and debit card information, as well as many other important personal information of victims.

1. [Infographic] How to recognize and prevent Phishing attacks

A previous phishing campaign was also discovered in February while trying to steal both Google and Facebook login information by disguising it in the Google Translate tool on mobile browsers. This sophisticated phishing campaign is found by members of the Security Intelligence Response Team (SIRT) belonging to the Akamai team.