Hunting Phishing: 82% of senior leaders believe phishing attacks are becoming harder to identify

GetApp’s latest study surveyed 349 employees and 215 SME senior/executive managers and owners who received one or more phishing attacks at work, to better understand how these threats are manifesting.

Temps de lecture : minute

25 October 2023

The art of war has, unfortunately, always been at the minds of Men since the dawn of time.

Starting with Australopithecus fighting with sticks and bones, as depicted in the Kubrick classic "2001: A Space Odyssey", humanity has since developed more efficient techniques, and has shown some genius-like qualities when elaborating them.

Spikes, bow and arrow, swords, catapults, Trojan horses... Ingenuity has prevailed as we were looking for new ways to eliminate one another.

However, History is not only made of conquerors, but also of those who resisted. No matter how smart, no matter how tough attacks can be, some will stand up and protect others, preserve what matters.

If the ruse is sly, let us be smarter. If the Trojan horse enters the city, let us tear it apart.

In its latest study, GetApp teaches us how to protect ourselves, spot and fight phishing.

Panic amongst entrepreneurs

More than two-thirds (67%) of *GetApp*’s respondents have experienced multiple phishing attacks at work, whilst 73% faced numerous attempts on their personal devices. Moreover, 82% of senior leaders stated that these attacks are also becoming harder to identify.

Phishing attacks are a cause for concern for 94% of senior leadership surveyed in GetApp’s study, whilst nearly a third defined it as a serious concern. The biggest cause for worry for senior leaders was the loss of customer private data as well as the financial loss that phishing attacks cause. Company financial data leaks were the second biggest concern, followed by the loss of employee data.

94% of respondents received a phishing attack via email, whilst 22% via text message, and 15% via phone call. The five most common types of phishing attacks include:

- Impersonations of companies.
- Impersonations of a bank.
- Package delivery.
- Disguise as a government agency.
- Impersonation of a co-worker.

The majority of respondents surveyed (69%) reported an incident of phishing when it occurred at work. 40% ignored or deleted the message. Meanwhile, 10% opened the message but didn't click on the link. 3% clicked the link, and 1% provided the scammer with company information.

The growth in phishing attacks is not a great surprise. This aligns with the findings of the latest *UK Government Cyber security survey* where phishing was identified as the most common type of cyber attack by businesses in the country.

There are many potential negative outcomes that can occur as a result of phishing. Yet, the biggest causes for worry according to senior manager respondents were the possible loss of customers' private data and financial losses.

Beware the emails

Phishing often takes the form of a digital message. Emails and SMS phishing (or 'Smishing') offer quick and easy ways to trick employees. However, some cyber criminals also use other means such as robocalls and hacked social media posts to acquire sensitive information from targets.

Therefore, knowing where to focus attention on security operations and training is important as hackers can employ many different types of phishing attacks. As a modern business relies on its digital communications, that may be exactly why cyber criminals seek to exploit them.

A significant element of phishing emails and calls is that they take on the appearance of communications from trusted entities. This makes it harder to detect that the attack is happening and allows the scammer to gain the trust of the target more easily.

It's most typical for companies to be impersonated, with half of the phishing messages taking this form. However, there are significantly more trusted organisations such as banks, government agencies, and even coworkers being impersonated in phishing messages.

These kinds of risks underscore the importance of *staff training in security awareness*. It is wise to keep employees informed of these new and more underhanded kinds of attacks that can occur. This way, people can be on the lookout for more realistic and specialised impersonations.

However, the surveys also shows that a majority of respondents took the time to report an incident of phishing at work. All hope is not lost.

Brace yourselves

Being prepared to deal with these dangers, therefore, could be a major challenge for companies. Although, it is one that they must be ready to respond to.

It is important that SMEs consider mitigation methods such as putting in place security filters within email systems to limit the number of spam messages that successfully get through to an employee's inbox. Additionally, it is essential to have a plan set, cybersecurity expertise available, and the correct training and software implemented to fight back if an attack succeeds.

> *“Phishing is still an issue to keep an eye on judging from these findings. There’s a strong feeling amongst participants that attacks are increasing in frequency and the majority of SME senior managers believe they are getting harder to spot. This remains a major concern for email messages, with the vast majority of attacks coming from this source according to our data. This might prove especially problematic as about a quarter (24%) of our sample reported that they have received phishing messages impersonating coworkers, therefore extra caution from staff is necessary to catch some of these more nefarious methods*

> *before they cause serious harm." says David Jani, Content Analyst at GetApp UK.*

Article écrit par Paul Ferretti