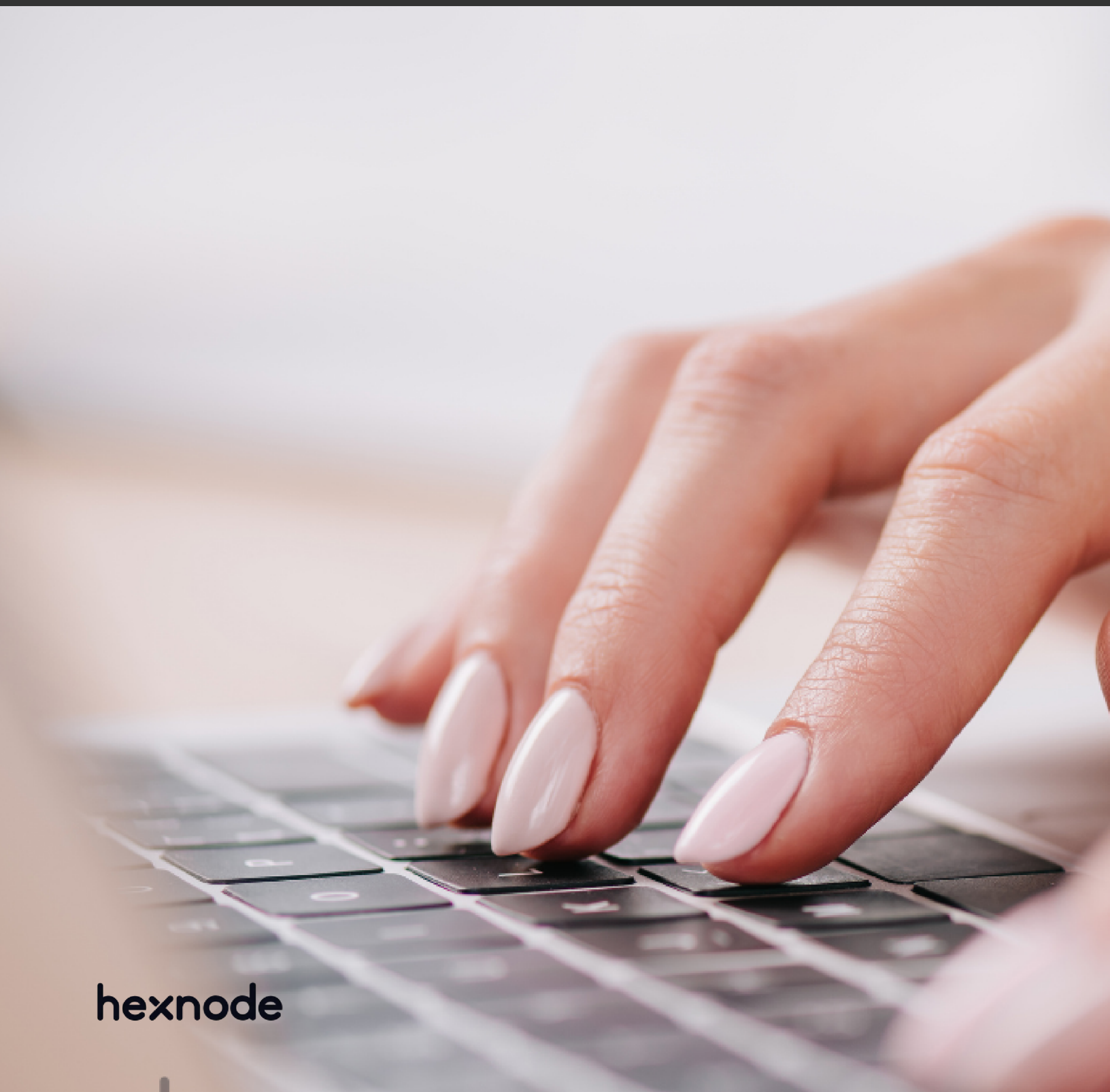
How UEM helps in protecting your organization from phishing attacks



hexnode

Phishing attacks bait unsuspecting users into downloading a malicious file or clicking on a link, which results in the system getting flooded with malware. These social engineering attacks are carried out by malicious actors who cleverly disguise themselves as being a part of a business or entity familiar with the targeted user. Though phishing attempts are commonly seen in emails, they can also surface as unsuspecting text messages or pretty much anywhere online.

These messages are often accompanied by a sense of urgency, which compels the user to perform various actions against their better judgment. Cyberattackers love to play on emotions and pressure. They usually take the effort to get to know the user before sending out these well-crafted messages that are personalized to capture the reader's attention at once. Most users usually fall into the trap and essentially hand out what these attackers need on a silver platter.

How widespread are phishing attacks?

Let's just say they've risen to a level worrying enough for organizations to seriously think about educating their staff on the dangers of these attacks. According to the report published by APWG, December 2021 recorded the highest monthly total of phishing attacks since 2004. The pandemic offered the perfect opportunity for these attacks to triple in the past two years. The early days of the pandemic were fraught with confusion and attackers were quick to seize upon this and spread havoc amongst users working remotely.

The financial sector became the most frequently targeted industry, being responsible for 23.2% of the phishing attacks. Attacks were also reported against webmail and SaaS providers, accounting for 19.5% of the attacks. Some of the other targeted industries in the final quarter of 2021 included:

- ECommerce/Retail – 17.3%
- Payment – 9.3%
- Social Media – 8.5%
- Cryptocurrency – 6.5%
- Logistics/Shipping – 4.1%

Phishing attacks should be taken as a serious security threat. Organizations can reduce the number of victims among their staff by offering periodic security training where employees can be taught to identify a phishing email and the various ways in which they can be targeted. You can adapt basic security measures within your organization to ensure users have their devices' passwords enabled and encrypted to protect any sensitive information they may be handling within the company.

Why prevention would be better than cure – understanding the ins and outs of phishing attacks

The phishing and fraud report released by F5 Labs gives us an idea of how these phishing attacks are carried out. The three most commonly used methods include:

- General – unrelated victims are targeted
- Semi-targeted – attacks are carried out on a specific organization or a group
- Spear phishing – a specific individual will be targeted

Why are these attacks carried out?

Some of the prime objectives behind phishing attacks are to:

- Access sensitive information for financial gain
- Download malware to gain access and control the victim's system
- Collect credentials to commit financial frauds or theft of intellectual property
- Circumvent app permissions to gain access to user's contacts and inbox

While these might not be all the objectives for phishing attacks, the primary motive behind these attacks would always be monetary gain. Now that we got the objectives behind these attacks cleared off, the next question would be to figure out who or what is at risk here when the attacks are being carried out? It would obviously be your organization and your employees. Not only will sensitive information leak out, but it would also damage the credibility of your employees and staff as well.

What are the common types of phishing attacks?

The best way to avoid being the next victim of a phishing attack is to identify the one that comes your way. Although there is a wide range of phishing attacks, these are some of the most widespread ones.

Email phishing

Malicious actors would send out emails to users impersonating themselves as a reputable brand or a person familiar with the user. They make use of various tactics well known in social engineering attacks to create a sense of familiarity that leads them to click on a link that directs them to websites to steal user credentials or inject malicious code into the system.

There are various ways in which you can spot a phishing email. These include looking out for the wrong domain within the sender's email address, identifying a lot of misspelled words within the email content, and checking out for shortened links. These links are shortened to bypass Secure Email Gateways.

Spear phishing

Spear phishing targets a specific individual. It begins with the attacker gathering information on the targeted individual through social media sites or company websites. These targeted individuals are often IT admins or executives. They create a sense of genuinity within these attacks by using real names and email ids of actual people from working within the organization. Perceiving this as an urgent internal request, the user would proceed responding to the mail, thus setting the wheels in motion.
So, what can you do? Look out for internal requests that seems out of place, such as getting an odd email from someone from another department. Be wary of password protected documents. This is usually a scam by malicious actors to steal your credentials.

HTTPS phishing

HTTPS or hypertext transfer protocol secure is often considered much safer to click as they use encryption to heighten the sense of security. Cybercriminals make use of HTTPS links within their phishing emails to throw off any suspicion users may have about the emails being authentic.
As stated earlier, it's always best to be wary of shortened links. Make sure the link is in a long-tail format and clearly shows all parts of the URL.

Angler phishing

Social media is another popular site for phishing attacks. Attackers make use of the various messaging features within the social media platform to entice users into performing a particular action. Look out for any abnormal direct messages. Getting a direct message from a user who rarely uses these features is a major giveaway. Never click links in a direct message even if it seems to be legitimate.

Clone phishing

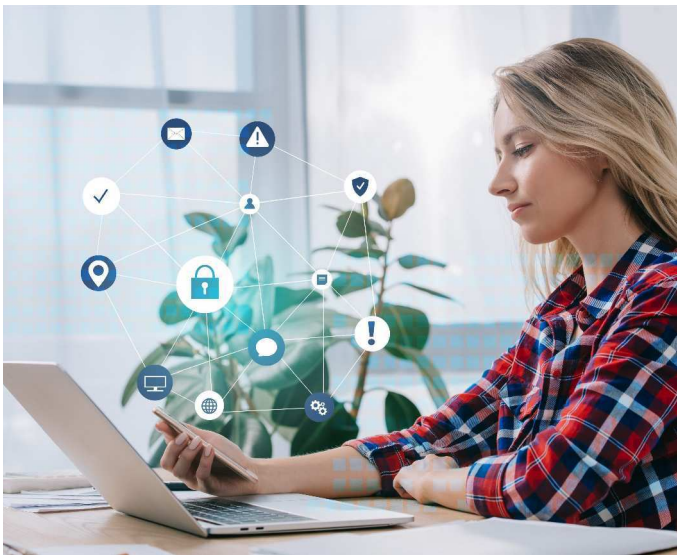
This is yet another commonly used phishing attack where the phished email has been cloned to resemble the original message sent by the organization. Due to the legitimate nature in which these emails appear, users could be easily tricked into responding to these email messages. Cloned phishing attacks are carried out to trick employees into giving away passwords and other credentials which can later be used to access enterprise applications and other records.
One of the reasons why clone phishing attacks are harder to spot is because they are well crafted and go undetected for several days until the damage is done. Organizations should make sure their security measures are strong enough to make sure cleverly disguised attacks such as these are spotted well in advance.

Some of the ways in which you can spot a clone phishing attack include getting an email from a service provider at unexpected times and looking out for emails that request personal information. Always make it a point to scan the attachments you get for malicious codes or viruses.

What are some of the best practices to prevent phishing attacks?

- Provide users with the right tools with which they can guard themselves and the information they work with.
- Give them periodic training sessions in which they can be educated on the role they play in upholding information security within the company.
- Conduct mock phishing scenarios.
- Patch all systems with the latest security updates.
- Develop a policy that urges end users to regularly update their passwords and increase their complexity.
- Deploy web filtering to block access to malicious websites.
- Encrypt all sensitive information handled within the company.
- Set adequate restrictions in place to prevent users from needlessly browsing through the internet, this minimizes the chances of phishing attacks from happening.
- Enable the use of spam filters to filter out blank emails and other suspicious emails from reaching the inbox of users.
- Use two-factor authentication to prevent hackers from accessing user credentials.
- Ensure all users connect to VPN to access corporate resources.
- Have systems in place where users can quickly report phishing attacks.
- Prevent users from sharing their passwords.
- Use SSL certificates to secure traffic flowing in and out of your website.

Where does UEM help in remediating phishing attacks?



Organizations are relying on multiple SaaS-based solutions to keep specific security configurations in check, and manage passwords, applications, and overall security of the devices in general. A Unified Endpoint Management (UEM) offers all of these capabilities from a single platform, saving admins from the trouble to rely on multiple tools instead. Here are some of the ways in which a UEM helps organizations deter phishing attacks to a large extent.

Endpoint protection

Various restrictions and security configurations can be set on the device to protect it from any unauthorized changes. Users can be restricted from making any changes to the device settings or unknowingly enabling any app permissions that could put the data stored within these applications at risk. The devices can be monitored on a continual basis to detect the presence of any threats and give real-time alerts to admins if any threats are spotted.

Encryption

Encryption safeguards the data by converting the plain text information into ciphertext. So, even if an attacker manages to intercept the mail, they would not be able to read it. Encrypting emails is extremely helpful in minimizing phishing attacks as it helps keep sensitive information safe when sharing it online.

Web filtering

Web filtering helps block access to malicious websites. It helps prevent viruses and malware from hooking onto the systems and exposing sensitive information to hackers and other external parties.

Patch management

This helps fix any vulnerabilities that could expose your systems or applications to cyberattacks and other threats. With the help of a UEM solution, applications can be

silently upgraded to its latest version without requiring any user intervention. You can schedule OS updates during off-hours to ensure productivity does not get affected.

Secure access to networks

Configure email settings to make sure only authorized users are connected to your corporate network. Enable the auto-join feature to ensure users don't have to remember complex passwords to connect to your network. It also minimizes the chance for them to share these credentials with other users.

Conclusion

The best way to mitigate phishing attacks is to provide adequate security training and educate users on the ill effects these attacks can bring on themselves and the organization they work for. Conducting these training sessions on a periodic basis helps users develop good habits when sharing sensitive information online. You can send out fake emails to users to test them out and evaluate the way in which they would respond when confronted with an actual attack.

Organizations have often underestimated the havoc phishing attacks can bring. They often target privileged user accounts where it's easier to get in touch with individuals with access to company confidential information. Implementing proper access controls helps restrict access to sensitive data and protect it from leakage.