A COMPREHENSIVE GUIDE TO PHISHING FOR BUSINESS PROFESSIONALS

STAGE2DATA

CONTENTS

1. INTRODUCTION

Phishing continues to be the most common form of cyber-attack due its simplicity, effectiveness and high return on investment. It has evolved from its early days of tricking people with scams of Nigerian princes and requests for emergency medical treatment. The phishing attacks taking place today are sophisticated, targeted and increasingly difficult to spot.

2. WHAT IS PHISHING AND HOW DOES IT WORK

Phishing (aptly derived from the analogy of an angler throwing out a baited hook) is a form of cyberattack using a disguised email as its weapon. Its aim is to trick the recipient, using the disguised email, into believing the message is something they need to read or have to open (or click on the link or download the attachment contained in the email). It could purport to be an email from the recipient's bank or an attachment supposedly from a colleague.

What differentiates phishing from other forms of cyberattacks is the insidious form of the message; cybercriminals masquerade as a trusted entity (or person), usually a person known to the victim or a company the victim is likely to transact with. It's one of the oldest forms of cyberattacks with the first instance dating back as far as the 1990s. Yet, it is still one of the most prevalent and pernicious attacks and the techniques are becoming more sophisticated every day.

What is especially disturbing is that even cybercriminals with negligible technical skills can now launch phishing campaigns thanks to phishing kits available on the dark web. The latter bundles phishing website resources and the tools required to execute the attack, ready to be installed on a server, whereafter the attack can simply start sending out phishing emails.

Recent phishing attacks that made waves:

- One of the most significant phishing attacks entailed getting Hillary Clinton's campaign manager, John Podesta, to offer up his Gmail password.
- Financially, the story of Walter Stephan, an Austrian aerospace executive, takes the bait for the largest sum of money scammed in one single attempt: $47 million.
- Retailer, Target, suffered a massive data breach when falling victim to phishing attack which affected 110 million customers.

The common denominator among phishing attacks lies in its disguise. Cybercriminals spoof email addresses so impersonate legitimate people and set up fake websites to impersonate websites that users trust.

3. FIVE TYPES OF PHISHING

Phishing attacks are becoming progressively clever and easy to launch. The convenience of phishing kits available to purchase on the dark web renders it easy for cybercriminals, even with minimal technical skills, to launch phishing campaigns. The emails used to execute the phishing attacks are also carefully crafted to avoid suspicion to ensure victims open these emails.

From the headlines, it is also clear that some phishing scams have been very successful and made international waves such as when hackers obtained access to Hillary Clinton's campaign chair, John Podestra's, Gmail account. Or when private photos of several celebrities were made public after, what was thought to be an insecurity on Apple's iCloud turned out to be successful phishing attacks. In 2016, employees of the University of Kansas also fell victim to phishing when they responded to a phishing email and handed over access to their paycheck deposit information.

Below five types of phishing attacks that people fall victim to are detailed.

(i) **Vishing**
This form of phishing occurs via phone calls and instead of emails, voice is being used to execute a vishing attack.

(ii) **Smishing**
Also known as SMS phishing, this is one of the easiest types of phishing attacks where the victim is targeted using SMS alerts. Smishing victims will usually receive a fake direct mes sage or fake disruptive event message with a cancellation link. This link redirects to a fake page designed specifically to collect personal and sensitive details.

(iii) **Search Engine Phishing**
This type of phishing entails creating a fake webpage that targets specific keywords and then waits for victims to land on this fake page. Once the victim clicks on the page link, he or she is hooked.

(iv) **Spear phishing**
In contrast to traditional phishing that relies on bulk emails being sent to millions of users, this form of phishing is targeted in nature. The emails used to execute this attack are care fully drafted to target a particular type of user after thorough research of the potential target has been conducted through their social media and business profiles. It is used on both individuals and businesses.

(v) **Whaling**
This is the big one, no pun intended. Whaling is similar to spear phishing, but the targeted group is even more specific and refined. It targets, for example, CEOs, CFOs or COOs (in other words senior management) and industries such as technology, banking, and healthcare as they are considered the big players in the information chain of any organization.

4. WHAT DAMAGE CAN PHISHING CAUSE TO YOUR BUSINESS?

A cyber-attack costs a small business on average $53 987. Although this is much less than the cost associated with cyber-attacks on medium and large enterprises that easily escalates to millions of dollars, when considered from a proportion to size point of view, it is substantial. One of the ways hackers wreak this havoc is by using phishing attacks. There are several different forms of phishing attacks which depend on the end goal of the scammer using them.

Phishing statistics released by Avanan show that 1 in every 99 emails is, in fact, a phishing attack. Of these phishing emails, 2 in 3 use either a malicious link or embed malware in the email. This amounts to 4.8 phishing emails per employee when calculated based on a five-day workweek. This is very alarming if you further consider that 30% of all phishing emails make it past IT security. The very success of this scam has encouraged and emboldened scammers to increase their attacks. In this regard, Avanan points out that phishing attacks increased with 65% from 2016 to 2017 and in 2018 alone, 83% of people received a phishing email or fell victim to a phishing attack. It has a massively damaging effect on productivity (67%), data loss (54%) and reputational damage (50%).

As mentioned above, the damaging effect of phishing attacks is most severe on productivity, reputation, and the loss of data.

At a fundamental level, brands are built on trust. When a phishing attack, therefore, results in, for example, the public disclosure of embarrassing or damaging emails, it tarnishes an organization's brand irreparably. This is in addition to the normal backlash associated with phishing attacks. Just consider recent headlines: "British Airways data breach: Russian hackers sell 245,000 credit card details" and "Uber concealed massive hack that exposed data of 57m users and drivers". No matter how formidable your organization, headlines such as these can damage an organization's reputation for years to come.

Despite brand being the foundation of an organization's market capitalization, data loss can be the most devastating loss of all. Statistics indicate that in 2018, 24% of organizations targeted by phishing experienced major data loss. Spear-phishing (the type of phishing utilized to target data) is aimed specifically at stealing sensitive information such as account credentials or financial information to use for nefarious purposes.

Finally, a combination of loss of reputation and loss of data equals a substantial decrease in productivity. Time will have to be devoted to recovering from the phishing attack, especially in the event of an attack involving malware, in which case employees may be distracted and systems need to be taken offline which may render some employees unable to perform their operations. This further translates to monetary losses for the organization.

5. TIPS TO SPOT PHISHING BEFORE YOU TAKE THE BAIT

Phishing attacks are one of the most prevalent and common security challenges for both individuals and organizations attempting to ensure the security of their information. Whether it's obtaining credit card information, or gaining access to passwords and other sensitive information, email, social media and telephone calls are just some of the communication forms hackers use to steal valuable data. Businesses are, of course, a particularly viable target.

To assist organizations to better understand how they can avoid falling victim to phishing attacks we have compiled a list of the ten most common ways organizations fall victim to phishing attacks and how to prevent them.

(i) Employers do not adequately train employees on their role in data security

Cybersecurity is a marathon, not a sprint. To minimize careless cybersecurity mistakes and to encourage employees to be vigilant, consistent cybersecurity training is necessary. Security issues should always be a top priority for employees, it is, therefore, important to keep your staff informed of phishers' latest techniques and phishing methods as well as the impact of a breach on the organization and on the employee him- or herself.

(ii) Employers do train employees and implement policies, but they never test the policy or effectiveness of the training

There are certain programmes and products that can send test phishing emails to corporate staff which provide metrics regarding security leadership and how effective an organization's anti-phishing programme really is. When performing phishing attempts against your own employees you can gauge their response and how they handle phishing attempts. This will indicate if your employees are ready to handle such intrusion. This also goes hand-in-hand with testing management to see if they are adequately enforcing the policies. Training, as mentioned above and testing is crucial as it takes only one or two users to compromise an entire system.

(iii) Employees are careless about their browsing habits

Employees can significantly reduce their odds of falling victim to a phishing attack by being sensible and applying some common sense while browsing online or checking emails. Always browse security with https and never click on website links if you are not absolutely certain it's authentic, rather type the URL into the address bar manually. You can further deploy a web filter to block malicious websites and ensure that your devices, email and applications are updated regularly to include the latest security patches.

(iv) Organization forego a coordinated and layered approach to security

Defending against phishing requires a layered approach to security that includes employees and IT preventative measures such as single sign-on (SSO) and strong authentication (to eliminate the need for employees to manually enter passwords to access systems, applications or information), browser add-ons and extensions (to prevent users from clicking on malicious links) and implementing spam filters.

(v) Organizations do not keep abreast of the ever-evolving phishing threat

With vast amounts of corporate data at risk, it is imperative for organizations to guard against the ever-evolving phishing trend. Cybersecurity threats, including phishing, how it works, the types of phishing attacks to be aware of, and so forth, should be high on the list of "must-knows" as it targets everyone in the organization: from the executive leaders to the administrative staff. Phishing scams are only going to mature over time which makes it imperative to remain vigilant and to safeguard data (your own personal data as well as corporate data) that may prove costly in the long run.

6. HOW TO PROTECT YOUR BUSINESS AGAINST PHISHING

Phishing scams are geared towards infiltrating your system in order to gain access to usernames, passwords and sensitive information such as credit card details. These scams are, unfortunately, also very common and often appear real. There are, however, steps that you can take to protect your business against phishing attacks.

With the average cost of a successful phishing attack estimated at approximately $1.6million for an SME, it's vital that you know how to identify a phishing scam and educate your employees about the risks associated with it.

(i) Prevent phishing emails from reaching users

The best approach to this preventative measure is to deploy specialized anti-phishing software either focused on cloud-based email or on-prem behind a firewall. There are a number of options available, each with its own unique set of capabilities including identifying malware attachments, man-in-the-middle attacks and spear-phishing emails. The overall aim of this software is to prevent suspect emails from reaching users' inboxes.

(ii) Update your software

Even with the specialized software mentioned above, it remains crucial to keep your software updated. Phishing attacks exploit outdated software therefore you should install updates for everything you're using, even something as innocent as a PDF reader, as it could ultimately become a security hole.

(iii) Train your employees on safe practices

It is equally important that your employees, as the most likely targets of phishing, are aware of the dangers and consequences of phishing. You have to ensure that everyone is on the same page and following the appropriate security guidelines regarding phishing to the letter.

(iv) Use two-step verification

When signing in with both a password and a second factor (either a security key, OTP sent to your mobile device or an authenticator app) adds an additional layer of security and helps to protect your accounts from phishing attacks.

(v) Conduct mock phishing attacks

Further to continuously training your employees it is also a good idea to send "mock" phishing emails to test their reaction to a (perceived) real phishing email. You can monitor your backend to see whether your employees either click on the link, report it, or send it to spam. It's a small exercise that can go a long way!

7. CONCLUSION

Phishing, it seems, is here to stay and we have to educate ourselves to avoid becoming part of the statistics. Stage2Data partners with world-class security software solutions providers to offer robust, multi-layered security products to combat next-gen malware, ransomware, and other enterprise threats. For more information, please get in touch.

ABOUT STAGE2DATA

Stage2Data is one of Canada's fastest growing and most trusted cloud solution providers. Since 1998 we have been a trusted data management company providing 100% Canadian data solutions. It has been proven by thousands of North American companies that we manage data securely and IT costs effectively.