CORE SECURITY
NEWSLETTER

Volume 1

Issue: 11.10.21

INSIDE THIS ISSUE

PHISHING SCAM

THE THREAT

Phishing is one of the most dangerous forms of cyber-attack as it preys upon and entices victims using the system they come to trust. The cybercriminals will use the information to create elaborate emails that will ensure the success of the attack.

Spear Phishing begins with the cybercriminal gathering and finding out information about the target company and then using that information to build a profile of the intended target. Third, the target is then sent a well-crafted email to move the intended target into action. Unfortunately, the moment the victim clicks on the email, it is too late.

Businesses lose billions each year because of phishing attacks, and the problem is only getting worst.

PHISHING FACTS

STATISTICS

98% of cyber-attack begins with a phishing email

20% of all employees click on phishing email links

67% enters their credentials on a phishing website

Webmail and (SaaS) users are targeted most

72% of phishing attacks use GMAIL as a vector of attack

Most BEC is sent from free webmail providers

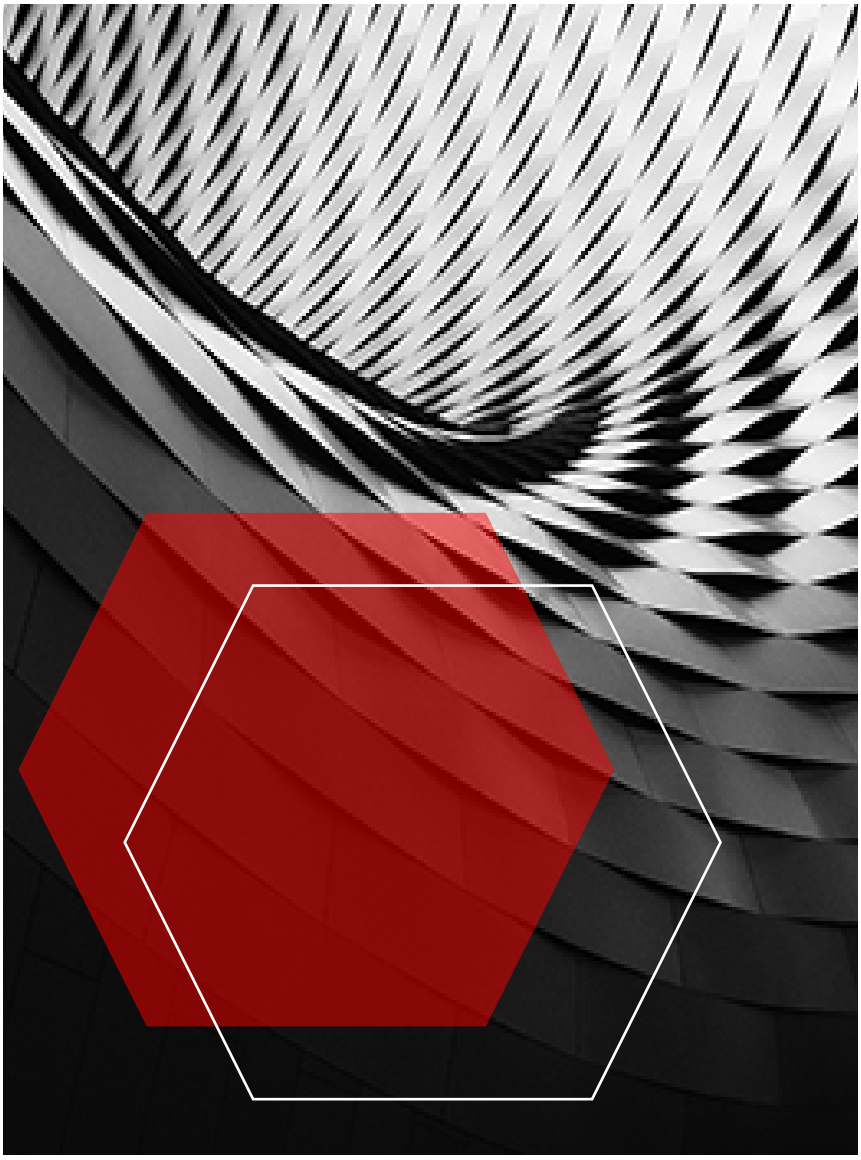
THE PHISH BAIT

BE AWARE

Just like going fishing, you first need to prepare the bait. In the attacker's case, it's finding out intimate details about their target, in this case, an organization or an individual–Information such as products, services, or affiliations.

Attackers harvest information from various sources such as social media to aid in their attacks. This detailed information enables the attacker to craft a compelling email that convinces the target it is from a reliable and trusted source; therefore, it is safe to click on the link in the email.

The unaware user has unsuspectingly released malware within the organization's network infrastructure by clicking on the link. This release of the malware will have a severe impact on the target as it traverses the network.



THE PHISH HOOK

DON'T BE HOOKED

The information is collected, so now the cybercriminal will design the hook for the catch.

In a scam, the hook can be anything. The attacker will design the scam based on information gathered to appeal to the particular victim's vanity or sense of urgency, for instance, inform the victim their bank has been hacked. Therefore, they need to log in and change their password. This notice will instill a sense of urgency in the victim to act immediately and without hesitation, thereby playing into the attacker's spider's web.

THE ATTACK

BE AWARE

This phase is where the actual attack happens. The attacker sends out the email and waits for the victim to act upon it. The attacker's actions here will depend on the purpose of the attack. The sent email will have parameters, e.g., the collection of credentials to escalate the phishing attack within the organization.

The attack can provide the attacker with crucial information about the company and its inner workings.

A favorite of attackers is the email addresses of c-level executives. These addresses can be used for nefarious reasons, such as authorizing or instructing unwitting employees to transfer large sums of money to a fake account.

The attack can be used to target third parties, vendors, and customers alike. Therefore, when companies implement an awareness process, they should include not only staff members but "Third Parties and customers' to ensure they are kept informed of phishing threats that may or may not affect them. In addition, the process should include affiliates as well. Not doing so may expose them to dangers, which may further complicate the already complex problem in the form of legal actions against the organization.

AWARENESS TRAINING

READINESS IS KEY

Like any aspect of readiness, awareness education and training are crucial frontline processes for defending your business.

Phishing can be done in many different ways. There isn't one fix-all solution that can prevent or solve it. Employees are an effective first line of defense when they are adequately trained. The human factor will always be a risk. However, studies have shown that well-trained employees are an effective first line of defense for an organization.

Companies should implement an automated and targeted awareness program that ensures each segment of the company workforce is adequately trained in their roles and responsibilities for information and cyber security. This program should include posters, computer screensavers, periodic and unexpected testing to ensure the security readiness and awareness remain constant in employees' minds.

An awareness process that keeps security fresh in the minds of its employees is vital in protecting the company, its employees, and customers.

CONCLUSION

Security is an important topic for all companies. Having an effective security process in place that ensure the regular training of staffs is a key "First Line" of defense measure that will aid in the security of the organization.

A fundamental aspect of a good security strategy is an Incident Response (IR) process. An effective IR process is vital in the time of crisis, as it enables stakeholders to carry out their task effectively should an incident occur and without hindrances. This process also allows an organization to notify its partners, vendors, and, most importantly, customers affected by the incident.

As an extra added measure, companies should invest in some form of cyber insurance. Then, if an incident happens, they are covered. Many insurance providers offer cyber insurance, so you should choose the one best suited for your organization.

Wayne J Shaw CEO

CONTRIBUTORS

Contributor (s) to this edition of the newsletter.

Wayne Shaw is the Founder and Managing Director of CORE.

CORE is a Managed Security Service Provider (MSSP) that provide selective cybersecurity services and solutions to clients, such as Penetration Testing, Simmulated Phishing Test, Awareness Training, Security Consultation, Security Resource, IT Security Audit, Security Policy Development and more.

Contact us for more information.

The CyberStorm newsletter is a monthly publication by CORE Security.

C O R E S E C U R I T Y

WE PROTECT YOUR BUSINESS

https://coresecurity.co.jp
info@coresecurity.co.jp