Phishing:

Still the Single Most Utilized Exploit of Cyber-Criminals

And What Can Be Done About It

Global Learning Systems

June 2019

STILL THE SINGLE MOST UTILIZED EXPLOIT OF CYBER-CRIMINALS

Most organizations have invested heavily in the latest security technologies with the goal of securing their computing networks. They've also developed and implemented policies and procedures that help them to operate efficiently and meet legal and regulatory requirements. Yet losses to security breaches for these same organizations continue to grow each year. This is usually the result of a lack of security savvy among internal end users.

Phishing exploits attempt to acquire sensitive information such as usernames, passwords, credit card details, money or intellectual property by masquerading as a trustworthy entity in an electronic communication. Communications pretending to be from popular social media sites, auction sites, banks, payment processors, IT administrators and other trusted sources commonly are used to lure victims. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is just one type of social engineering technique used to deceive users, but it remains among the most dominant and effective attacks being used by cyber-criminals today.

All too often security breaches are caused by users doing something that they shouldn't do, such as clicking a malicious link in an email message, opening an infected email attachment, using weak passwords, losing laptops or phones, or being tricked into giving up their credentials through social engineering attacks. Recent significant crime and cyber-attack data from law enforcement and industry supports this conclusion and includes the following:

- According to Verizon's 2018 Breach Investigation Report, 92% of Malware is delivered by email.
  - 77% of recent compromised attacks were file-less.
  - According to a recent briefing provided to the public by the Federal Bureau of Investigation (FBI), over 80% of all of successful data thefts that occurred last year began with an end-user error such as clicking on a malicious link, visiting a viral website, or opening up a contaminated file.
  - Security Technology Provider SonicWall recently reported that over 90% of cyberattacks began with a spear-phishing email.
- Targeted phishing attacks are the top security threat faced by IT Security decision makers, according to a 2018 global threat report published by CyberArk.

ALL TOO OFTEN SECURITY BREACHES ARE CAUSED BY USERS DOING SOMETHING THAT THEY SHOULDN'T DO

WHAT DO WE KNOW ABOUT THE PREVALENCE OF PHISHING?

THE LATEST STATISTICS

The Anti Phishing Work Group (APWG) is a coalition of organizations that is unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities. APWG's quickly expanding global membership has grown to more than 1,800 institutions worldwide. This footprint positions it as one of the single best sources for data relating to phishing exploits and cybercrime. Every quarter the APWG publishes a Phishing Activity Trends Report that analyzes phishing attacks reported to the APWG by its member organizations and others that report attacks through the organization's website and by email submission. On March 4, 2019, the APWG released its 4th Quarter 2018 Report and the data within it indicates that every year and every quarter, phishing attacks remain on the rise.

According to the report:

The total number of phishing sites detected by APWG in 4Q was 138,328.

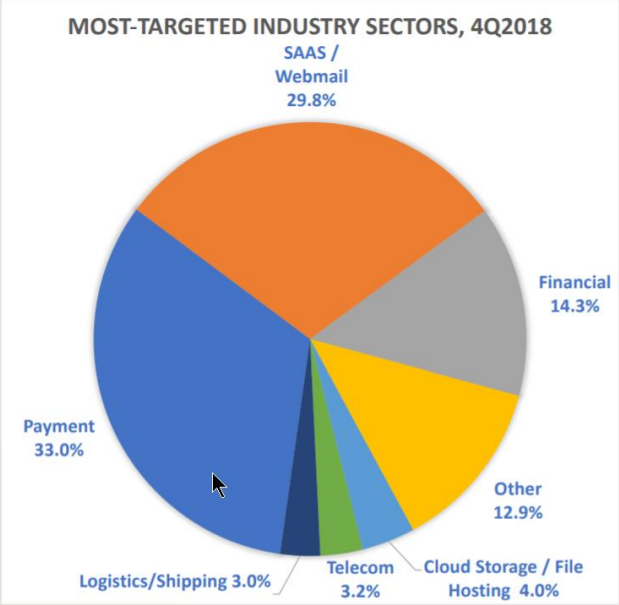

Figure 1 — Q4 2018 Targets of Phishing Attacks by Sector

- The payment sector became the most targeted business sector during the quarter, with approximately 33% of reported attacks.
- The SaaS/WebMail sector came in a close second with over 29% of attacks reported.
- Other sectors affected during Q4 included Financial Services, Healthcare, hosting providers and ISPs and Entertainment and Media.
- The number of brands targeted by phishing remained constant throughout 2018, although new companies and institutions were always being targeted. It is important to keep in mind that the vast **majority** of electronic attacks and cybersecurity compromises go unreported. For this reason, the

APWG report doesn't fully reflect the urgency of the matter or actual damage being caused by these types of attacks.

Other key findings of the report include:

- Monitors are detecting an increased number of redirectors prior to the phishing landing page - and as well after the victim submits his or her data - in an effort to obfuscate phishing URLs from detection.
- Phishers are using the HTTPS Encryption Protocol to increasingly fool victims. The HTTPS abbreviation and the green padlock symbol in the address bar usually signify that the data exchanged between your browser and the site you're visiting is encrypted. Over 80% of respondents in an APWG survey believed the symbol indicates that a site is legit and safe. Unfortunately, it is often neither one or the other, as scammers are now increasingly taking advantage of HTTPS. In late 201, merely five percent of phishing sites implied legitimacy with HTTPS. By the end of 2018, however, the amount rose to nearly 50% by the end of the third quarter of 2018.

STATISTICAL HIGHLIGHTS FOR 4TH QUARTER 2015

PEOPLE AS PRIORITY/TRAINING

As mentioned earlier, and as evidenced in all of the related statistics published by both law enforcement and industry, more often than not people are the weakest link in an organization's information security posture. Because of this, companies that do not train their personnel to accurately recognize and respond to security threats are setting themselves up for failure. Security Awareness Training is a key factor in reducing the risks associated with members of your organization.

Figure 2 — Q4 2018 Statistical Highlights

Security awareness training programs should include useful information relating to the latest security threats. Effective training programs also should include content specific to the company's security

Statistical Highlights for 4th Quarter 2018

	October	November	December
Number of unique phishing Web sites detected	56,815	35,719	45,794
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	87,619	64,905	87,386
Number of brands targeted by phishing campaigns	293	233	310

policies and procedures. This typically should include social media, acceptable use, data retention, and bring-your-own-device (BYOD) policies when applicable. During the training program each employee also should be asked to read and accept company policies relating to acceptable usage. This puts each employee on notice that he or she must be vigilant about security in the workplace. The spirit and overarching theme of any security awareness training program should be that security is the responsibility of everyone in the workplace and that everyone needs to remain vigilant when it comes to recognizing and responding properly to information security threats.

The Information Security Forum (ISM) is a leading authority on cyber, information security, and risk management. ISM is an independent, not-for-profit organization, with a membership comprising many of the world's leading organizations featured on the Fortune 500 and Forbes 2000 lists. The ISM recently published a list of principles that can help organizations embed positive security behaviors into employees. They included the following key areas as outlined below.

MAKE SYSTEMS AND PROCESSES AS SIMPLE AND USER-FRIENDLY AS POSSIBLE.

Organizations should have all staff members attend a yearly training course at a minimum. This can take place in person or online, depending on what makes the most sense for the organization. In many companies, employees work across numerous geographies, and because of this it is hard to assemble personnel in live sessions. It is also difficult for staff to measure content retention when dealing with large live audiences. For this reason, many companies are choosing online training.

Online training provides an excellent platform to measure progress and generate reports that can be used internally for compliance and audit purposes. Online training should be highly interactive — not something that can be clicked through quickly.

In additional to the yearly security awareness training module for all employees, an abridged security awareness training primer should be kept on hand by Human Resources departments and provided to all new employees when they are hired. This gives new employees an immediate lesson on awareness and also spells out exactly what is expected from them concerning security during their onboarding.

TESTING THROUGHOUT THE TRAINING MODULE(S) SHOULD BE INCLUDED AS WELL. THIS ENSURES THAT THE CURRICULUM'S CONTENT IS BEING RETAINED BY THE END USER.

- Help employees understand why their security habits are important.
- Motivate workers to protect the business, and empower them to make the decisions necessary to do so.
- Don't simply give orders to employees — sell them on security habits.

- Use multiple departments, like marketing and human resources, to help embed security behaviors.
- Hold employees accountable by rewarding the good and confronting the bad.

ONE OF THE MOST EFFECTIVE WAYS TO MEASURE STAFF RETENTION OF THE CONTENT PROVIDED DURING INFORMATION SECURITY AWARENESS TRAINING IS TO FOLLOW UP TRAINING WITH PHISHING EXPLOIT STUDIES.

Phishing awareness studies enable organizations to assess and improve upon their user's information security skills weaknesses through testing and analysis. Effective programs utilize creative simulated phishing attacks that are designed to test and evaluate user security awareness, as well as the delivery of additional training programs to educate employees further.

To create tests, simulated scenarios that are encountered frequently in information security incidents across the globe are delivered to end users. In a safe and quantifiable manner, these simulations are created and deployed as a test using email, with minimal impact or disruption to workplace productivity. The test emails typically should contain a link that redirects users to a landing page with information regarding the exercise, a mimic of an existing website or a login form for potential credential grabbing that allows for more precise metrics on the organization's security standing. Tests should be completely customized for each organization's specific requirements, enabling the organization to decide whether to target a single department, multiple groups of end users, or its entire workforce in one or a series of exercises over a predetermined time frame. In addition, the content of the phishing messages can be generic or specific to the organization's environment.

TESTING FREQUENCY AND ATTACK SCENARIO SOPHISTICATION

ANALYSIS AND REPORTING

Each organization will have different needs that will be determined by many factors. These typically will include business size, current state of user awareness, corporate structure, roles of employees to be tested, geography, other information security programs previously adopted, business sector and a long list of other variables. At a high level, it is safe to say that it is very important to establish some level of frequency in testing. Most companies test employees on a monthly basis for the simple reason that a monthly study allows the organization to document where the security posture (from an awareness perspective) has been historically, where it is at any given time, and in what direction it is progressing.

Security programs managed in this fashion become an enabler of the overall success of the business and also provide the organization with an ability to quantify risk reduction accurately.

Testing attack scenarios with varying levels of sophistication also are useful when measuring awareness among employees. For instance, attack scenarios written with poor English and many typos should be more easily recognizable as phish/cyber security threats to employees than attacks crafted to simulate a well written memo from a trusted source and mailed from a trusted email address. Testing scenarios should be designed to come from simulated trusted external sources (like banks or service providers) and also from simulated trusted insiders or partners (like IT team resources, HR or executives) of the organization. By deploying a series of tests over time, the organization can observe trends and use a targeted approach toward measures in hardening its information security stance. A well-rounded testing program will take attack frequency and sophistication into consideration when measuring effectiveness

Metrics for each test should be captured and analyzed to identify potential weaknesses in the organization's information security posture from the perspective of user behavior and awareness.

Metrics and information gathered should summarize the purpose of the exercise, who was targeted, how they were targeted, who clicked on the link supplied in the message, who submitted credentials, relevant statistics regarding the metrics captured against the intended target, and finally, grading criteria upon which improvement can be easily gauged.

Enhanced Employee Training

At the conclusion of each test, the organization should determine what next steps are needed to improve awareness among employees. This could include the planning of additional tests, or alternatively crafting or creating attack tools.

Craft phishing attacks. Adversary counterfeits communications from a legitimate/ trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.

Craft spear phishing attacks. Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).

Craft counterfeit certificates. Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.

Create and operate false front organizations to inject malicious components into the supply chain. Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.

CRAFT ATTACKS SPECIFICALLY BASED ON DEPLOYED INFORMATION TECHNOLOGY ENVIRONMENT.

Create counterfeit/spoof website. Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment. Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.

Figure 3 – National Institute of Standards and Technology (NIST) Cyber-Security Assessment Testing Framework Criteria

BEST PRACTICES

Organizations should protect their brands and employees properly by securing their computing networks correctly. They also should monitor their brands and notify law enforcement and industry authorities, including the APWG, as soon as they discover that their brands or personnel are being phished. Corporate end users should:

- Upgrade operating system and browser software whenever new versions are available. Many browsers now come equipped with anti-phishing functionality.
- Carefully examine all email messaging to verify the authenticity of the sender and the source from which it was sent.
- Avoid clicking on unfamiliar links in email. Instead, type the destination URL into your browser.
- Avoid opening attachments within emails sent from questionable or unfamiliar sources.
- Be careful about clicking on links that will take you to an unfamiliar website; also avoid clicking on links that take you to an IP address.
- Question messages that make commands or request action (like resetting a password).
- Choose smartphone apps wisely; use caution when granting permission to use apps in accessing sensitive files or personal info.
- Delete suspicious emails before opening them.
- Do not avoid browser or software warnings.
- Only accept trusted certificates

CONCLUSION

THE MOST DOMINANT AND SUCCESSFUL ATTACKS UTILIZED BY CYBER CRIMINALS TODAY ARE PHISHING EXPLOITS.

Prior to the existence of the internet, criminals had to physically attack their prey, break and enter, intercept mail or dig through garbage to steal personally identifiable information. Now that most of society's information is available and exchanged with the ease of a click online, criminals leverage the internet to steal account credentials, money, identities, sensitive intellectual property and private data. Only 25 years ago, illegally accessing a person's bank account would have required forgery and a visit to the bank. This could take hours and would place the perpetrator under the scrutiny of security guards, bank tellers, other customers and security cameras. It also would leave clear evidence of a crime and the perpetrator that committed it. Today, cyber-criminals can deliver their attacks anonymously with a basic computer and internet connection right from the comfort of their own homes or from anywhere in the world. They're also able to attack hundreds, if not thousands, of potential victims at a time with the simple click of a mouse.

Achieving absolute security in the enterprise is simply impossible. Improving security usually costs time and money above and beyond what a company may be willing or able to spend. The most effective compensating control to mitigate the threat to the workplace posed by people and the human element is security awareness training along with regular exploit testing.

For more information on how to obtain assistance with this challenge, please visit

http://www.globallearningsystems.com or contact us by email at info@globallearningsystems.com .

ABOUT GLOBAL LEARNING SYSTEMS

Global Learning Systems (GLS) got its start nearly 30 years ago, just as the first "digital natives" were being born and training began to move beyond the classroom. The GLS of today is a marriage of two former subsidiaries: Electronic Learning Facilitators (ELF), developers of award-winning custom learning solutions, and Keystone Learning, pioneers of video-based, web-hosted software and business skills training products.

In the late 1990's, as GLS was providing learning products and services to a wide array of corporate and government markets, a common customer challenge began to emerge: the threat posed to organizations by poor security awareness and lax employee behavior when it came to basic cybersecurity precautions, like using strong passwords and recognizing suspicious emails. Seeing the need, GLS drew upon in-house expertise in behavior change program design and off-the-shelf learning product development to produce engaging security awareness programs focused on changing those high-risk behaviors.

Today Global Learning Systems puts its 30 years of experience to work providing employee security awareness and compliance training programs, supported by our OnDemand Learning Management System and phishing simulation tool. Our program effectively promotes cybersecurity behavior change, protects your organization and Strengthens Your Human Firewall®.

As a trusted provider with a premiere list of corporate, government and non-profit clients, we have maintained long term relationships with both small businesses and Fortune 500 companies. GLS has been recognized for four consecutive years in the Gartner Magic Quadrant for Security Awareness Computer-based Training, and has won many other industry awards for our innovative courseware and reinforcement programs. We welcome the opportunity to partner with you to help safeguard your organization from the rapidly-changing cyber threat landscape.

About the Author

Jeffrey Bernstein is the managing director of GLS' partner, Critical Defence and has worked within the information security industry for over 20 years. Critical Defence is a U.S. based provider of security consulting solutions that are focused on the protection of people, property and information. The firm was founded in 2007.

SOURCES

1. Phishing Activity Trends Report: 4th Quarter 2018; Unifying the Global Response to Cybercrime. Anti-Phishing Working Group (APWG)
2. NIST CyberSecurity Framework. National Institute of Standards and Technology