MARCH, 2020

Phishing Attack Simulations

Fortification of Your Human Cyber Defenses

The explanation of new and old ways of phishing attacks and recommendations for effective measures to prevent them

LIFARS
your digital world, **secured**

Contents

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

WHY SHOULD YOU TAKE PHISHING SERIOUSLY?

Phishing is a cyber threat that anyone can utilize. You don't need to be a proficient hacker to gain access to a reasonably secure information system. All you need to know is how to use Internet search engines to find a working toolkit, a webserver, and a bit of research. The effects of such a threat can be devastating.

Phishing is a social engineering technique that uses psychological manipulation and deception to coerce someone into performing a certain action that is not in their (or their employer's) best interest. Phishing involves malicious actors sending well-crafted emails that urge the recipient to click on an link in the body of an email, which can redirect them to a fraudulent website designed to steal login credentials, credit card information, etc. In some cases, the threat actors attach documents containing malicious macros that may drop malware on the recipient's machine.

Despite phishing being included in just about every Employee Cybersecurity Awareness Training, employee awareness appears to remain insufficient as many employees remain unprepared to identify a phishing attempt and react properly - resulting in employee behavior that jeopardizes businesses. This may be the due to the following:

- Maturity of companies' awareness programs is stagnating
- Awareness programs lack testing and measuring
- Content is not presented in compelling and captivating manner
- Majority of users never experienced a phishing attack so there's no immediate experience
- Companies are not updating the content of their programs to prepare employees to identify the latest phishing methods

Dealing with phishing attacks presents various technical challenges. However, since these attacks are exploiting human vulnerability, there is only so much you can do on a technical level. Even with company efforts to deploy firewalls, antimalware solutions, network segmentation, and patching/updating, adversaries can circumvent these controls and choose the path of least resistance. There is no technical security patch for human vulnerability yet. That's why the organizational, procedural and process controls are still the most effective solutions.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

PHISHING SCENARIOS

There seems to be a public underestimation of the ramifications of a single phishing attack. Those who are less tech-savvy may think that this is just the user's problem and a simple password change is sufficient, therefore continuing business as usual. However, this is not always the case; so let's have a look at some scenarios this single incident may lead to.

The first scenario involves a nonprivileged user connected to a domain clicking on a link in the body of an email. In some cases, even opening a malicious email may pose a risk of malware dropping onto the user's computer. After the initial click, a counterfeit website designed to look trustworthy will appear, posing yet again, a risk of malware being dropped to the user's machine. This website may ask the user to enter credentials to a well-known web application. Awareness trainings in the past had taught our user, that when a symbol of a lock is present in the URL bar and the URL starts with https://, the website is secure. So, the user enters his credentials and hands them out to cyber criminals because they use Let's Encrypt certificates, making their counterfeit site look legitimate. Now, let us immerse into some statistics. The 2018 Global Password Security Report shows that 50 percent of users use the same passwords for their personal and work accounts. A 2019 online security survey by Google identified that 65 percent of people use the same password for multiple or all accounts. This horrifying data indicates that there is a big chance that the attacker would gain access to other information systems as well, unless there is a multifactor authentication (MFA) in place.

The second scenario is the same as the first, with the exception that it involves a privileged user such as administrator. For phishers, administrators are a very sought-after group of targets and they represent frequent subjects of spear phishing campaigns. If this is the case, an administrator may hand out very sensitive credentials with high privileges and the attacker may start to perform actions on his behalf, gradually taking control of the company's infrastructure.

The third scenario includes an administrator opening an attachment embedded in a malicious email. With the right pretext and circumstances, the attacker may coerce the administrator to run malicious software on his machine that installs a Remote Access Tool (RAT) which then enables the attacker to take complete control of his computer. The attacker can now log every keystroke, monitor his actions, listen to his microphone, view his webcam and has virtually all the power that administrator has. And the administrator is oblivious to all of that.

Now, let's have a look at a real-life incident that happened in December 2015 in Ukraine, which came to be known as the first hack ever to take down a power grid. It all started, apart from the reconnaissance stage, with an email to various IT administrators of some electricity companies that contained a malicious Office document. When the recipients

opened this document, a popup displayed a security warning that macros have been disabled with a button to 'Enable Content'.

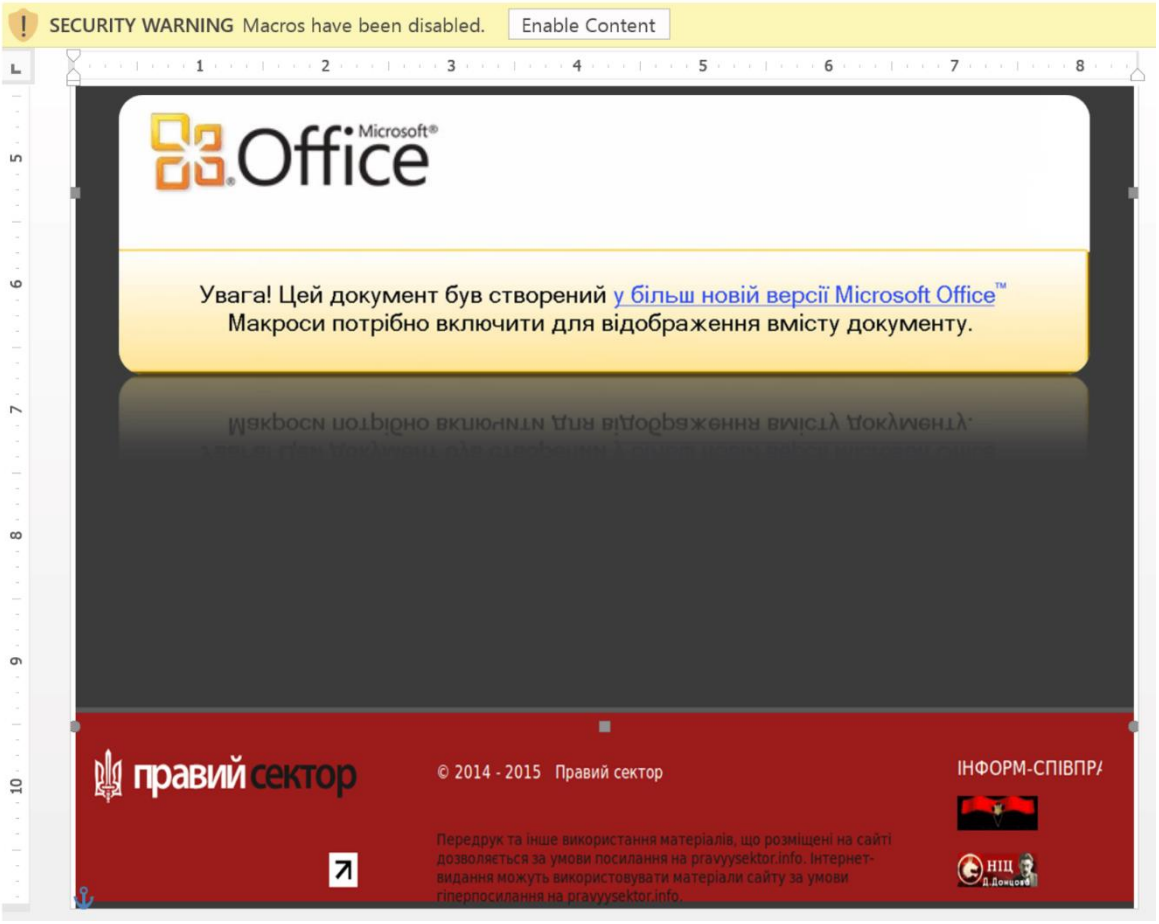

Figure 1 A sample of BlackEnergy 3 infected document (source: E-ISAC - Analysis of the Cyber Attack on the Ukrainian Power Grid)

The actual content of the document contained a fraudulent Microsoft-like banner using social engineering to lure the user to click on the 'Enable Content' button. Enabling the macros caused the BlackEnergy 3 malware to install on the user's computer. This allowed the adversary to gain access to the infrastructure for more than 6 months before the power outage. During this time the attackers silently gathered all information, harvested credentials, escalated their privileges and moved laterally through the environment. This Advanced Persistent Threat (APT) had many complexities in which we will not delve here. The bottom line is, that the adversary was able to take down about 30 substations offline and left more than 230 000 residents without electricity. All of this started with simple email.

DIFFERENT TYPES AND SOPHISTICATION LEVELS

The term 'phishing' encompasses different attack techniques, methods, and levels of sophistication all sharing one or more of these objectives:

- To steal money,
- To steal sensitive information,
- To gain access to computing power,
- To gain access to information systems, or
- To get a foothold in infrastructure in order to launch APT attacks.

The goal to **steal money** is usually achieved by luring out credit card information, counterfeiting PayPal login pages, or websites of reputable banks. Phishing attacks relying on counterfeit Internet Banking websites will likely due to the increasing number of banks implementing MFA, decline. In order to break through MFA, attackers need to possess usernames and passwords and take additional steps to gain access to a second factor like phone, token, grid card, or biometric data. In order to do this, they need to either hack the user's phone, employ fake cell towers exploiting SS7 vulnerabilities to read incoming SMS messages or perform a physical attack to gain access to tokens or grid cards. Although this is all possible, it is not likely to be done on large-scale using SPAM-like generic phishing attacks. However, prominent targets worthy of these efforts should be aware of these techniques and of targeted spear phishing attacks using sophisticated social engineering practices.

The objective to **steal sensitive information** is achieved by attackers employing phishing attacks as a first stage of a more complex attack leading to a data breach to gain access to information like usernames, passwords, credit card information, proprietary data or personally identifiable information, with intention to either directly exploit this information, or to sell it on black markets. Social security numbers can be sold for as low as $2 for fraud/identity theft; driver licenses can be found for as low as $10 to create fake IDs; healthcare information and records can be worth up to $1000 per account; and passport information sold as fake IDs may cost over $1000.

There seems to be a cyber security myth among general public, that if you don't use your computer for banking transactions or you don't store sensitive information, you don't need to pay special attention to securing your machine. But cyber criminals are even after the **computing power** of your computer so they can use it to perform their malicious activities. After they infect your computer with malware by delivering it via phishing email, your computer becomes a slave and a part-time employee in a big machine called a botnet working under the attacker's command. With a large enough botnet, adversaries can perform DDoS attacks capable of disruption of online services, or perform cryptocurrency mining.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

Getting access to information systems is achieved by luring out login credentials on counterfeit websites or by installing malware via infected email attachments. This initial breach, if undetected, may serve to launch APT attacks which bear the most devastating impacts because of their longevity, network propagation, amount of information exfiltrated and reputational damage. Around 90% of all data breaches and APT attack start with social engineering, like phishing.

There are several types of phishing attacks we can recognize:

- Common Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing
- Deepfake phishing

Common phishing can be imagined as catching fish with fishing nets. Phishing emails are sent to massive amounts of recipients in SPAM-like fashion utilizing SPAM lists obtained from black markets, or even from public sources. These phishing attacks are usually poorly executed, contain misspellings, don't address and greet the recipient by name, sender email address is usually different from authentic email address and contain other inconsistencies, that should raise some red flags in a cautious reader. However, the target audience for this type of phishing is the unsuspecting, gullible people that usually fall prey for these scams. The attackers are relying on the assumption that if someone is willing to believe that their bank is asking them to provide their credit card information, they will likely do it. Attackers also like to rely on inflicting fear in their targets. Such emails could look like this:

From: Bank of America <support@bankofamerica.00emt123.com>
Subject: Notification of Iregular Activity
To: Undisclosed Recipients

Dear Member,

We detected unusual activity on your bank account and it has been suspended for your securty. If you like to contininue your using your account, please follow this link:

http://www.bankofamerica.com <http://bankofamerica.00emt123.com>

Please sign in and verify your account by entering your debit card information. After verification we will do all the necessary steps to protect your online account. If you do not perform this action we may place limitations on your account a your debit card.

Best Regards
Bank of America

We can see that the sender email address is a very suspicious domain, there are several typos, grammatical errors and there is no personal greeting. The phishers are inducing fear by scaring the target into believing that their debit card may have been misused or threatening the recipient that his or her account will be locked if they don't perform the required action.

This email would be sent to thousands of recipients, many of which would not be delivered due to effective SPAM filters. And out of the emails that would go through, only a small part would be clients of Bank of America. The actual success rate of this campaign would then depend on the cautiousness of the recipients, quality of the phishing webpage and other circumstances.

Spear phishing is, in terms of sophistication, on a different level. It can be imagined as fishing with harpoons, targeting the specific species of fish. In this case, spear phishing emails are sent to a specific person or group of interest, likely a person with high privileges such as an administrator. An important part of spear phishing campaigns is reconnaissance, where the attacker gathers relevant information about their target using Open Source Intelligence (OSINT), in order to make a believable and personified pretext. The email itself is well crafted; the sender email address is usually spoofed to look legitimate and may look like it's coming from a person you know, there's accurate grammar, targets are greeted by their name, and overall it may be very difficult to distinguish a legitimate email from a phishing email. Target groups may be administrators, people with information that attackers are after, people with access to information systems of interest, accountants, decision makers or employees of target organization. Imagine an adversary that is interested in exfiltrating proprietary information from a specific company. He performs reconnaissance, finds a LinkedIn profile of that company and finds out that Joe Smith works there and that there's a picture of Joe and his coworkers from a conference that was held in Las Vegas last week. Now, the attacker tracks down Joe on Facebook and finds out, that last week Joe checked-in a hotel and there is a picture of him posing under the hotel's logo. The attacker now has a good pretext and is ready to launch his campaign. His spear phishing email could look like this:

From: Las Vegas Hotel <Matthew.Locke@lasvegashotel.com>
Subject: Lost and Found
To: Joe Smith <Joe.Smith@targetcompany.com>

Dear Mr. Smith,

On behalf of our entire staff, we would like to thank you for choosing Las Vegas Hotel. We are honored that you have chosen to stay with us and look forward to providing you with an accommodation soon.

We are happy to inform you, that an item was found in your room and is kept safe in our storage. Please, check the attached picture and let us now if the item is yours. If the item is yours, please follow this link and fill out our Lost and Found reclaim form:

https://www.lasvegashotel.com/lost-and-found <https://www.lasvegashotell.com/lost-and-found>

Sincerely,
Matthew Locke
Hotel Manager


Your item.jpg

As we can see, this email looks legitimate. It is targeted directly to a person that stayed in a specific hotel and it is more than likely, that he will be interested to know what item has been found in his room. Now, what he doesn't know is that the attacker has used steganography to embed malicious code in that picture. Once the picture is opened, the code will connect to compromised website and drop malicious payloads onto his system. The actual picture may present any random item. Even if the victim would like to claim the item, the link would take him to a fake website only to lure out some more information, like personally identifiable information and/or login credentials.

Whaling is essentially spear phishing targeting the biggest fish like CEOs, high-profile politicians or government officials. The people that usually have lot of money and lot of valuable information. And it is likely, that these people don't spend much time on raising their awareness on cyber security threats so they might be the perfect target. Phishing attacks can be a powerful force that might even swing the election of the President of the United States of America. Even despite best security practices and various security controls, attackers were able to bypass these measures by targeting personal Gmail accounts of Hillary Clinton's campaign chairman John Podesta and various staffers to exfiltrate and publish thousands of emails on WikiLeaks. There were several indicators in the phishing email sent to Podesta, that should have raised some red flags.

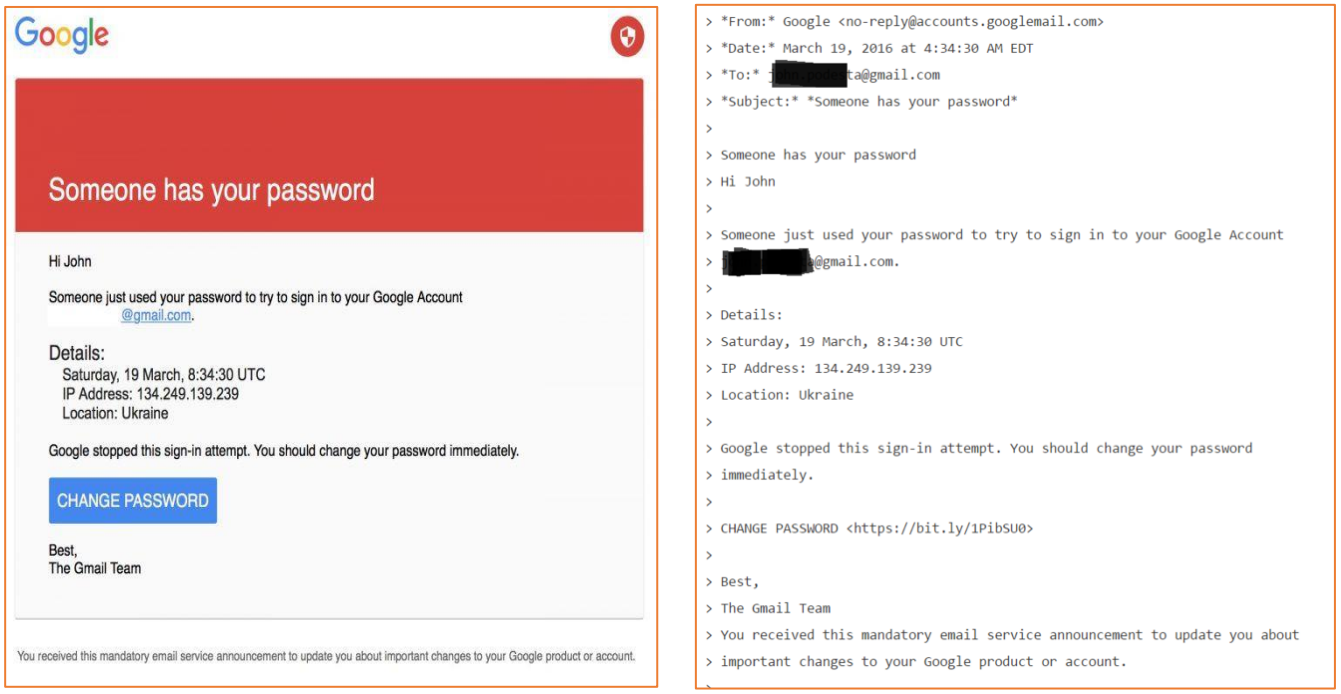

Figure 2 John Podesta's phishing email (source: yahoo! Finance andCBC News)

Figure 2 shows original (left) and plain-text version (right) of Podesta's phishing email. The picture on the left looks legitimate at a first glance, however, after inspection from a cautious recipient some inconsistencies with legitimate Gmail security warnings may be found. Such a minor thing as a comma after the greeting, different wording in sentences and different email closing and signature may not be spotted easily. But the most important red flag is the 'Change Password' button. Upon hovering the cursor above the button, your email client or a browser would tell what location this button is pointing to. As it is shown in the image on the right, it points to a URL shortening service bit.ly that has been used to hide the actual URLs in phishing scams. Upon clicking on this button, Podesta was redirected to a counterfeit Google password change site and he handed out his credentials to the criminals.

Smishing (or SMiShing) stands for phishing via SMS. The malicious link is delivered via cell phone text message using fake gift cards, lottery wins, password change requests and other as bait. There has been a growth in popularity of this type of phishing due to massive increase in our reliance on mobile phones. The impact of falling for this type of attack is the same as in other types of phishing. It could be losing control over your personally identifiable information, sensitive information, your login credentials, or infecting your mobile phone with malware. Figure 3 shows an example of a typical banking Smishing SMS, where the attacker attached a link to a malicious site for credential harvesting. A cautious recipient would notice that the URL is pointing to a fake domain of a well-known bank.

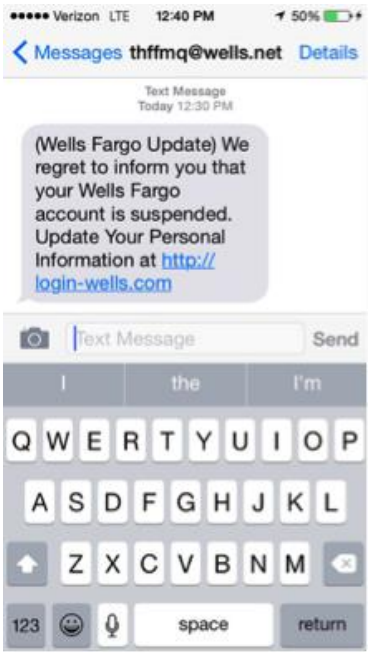

Figure 3 Example of Smishing (source: www.social-engineer.org)

Vishing stands for Phishing over the phone, or Voice Phishing. It is used for similar purposes as phishing and, depending on the skills of the social engineer, may be very powerful. In order to be effective, the attacker must put a lot of work into the preparatory phase and make use of OSINT to be able to react swiftly to any course of direction the phone call may take. Vishing may be a dangerous weapon that can be used for credential harvesting, information gathering for use in later attacks, or even for full compromise. Vishing may be coupled with a plethora of supporting attacks like spear phishing, dumpster diving (going through rubbish to find intel in paper form), baiting (leaving infected media to be found and inserted by targets), or other to build a solid pretext. Vishers are frequently impersonating IT support, colleagues, contractors and even people in distress and in need of help. People's desire to help other people is something, that attackers like to exploit. For example, imagine a regular employee getting a phone call from a CEO asking where his supervisor is. The employee responds that his boss is now on a flight to another city. The CEO is upset because he needs to make a quick payment in order to complete a business he just made, and he always has the supervisor to do it. He tells the employee that he needs to step up and perform the transaction himself and that he just emailed him an invoice. The attacker exploits the fact that regular employees in big corporations are not used to talk directly with CEOs and that people in general tend to submit to authorities. And in this situation, there is the highest authority in a company that's in need of help. The attacker is relying on a fact that the target is not used to speak with the CEO and will not question whether it's him on not, despite that his voice may be different.

Deepfake phishing is an emerging threat that is exploiting the latest developments in deep learning and AI. Until recently, the use of deepfakes had been used to create entertaining video clips of famous people doing and saying things they never did or said. There has been a deepfake video of President Barack Obama giving a public address to warn people from scams and saying profanities about President Donald Trump. Deepfake phishing is almost the same thing as vishing, but it is more cunning because the voice that is instructing the employee to make the payment is in fact the voice of the CEO. More precisely, it is a voice synthesized from samples of CEO's voice available online in form of PR material, interview, or public talks. The more samples there are, the more convincing the final product will sound. In 2019 there was an attack on a UK-based energy company where fraudsters were able to convince an executive to make a fraudulent transfer of 220 000 EUR by creating a model of the CEO's voice. The voice model was so convincing, that it made the executive truly believe he was speaking to his boss, as he recognized his light German accent and the melody of his voice.

SECURITY CONTROLS TO PREVENT PHISHING

Phishing attacks are targeting people. Therefore, the most effective controls to prevent all types of phishing attacks are non-technical, such as implementation of mature awareness programs. Yet, technical controls exist that can dramatically mitigate these attacks. Multi-layered approach comprised of preventive, detective and reactive controls (defense in depth) is the only way to reduce the risk of compromise to an acceptable level.

TECHNICAL CONTROLS

Spam filters are used to detect unsolicited, unwanted or malicious emails and to block them from reaching users' inboxes. They work by scanning the content of messages for words frequently used in spam or phishing, by examining email headers, checking IP address reputation, checking blacklists, or employing customized rules. Since around 70% of all email traffic in the world is spam, this is a must-have control, even if it may not be 100% efficacious. It may stop a reasonable amount of common, massively distributed phishing.

Real-time Blackhole List (RBL) is a list of IP address owners that send a lot of spam and is being constantly updated. It may include ISPs whose customers send spam or ISP servers hijacked for spamming purposes.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

Sender Policy Framework (SPF) is an email authentication method that reduces the risk of spammers and phishers spoofing the sender email address. It detects forging sender address during the email delivery by checking whether an email claiming to be from a specific domain originates from an authorized IP address.

Domain Keys Identified Mail (DKIM) is also an email authentication method to reduce email address spoofing that works by affixing a digital signature linked to a domain name to every outgoing email message.

Domain Message Authentication Reporting and Conformance (DMARC) is an email authentication protocol that extends the above-mentioned SPF and DKIM authentication methods to protect the domain owners from unauthorized use of their domain.

Digital email signing is used to ensure authenticity of an email using a pair of cryptographic keys. A private key is used to digitally sign an email by the sender and public key is used to verify the signature.

Valid website certificates are essential to let the users know, that your website actually belongs to your organization and hasn't been copied for malicious purposes.

Least privilege is a security principle that requires that users, programs or processes must be able to access only the information or resources that are necessary for their legitimate purposes. For example, a regular user should be working on a user account with restricted privileges and not on an administrator account. This ensures that when a malware infects the user's device, it will possess only restricted privileges.

Network segmentation is a good practice for division of computer network into subnetworks separated by firewalls. This practice provides isolation, so when a device in one subnetwork is compromised, the infection will not spread across the whole network.

Single Sign On (SSO) is a user authentication service that enables users to login to several web applications by using one set of login credentials. It reduces the risk of users having to remember the look, URLs and credentials for multiple login landing pages that phishers may try to copy. We recommend using SSO only with multifactor authentication.

Multifactor authentication is a method in which a user is granted access to a resource only after presenting two or more identifying information. It may be something you know (a password), something you are (biometry) or something you have (a token). If an attacker is successful with his phishing attack and gains a user's password, multifactor authentication will ensure that he will not be granted access, unless he somehow gains access to the second authentication factor.

Web filtering may provide an additional layer of defense by preventing users from visiting known phishing and malicious websites.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

Update, patch and vulnerability management are good practices which enable an organization to use the latest versions of software and apply security patches. This way an organization may prevent adversaries from exploiting known vulnerabilities in software.

Anti-malware software is an essential security program that's used to prevent, detect and remove malicious software.

Sandboxing of email clients and web browsers is a practice of running these programs in a separate highly controlled environment within the operating system without the risk of infecting the operating system in case of malware execution.

Host hardening is the practice of uninstalling or turning off all unnecessary programs or services within the operating system to reduce the attack surface.

ORGANIZATIONAL AND PROCEDURAL CONTROLS

Comprehensive **security awareness trainings** remain the most efficient preventive security control to reduce the risk of phishing attacks and other cyber threats. Awareness raising program should be a subject of careful planning that's based on defined objectives. Employees should be divided into groups based on their roles and responsibilities. Different level of knowledge is needed for clerical staff, administrators, executives and third parties. An awareness raising program can incorporate various means of information dissemination, activities, and should include measurement, evaluation and periodic improvement.

Incident reporting requirements should state that all personnel are required to report any suspicious occurrences within company's assets, for example the receipt of suspicious email, suspicious phone call or unusual requirement from a person within or outside the company that uses a promise of benefits, fear or is threating if the employee wouldn't comply.

Incident response policy and procedures are documents required by most of the national and international information security standards and legislation. IR policy and procedures should define the roles and responsibilities for incident handling, description of all phases of incident handling and reporting to third parties.

Secure email and web browsing policy should define the principles of safe usage of emails and Internet browsing. It should be mandatory for all employees to read and understand, and periodic trainings should be performed in order to stress the importance of these issues and to refresh the employees' knowledge.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

Out of band verification for above the limit transactions and sensitive operations should be mandatory in order to prevent adversaries from performing spear phishing, vishing or Business Email Compromise (BEC) attacks and stealing large sums of money.

Registering all domains that might look like the authentic domain is a good practice to prevent using such domains for phishing purposes. Some letters look similar and attackers are using this fact to set up counterfeit websites with similar looking domains. For example, *domain.com* and *dornain.com* may look similar, because *rn* and *m* have very similar shape.

Not promoting employee contact information is a good practice of not disclosing publicly all emails and phone numbers of employees in order to make it harder for attacker to reach and target the right person.

Discourage sharing of personal information on social media during awareness raising trainings is something that should be reminded periodically. Employees must understand the risks and ramifications of them disclosing personal information to information security.

Phishing attack educative simulations is a practice of sending phishing emails to organization's own employees in order to educate them on how to spot such emails and to teach them that clicking on links or downloading attachments may put the whole organization at risk.

Phishing attack penetration tests is a practice of performing phishing attacks from the point of view of an attacker for the purpose of finding out the weak links in the organization's security., strengthening its resiliency, or measurement of the effectiveness of trainings.

LIFARS PHISHING ATTACK SIMULATION

Our Cyber Resiliency Team can simulate a real phishing attack on your organization and based on the results collected and our in-depth analysis of the company email system, we can help optimize the system to increase the overall security posture to help keep cybercriminals from entering your network.

OBJECTIVES

There are several reasons to perform a phishing attack simulation in your organization. The objectives for this activity may be the following.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

To strengthen resiliency of your human firewall by empowering your employees with knowledge and practice of detecting and unmasking this type of social engineering attacks. It's very important to raise your employees' awareness of social engineering, but only real-life experience can harden this knowledge and prepare them for real attacks, which are not a matter of if they happen, but when they happen.

To protect your organization's information which may be subjected to a data breach in case your environment gets infected by malware delivered by email or can be leaked in good will by your employee deceived by treacherous adversary.

To protect your employees from being persecuted for data leaks caused by their actions under influence of professional social engineers and hackers. Experience and training gained by a phishing attack simulation will help your employees be aware from being exploited in their personal life as well, paving road to a safer home office environment.

To measure the effectiveness of your security trainings it is important to ensure periodic improvement and to set up your awareness program in a carefully planned manner. If you can't measure it, you can't manage it.

To identify weak spots in your security and we're not talking solely about your employees. There are still other aspects of your security that might benefit from performing phishing simulations, like weak passwords usage, email filters, old versions of software and others.

To provide additional training in areas uncovered by phishing simulation that might need your attention. We can train your employees on all aspects of cyber security that might be needed in order to achieve your company's business and security objectives.

ETHICS

Conducting phishing attack simulations carries a lot of responsibility and there are several ethical considerations. First, simulated phishing attacks must be authorized at an appropriate level within our clients and thorough discussions should be carried out on the risks and opportunities of such an exercise. LIFARS will be happy to be part of these discussions and will provide answers to all questions, that may arise.

Second, the simulation must be conducted professionally with best interests and confidentiality in mind. LIFARS has elite specialists and ethical hackers at your disposal and we consider trust to be the basis of our relationship with our clients.

Third, LIFARS will consult with our clients on all ethical considerations of performing the testing of the ability of your employees to resist the attack which, if conducted insensitively, might hurt someone's feelings. There is a reason why adversaries are

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

choosing this attack vector so frequently and it's because it works. One cannot expect their users to spot every top-notch spear phishing attempt. And deploying unexpected highly sophisticated attacks and then name, shame, or even persecute your own employees would probably not strengthen your staff's morale.

Therefore, LIFARS is advising to perform these tests in an ethical manner in order to fulfill the objectives of such testing, and at the same time to do it in a way that will not undermine the workplace relationships. This can be achieved by carefully selecting the target groups, informing the targets up front, offering to opt-out of testing, adjusting the difficulty and sophistication level of the attack, providing training and training material ahead of the testing, anonymization of results or gamification of such exercises. But on the other hand, there might be cases when you need to know your posture and preparedness for these attacks, and the only way is to learn the hard way.

TYPES OF SIMULATIONS

LIFARS is prepared to offer our clients all types of social engineering testing and simulations, such as:

Phishing attack educative simulations, where we apply the aspects discussed in the ethics part of this paper. Phishing emails are sent to users and if they fall for the attack, like clicking the link or downloading and opening an attachment, an educative landing page is presented with hints and tips advising them on how to prevent this in the future.

Phishing attack penetration test is performed from the perspective of an attacker, where we simulate the action of an adversary trying to exploit our client's users. It's possible to simulate an malicious insider (white-box testing), where our client provides us with all the information that an insider would possess, like the complete list of employees, their contact information and positions held, information technology used, etc. If our client wants to know how successful an outside adversary could be, black-box testing, where LIFARS would have to obtain all the information on targets by performing reconnaissance, should be performed.

Vishing attack simulation is a test of your employees' resilience to malicious phone calls. We would make several phone calls and test how much information an adversary would be able to gain and prepare a report on how this information could be used for malicious purposes.

METHODOLOGY

Before any social engineering attack simulation, it is advised to prepare your employees by performing training, publishing self-learning material and informing them of your intent to perform testing or simulation. Depending on the type of simulation, the

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

methodology may be adjusted to reflect the needs and specific conditions in the target organization.

For any successful social engineering attempt, the key is preparation. This can be done by collecting relevant information on the target, that can be used to prepare believable pretexts. Using Open Source Intelligence (OSINT), the tester will try to gather information about the company's social media use, information on company's vendors, whether the corporation uses call centers, if there is an organizational chart or even employee contact information available, if there are multiple site locations, if there is BYOD allowed, etc. It is beneficial to find out, whether there are domains visually similar to targeted company's domain available to purchase. At the same time, the technical preparation will take place. The tester will set up and configure his phishing tools, frameworks, webservers or ethical malware that might be needed to perform the simulation.

Based on information collected, the tester can decide on possible phishing scenarios. If there is a specific bank the company is using, the pretext may be to the request to review the banking information, sending an attractive offer or security warning. If there are specific vendor partners, the pretext may include impersonation of the vendor sales manager or technical manager, sending invoices or info sheets with malicious macros. If the tester will find out about specific web applications their employees are using, he could send fake links to the that application trying to collect login credentials. The possibilities are endless.

After crafting the phishing email, based on the pretext that has been chosen, the phishing website can be set up. If a decision has been made to target one of the publicly available web applications or websites, the tester will clone this website and add a login form that will be used to steal users' credentials. Another possibility is to insert ethical malware on the website to drop on an user's computer to gather information on the victim and send it to tester's webserver for statistical purposes or to create an attachment of the email that will contain ethical malware.

At this stage, the phishing email would be sent to a target group of employees and their behavior would be observed and the users' actions regarding the email would be recorded during the testing period. Data, like the number of clicks on the link, number of users submitting their credentials and the number of users reporting the incident will be evaluated and analyzed. After the testing period is over, an informational email should be sent to the target group to provide them with information on the signs and red flags that were present in the phishing. After the testing period, the report with results and recommendations will be produced and provided to the client.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

REMEDIATION

Our team will follow up by conducting an audit of the entire email system to help identify gaps in your security. We will examine email use within your organization for a period of time and based on the results collected and our own experience we will set up filters, whitelists, and blacklists to prevent common and advanced (targeted) email attacks on your organization.

Many businesses have technology in place capable of providing reasonably good email security. We will evaluate and fine-tune your existing technology to provide optimal security for email communication. We ensure that all security controls in place are properly configured and functioning optimally.

Even with the most advanced technology in place, the human factor should not be underestimated. A well-educated and vigilant workforce plays a crucial role in preventing advanced social engineering attacks, including email attacks. Our Cyber Resiliency Experts will train your employees with real examples from the assessment stage to demonstrate the threat and importance of being prepared.

To learn more about our Phishing Attack Simulation Solution, contact one of our Cyber Resiliency Experts today!

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com