www.codegreen.ae

Defend Against Phishing Attacks

How To Stay Safe from Phishing Attacks

codegreen SYSTEMS

So what is phishing attack?

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication (Ref: Wikipedia).

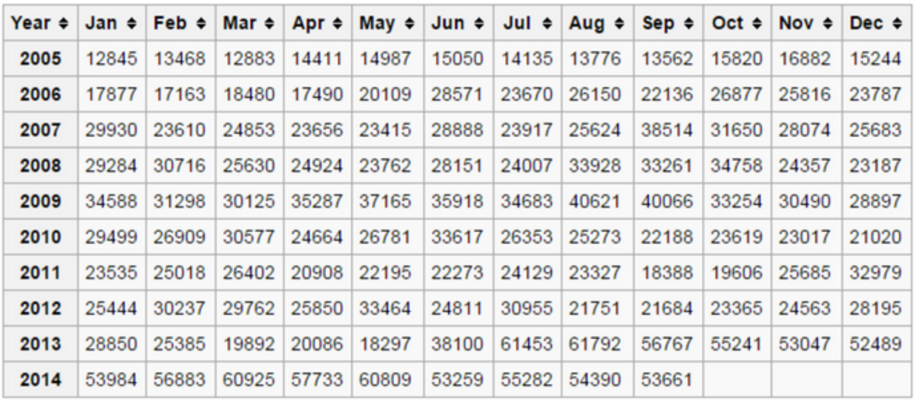
Thats just one way of defining it, but essentially its an act of deceiving some one and obtaining sensitive information and/or proxying them to do other malicious cyber acts - all with out the victim knowing about it.

The next level to this is called Spear Phishing, where 'Spear Phisher', instead of targeting a wider audience of victims, targets a specific individual or groups within an organization. Most of the time it starts by getting the victim click a link delivered via email or social engineering etc to gather sensitive info. Spear phishing emails, for instance, may refer to their targets by their specific name, rank, or position instead of using generic titles as in broader phishing campaigns.

But does it work? Really?

It does, and often causes more damages in terms money and reputation loss than one could even speculate.

The chart on the right shows the total number of unique phishing reports (campaigns) received. Source Wikipedia.



Year ♦	Jan ♦	Feb ♦	Mar ♦	Apr ♦	May ♦	Jun ♦	Jul ♦	Aug ♦	Sep ♦	Oct ♦	Nov ♦	Dec ♦
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661			

Source: Wikipedia

The seriousness of these threats may sound very theoretical, but the reality is that phishing attacks actually are achieving their malicious goals. With alarming regularity, organizations are in the news reporting devastating breaches resulting from phishing and spear-phishing attacks. Anthem Inc, Epsilon, RSA, the United States Department of Energy facilities at Oak Ridge National Labs, Pacific Northwest National Labs and the International Monetary Fund are just some of the organizations hit with email borne threats that led to data breaches.

> “Health insurer Anthem Inc. said the database that was penetrated in a previously disclosed hacker attack included personal information for 78.8 million people, including 60 million to 70 million of its own current and former customers and employees.”

Source: wsj.com

> “The report looks at analyses of almost 80,000 security incidents that hit thousands of companies in 2014. It found that, in many companies, about 25% of those who received a phishing email were likely to open it.”

Source: bbc.com

Types of Phishing

Phishing attack is carried out through various methods. Most phishers are technically innovative and can afford to invest in technology. Most of recent attacks use phishing as a way to get initial foothold in to the system. Some of the more prevalent ones are listed below.

Phishing form: This attack starts with a phishing email that includes a link to a website. When the user clicks on that link, it simply takes you to a look alike of a site familiar to you, such as LinkedIn, facebook or your corporate Outlook Web Access. When the user types in their user name and password thinking thats its the real site, it captures that information and records it, and then in most of the cases, typically forwards you to the real site and logs you in - so this leaves no clue for the user that something unusual have happened - thats makes it even worse.

Browser Exploitation: Browsers and their plug-ins contain vulnerabilities that can be exploited simply by visiting a malicious website. An attacker can send an email with a link, which takes the user to a malicious website (which is often designed to look like a legitimate site.) Just by visiting that site the user’s browser and machine would be compromised and the attacker would have full access to the user’s computer. In addition, a completely legitimate website can be attacked to make it malicious. So a user could be browsing a legitimate website that’s been attacked on the back end and injected with malicious code, which then exploits their browser.

File Format Exploitation: Opening a malicious email attachment is another way to trick users. Attachments are typically PDFs or Office files because those applications are widely distributed and used across all platforms, and the chances that the recipient would run or open that attachment is relatively high. Once the malicious attachment is opened, it exploit vulnerabilities in a given application or it may run a malicious macro.

Malware Based Phishing: This refers to scams that involve running malicious software on user's PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities - a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

Ransomwares like CryptoLocker CTB-Locker, Teslacrypt, CryptoWall, TorrentLocker, and BandarChor were spread via phishing mails. CryptoLocker is one of the most notorious attacks we've seen in a while, one which ruined many administrators days. Many of these have a very low detection rate by traditional Anti Virus, which make it difficult to prevent.

Costs and Downfall of Phishing Attack

The costs of dealing with an attack fall broadly into three categories:

Cost of Remediation: A successful phishing attack, burdens the administrators with identifying and cleaning compromised machines, which may extend beyond just the specific targeted recipient machines, causing considerable operational cost.

Financial Loss: Financial ramifications of a post phishing attack are significant . While hard to quantify, organizations need to consider how they value their most critical information assets. RSA noted in the EMC Earnings Call (Q2 2011) that as a result of their data breach, $66M was spent to replace tokens, monitor customers, and handle the fallout from the breach.

Reputation Loss: The most difficult to quantify is the reputation loss associated.

Challenges In Defending Phishing Attacks

Phishing attacks are certainly not recent phenomena – so why have they been so successful despite of all the security controls we have in place, with numerous high profile data breaches reportedly initiated via phishing attacks and countless other unreported and/or still undetected cases? The answer lies in the target and intent of a specific phishing message. Historically, phishing attacks were focused on the login credentials of end-users – with a focus on accounts such as online banking, PayPal, or eBay accounts. These types of attacks were typically broad-based, high volume attacks with very small open rates.

Due to the high volume nature of the attack, many anti-spam solutions were quick to detect these messages in spam traps and suitably effective in filtering these messages. But even then occasional phishing messages and targeted phishing attacks was missed and passed to an end-user. Many times the victims tended to be individuals and the damage limited to the specific account that the user provided credentials to.

The issue now is that many phishing attacks are highly targeted with low volumes of messages. In addition to the increased use of compromised accounts to launch attacks, this has resulted in the reducing the effectiveness of reputation services associated with spam solutions to detect phishing messages.

In a further effort to bypass spam filters, phishing messages are increasingly crafted with sparse features and little or no malicious content. The call to action is nothing more than a simple URL. With such sparse content, traditional spam filters are not well equipped to determine if these messages are legitimate or malicious threats.

How to Protect Against Phishing Attacks?

There are essentially two major ways to defend against phishing scams: User Awareness Training and Technical Security Controls.

We recommend you implement a combination of both user training and technical controls for an effective counter measure in place. Relying on just one approach will probably not decrease your risk to an acceptable level.

User Awareness Training

Here are 16 simple tips you can share with your users as a starting point.

1. Don’t trust links in an email, unless you know the person and have some level of trust.

2. Never give out personal information upon email request unless you know the person

3. Look carefully at the web address; it could be a close approximation of the real URL

4. Make it a habit to type or do a book marking of the those URLs you often use and are valuable and sensitive

5. Don’t just simply call up company phone numbers listed in emails or instant messages; check a reliable source such as a phone book or credit card statement or company web site   address.

6. Don’t open unexpected attachments or instant message download links

7. Be suspicious if emails says “do X or something bad will happen”. You know thats silly.

8. Be suspicious of any email with urgent requests for personal financial information

9. If the email sounds too good to be true, its probably is. Ignore them.

10. Always ensure that you’re using a secure website when submitting credit card or other sensitive information via your web browser; look for the https:// and/or the security lock icon 🔒 https://

11. Regularly log into your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate

12. Use a reputable anti-virus program

13. Enable two-factor authentication whenever possible. This combines something the user knows (such as a password or PIN) with something the user has (such as a smart card or token) or even something the user is (such as a biometric characteristic like a fingerprint).

14. Keep your operating system updated, ensure that your browser is up to date and security patches are applied.

15. Always report “phishing” or “spoofed” e-mails to your IT department, immediately

16. Use strong password and most importantly try avoiding reusing of password for multiple sites as much as you can. This doesn't prevent phishing attack, but reduces the impact

Technical Security Controls

Of course, training need to be coupled with technical security controls. These technical controls will prevent or block many of the threats so that they never reach your users. We’ll take a look at some of the different types of controls and how they work.

Vulnerability Management: This is your number one defense against attackers. It identifies existing vulnerabilities in software programs, browsers and plug-ins and helps shield your organization from potential damage, as well as mitigate vulnerabilities through patching, changing configurations or making application updates to remove vulnerable codes. Programs like Microsoft Office and Adobe Reader are the typical applications that get exploited through phishing, so it is important to stay on top of any vulnerabilities associated with these programs.

You also need to make sure your vulnerability management program is maintained and monitored over time. The key to vulnerability management is to get visibility on client-side vulnerabilities, focus on solutions that highlight vulnerabilities exploited by malware kits, as well as validate and prioritize vulnerabilities to identify high-risk issues that must be fixed immediately.

Patch Management: Patch Management is used to fix vulnerabilities based on the vulnerability management. Some fixes are implemented through patching and some are through changing configurations. Software updates and security updates need to be done in a timely manner to keep up with patching vulnerabilities.

Malicious URL and attachment blocking: This be done with web filters and SPAM filters. There are also web filters that you install at the Internet gateway of your company that will block malicious URLs. Modern Antivirus Softwares have this capability built-in to the agent as well.

Intrusion Prevention Systems: This is another form of defense. If, for some reason, a user does click on a suspicious link, and a website is serving up a browser exploit, an IPS can detect that and block web-based exploitation.

Data Loss Prevention (DLP) / Egress filtering: This is a system designed to detect a potential data breach and prevent it by monitoring, detecting and blocking sensitive data while in use, traversing over the network or in storage and before it leaves the gateway

Disabling Java: This may sound like a drastic approach, but Java has been a huge attack vector for compromising systems via malicious links in phishing emails. If you are using critical applications running on browser-based Java, or if your users need Java to get their jobs done, you may want to configure the browser to prompt and ask for permission before launching Java and educate your users to only allow Java on websites they trust. This is one of the simplest and cost effect mechanism to thwart phishing attacks

Is My Organization Vulnerable?

In order to combat social engineering attacks, you need to know where to start, and then measure the progress you make. Here are some guidelines to do so. Get visibility into the problem as the first step in thwarting attacks against your network. If you're running a program to reduce your phishing risk, then first of all, you need to know the size of that risk. How do you quantify that? Is your company currently doing well, or not so well? Where do you stand? Gaining visibility it is like putting a stake in the ground. By implementing a penetration testing solution you can answer questions such as:

- How are you vulnerable?
- Where you are the most vulnerable?
- Do you know if the security investments you are making are worth it?
- Are you making progress over time?

Social Engineering Campaigns

Such campaigns can be implemented inside your company as a test to measure how many people click on a phishing email and how many submit fake log in forms. You can also host your own malicious website to see if your browser is vulnerable and if your security controls are working. Your social engineering campaign will expose user susceptibility to scams and will also test browser security, web filtering and other security controls.

Penetration Tests

Conducting a penetration test from compromised machines to determine how far an attacker would get can really be helpful. Can you get to the credit card database or not? This is a typical goal that an attacker would try to attain, because it gives them access to valuable, financial information.

How CodeGreen Can Help?

CodeGreen team can help evaluate your infrastructure and the controls in place. We can also do a targeted spear phishing campaigns to the entire employees or to a groups of employees to assess and report their susceptibly to such attacks.

Questions or enquiries? contact sales@codegreen.ae