



Phishing Statistics & Defences

By: Ramil Davidov, Ashish Bhayana



What is phishing?

- The attempt to acquire a users private information such as their usernames, password, and bank details
- The attacker hides himself as a trustworthy entity through electronic communication to steal personal information
- The attacker uses bait to catch a victim (attack is traditionally known as fishing due to this reason)

Why Are Phishing Attacks So Successful?

- Detection
 - Hard for new users to detect
 - Pool of potential victims doesn't die but changes
- Cost
 - Easy to find a tool to hide identity and infect users
 - Many events where phishing can occur
 - Social Media
 - Email
 - Counterfeit Website
- Flexible
 - Easy to update code for the attacker
 - Tech-savvy and new computer users can be victims
 - Simple and basic programming skills required

Taking steps to Prevent Phishing?

The user should train themselves 4 key concepts:

- ◇ Recognize suspicious activity
- ◇ Avoid suspicious activity
- ◇ Report suspicious activity
- ◇ Update Security Softwares

There are other ways phishing can also occur such as random spam, pop-ups, and viruses such as a trojan.

Proper protection from these attacks consist of:

- ◇ Firewall
- ◇ Spam Filters
- ◇ Anti-spyware software
- ◇ Anti-virus software




Type of Phishing Techniques

- ◇ Web-Based Delivery
- ◇ Instant Messaging
- ◇ Keyloggers and Screenloggers
- ◇ DNS-Based (Pharming)
- ◇ Session Hijacking
- ◇ Maleware

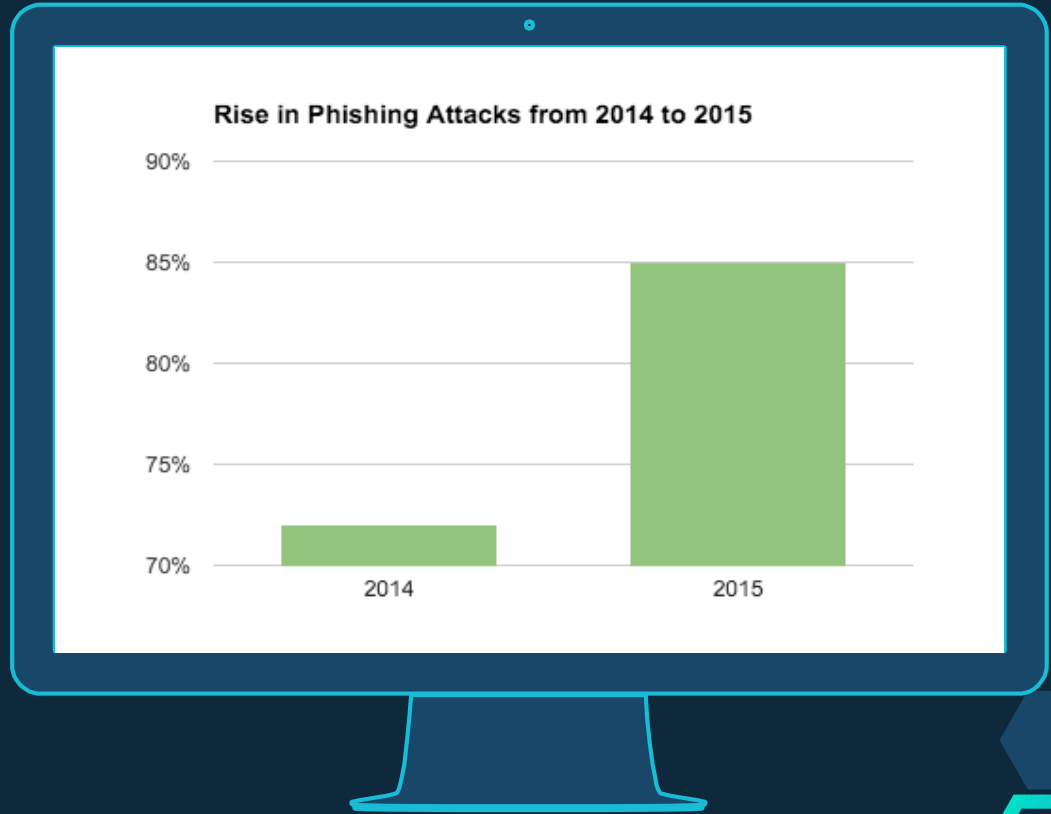
....and MORE!





Since the internet is internationally used around the world this means there is an increase in victims since all users are not as computer friendly as others

Statistically speaking, phishing attacks have increased by **at least 12%** from 2014 to 2015. Which shows how phishing attacks are still successful



A cluster of several hexagons in various shades of blue and cyan, some solid and some outlined, arranged in a non-uniform pattern in the top-left corner.

445,500

Around this many users fall victim to Phishing every year due to easily avoidable mistakes





Vulnerability of Phishing is world-wide





How many people take the bait?

On a daily basis:

- ◇ 156 Million Phishing Emails Produced
- ◇ 16 Million avoid Spam Filters
 - Many emails are destroyed by filters
 - 10 - 20% make it past the filters
- ◇ 8 Million links are seen by users
- ◇ 800,000 links are clicked by users
 - Majority of the internet community avoids it
 - 10% of the community is lured into the link

- ◇ 9% of online Canadians have been phished unknowingly
- ◇ 3% have entered bank details on an unknown website
- ◇ People who take the bait lose their
 - financial information
 - identity





Snapchat snared by Phishing Attack

On Feb 29, 2016 several co-workers which are employed by Snapchat had their personal information stolen by an attacker whom impersonated their Chief Executive Officer

The isolated email phishing scam was targeted towards Snapchat's payroll department where the attacker asked for employee payroll information and successfully acquired that information due to his image as a trustworthy employee.

In result of this attack, the company was robbed of important employee information such as Security Security Number, Salary, Bank details, Addresses, and emails.

This imposes danger to the victims because it is in the hands of a criminal which can find where they live, work, their personal information, and steal their identity

A cluster of several hexagons in various shades of blue and cyan, some solid and some outlined, arranged in a geometric pattern in the top-left corner.

Businesses at risk

- The typical damage of breach was \$35,000 for small to mid-size business and \$690,000 for enterprises.
- Financial institutions tend to be a high interest for attackers.
- Attackers look to target financial officers/accountants to reach the corporate funds.



Spear Phishing – Attack on small Bussiness



What is Spear Phishing?

- Spear phishing are those emails that appear to be from someone or a company you know. They use fake logos, may include information about you from a social media site.
- It is reported that 38% of spear phishing targets companies with 250 or less employeses.





What is the difference?

- Spear phishing is a subset of phishing
- Regular phishing targets a wide range of users.
- Spear phishing targets a key number of individuals
- The key number of individuals are expected to have very special access to vital information the attacker is seeking. (ex: company executive can be a victim)
- Regular phishing is a social engineering tactic
- The attacker attempts to steal sensitive information by “baiting” the user
- Any user can be a victim of this attack



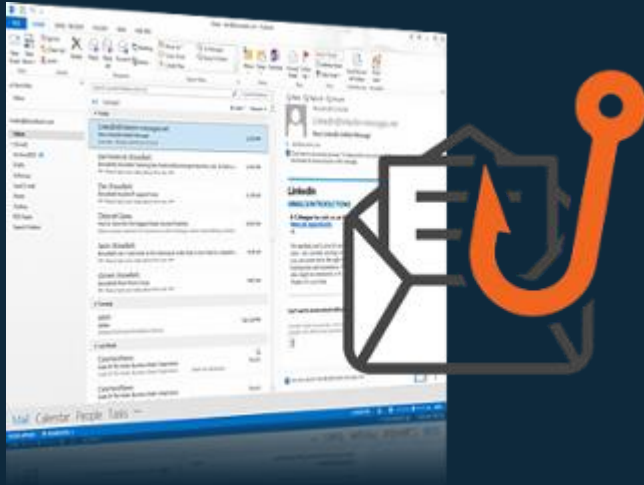


Spear Phishing – Small Business Target Industries

1. Manufacturing -22%
2. Finance, Insurance and Real Estate – 17%
3. Professional Services – 17%



Attack on Enterprises



- Email has been the threat vector of choice because its easy, there are no skills needed and you can attach a pre-built piece of malware to your message.
- Employees tend to trust the internal network, feeling protected behind their companies infrastructure. Cyber criminals exploit that trust.





Attack on Enterprises – Case Study

- PhishMe conducts a report in which 8 million phishing simulation emails were sent to 3.5 million enterprise employees.
- 87% of the employees who opened a phishing simulation email did so on the day it was sent. This means organizations have little time to catch a targeted attack.
- 67% of those who responded are repeat offenders.
- Business communication emails were most effective. Emails with subject lines “Files from Scanner” (36%) and “Unauthorized activity/access” (34%) were the most common.





Attack on Enterprises – Case Study

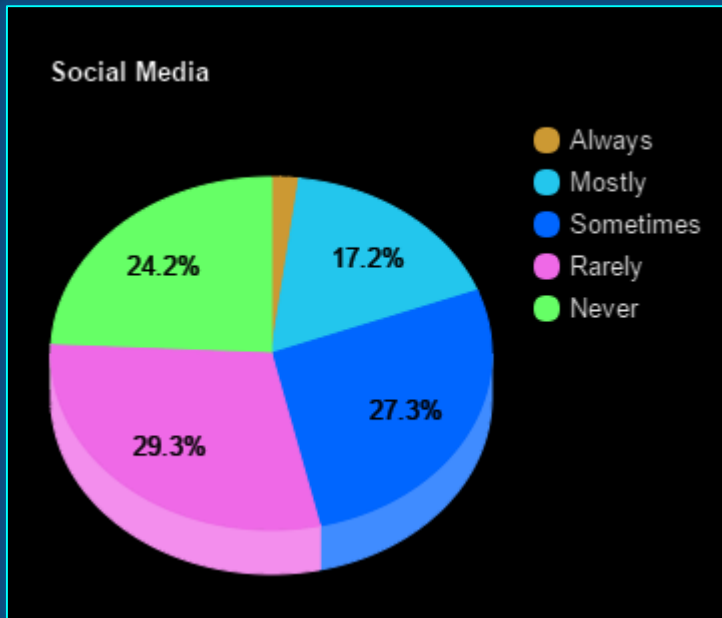
How does effective training impact these stats?

Behavioural conditioning decreased susceptible employees likelihood to respond to a malicious email by

97%



Social media attacks



- In a survey conducted by SecurityAdvice, almost 50% of the employees are likely to accept invitation from a stranger on social media.
- LinkedIn and Facebook are two social media sites with the largest threat.




Defence against emails

- Emails have a generic “Dear Customer” or have spelling/grammatical errors that should be considered suspicious.
- Don’t open attachments you were not expecting.
- Be aware of clicking on links within emails. Attackers tend to use misspellings of a company website to get the user to another URL. Instead of clicking the links, user should manually enter the websites, or hover over the URL, to reveal the destination.





Donut time!

- ◇ What is one type of phishing technique?
◇ **A: Email/spam, Instant Messaging, Screen loggers,...**
 - ◇ What is spear phishing?
◇ **A: An e-mail spoofing fraud which targets users with special access to assets**
 - ◇ What industry is the most susceptible to a spear phishing attack?
◇ **A: Manufacturing**
 - ◇ In the case study, behavioural conditioning reduced the susceptibility of an employee to respond to an email by what percentage?
◇ **A: 97%**
 - ◇ What two social media sites are the largest threat to employees?
◇ **A: Facebook and LinkedIn**
- 



Thanks for watching!

Any questions?





References

- ◇ <http://searchsecurity.techtarget.com/definition/phishing>
 - ◇ <https://getlogdog.com/blogdog/why-phishing-attacks-are-still-so-successful/>
 - ◇ <http://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html/>
 - ◇ <http://www.phishing.org/phishing-techniques/>
 - ◇ <https://duo.com/assets/img/blog/rise-phishing.png>
 - ◇ <http://www.getcybersafe.gc.ca/cnt/rsracs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx>
 - ◇ <http://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/>
 - ◇ <http://phishme.com/millions-of-emails-sent-in-thousands-of-phishing-attack-simulations-reveal-how-frequently-enterprise-employees-fall-victim-to-phishing-attacks-2/>
 - ◇ <http://searchsecurity.techtarget.com/tip/Phishing-The-business-risks-and-strategies-for-mitigating-them>
 - ◇ <https://business.kaspersky.com/how-phishing-affects-businesses/3793/>
 - ◇ <http://www.nationalcybersecurityinstitute.org/small-business/spear-phishing-attacks-target-small-businesses/>
 - ◇ <http://www.privacyrisksadvisors.com/news/why-are-manufacturers-so-prone-to-cyber-attacks/>
- 