Survey on data breaches effects and security risks

[1]Shruti Pankajkumar Parekh, [2]Richa Agrawal, [3]Shyamal Pandya

[1]PG student, [2]Assistant Professor, [3]Technical evenglish
[1]Information Technology,
[1]Silver Oak college of engineering & technology, Ahmedabad, India

***Abstract* - The World Wide Web (WWW) plays an important role in today's world. Users prefer online shopping and social networking. Phishers takes this opportunity as a chance to steal users' personal information which includes usernames, passwords, security numbers etc. This paper gives a survey on how much phishing harms users' data. It also gives survey on data breaches in current year, 2016.**

***Index Terms* - Malicious URL, data breaches, phishing attack, world wide web**

I. Introduction

Malicious URL has become the major concern for users in today's world of online shopping, social networking and surfing. Phishing attacks aims to get user's confidential information and credentials like passwords, bank account information etc. The World Wide Web becomes important part of everyone's life. The World Wide Web (WWW) is being used by users for online banking, online shopping, e-commerce, user's sensitive information, social networking etc. In this type of usage of internet contains some of malicious webpages which is harmful for user's sensitive information.

The phishers are getting smarter now-a-days. They know how to breach the sensitive data of users. This is illustration of how phishing takes place:

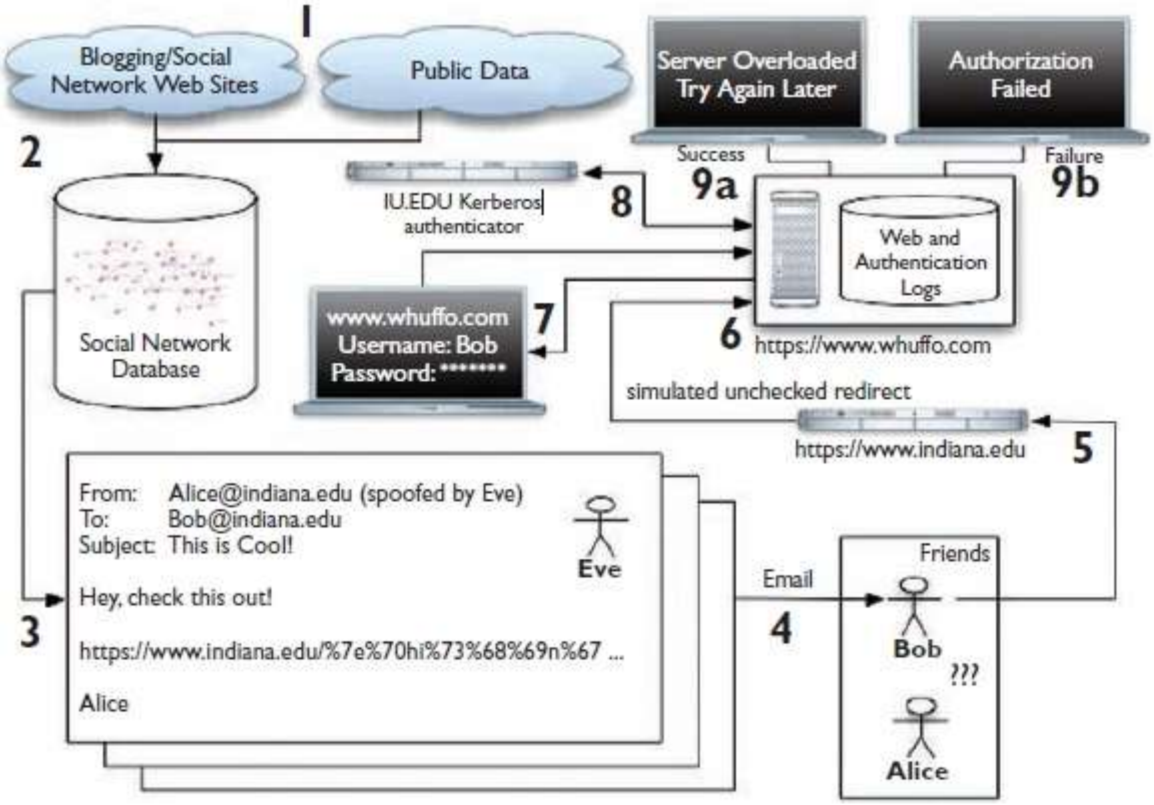


Figure 1 Process of data breaches

As shown in figure 1, the public data, social networking websites and blogging data is collected in the first step. The data is then stored in relational database. The email is spoofed by Eve "as Alice" to Bob i.e. a friend. Then the email is sent to Bob. The receiver, Bob understands that his friend Alice sent the email. Bob checks the email, clicks the link given in the mail and redirected to the malicious webpage whuffo.com. Bob is asked for his university credentials. His credentials are verified by university authenticator. In this way, the phishing is done.

II. Classification of malicious URL

While surfing over the internet, users need to be alert for malicious URL. The features of malicious URL are:

- Age of domain
- Number of dots
- Non-matching URLs
- IP-based URLs
- “Here” links
- Number of links
- Number of domains
- JavaScript

III. Background study

The word phishing was introduced by APWG due to social attacks against America On-line accounts by phishers. The word phishing came from the word fishing. As fishers, i.e. attackers use a lure, i.e. social messages to fish, i.e. to steal personal information of users.

The APWG phishing activity trends report analyzes phishing attacks reported to APWG. Most of the sectors affected are given by APWG:

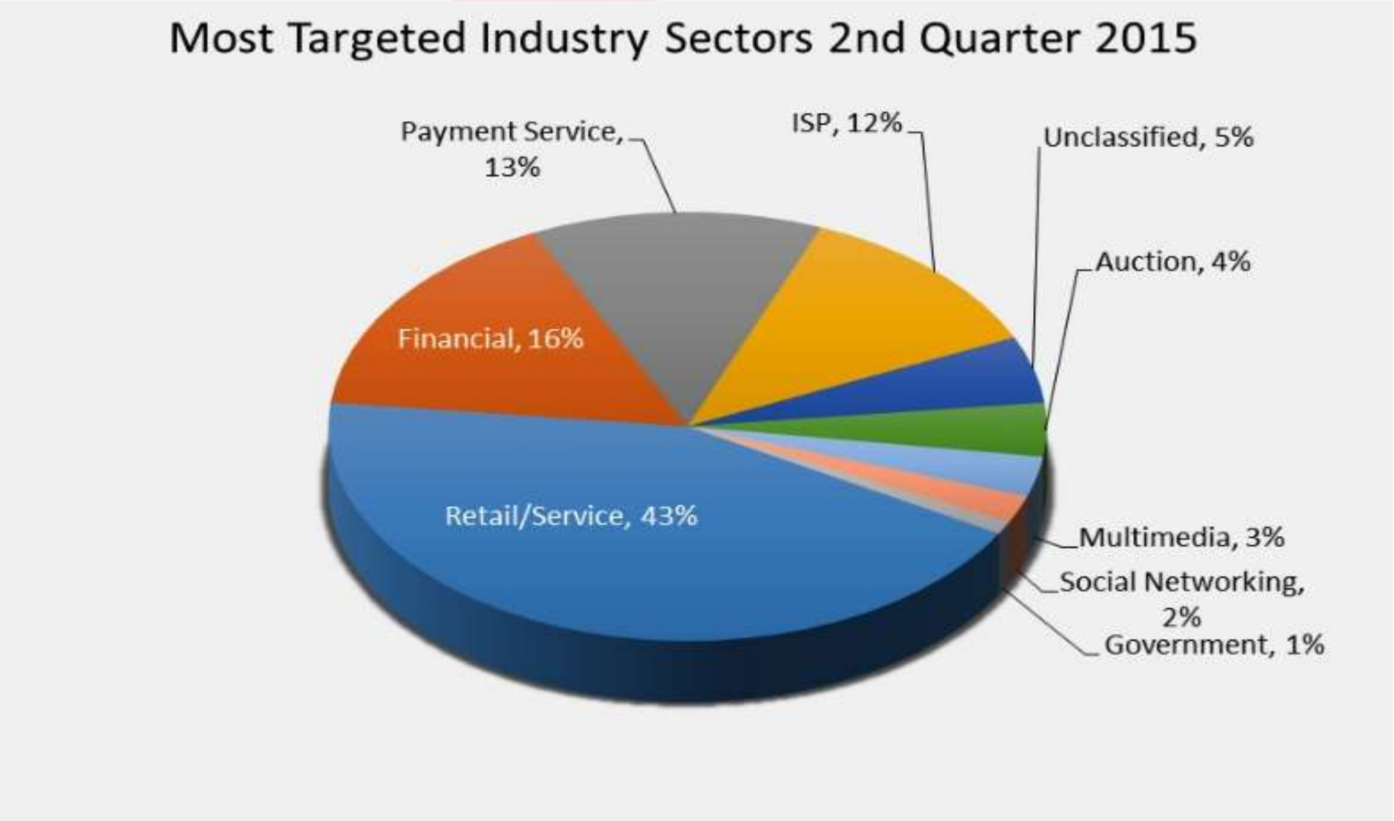
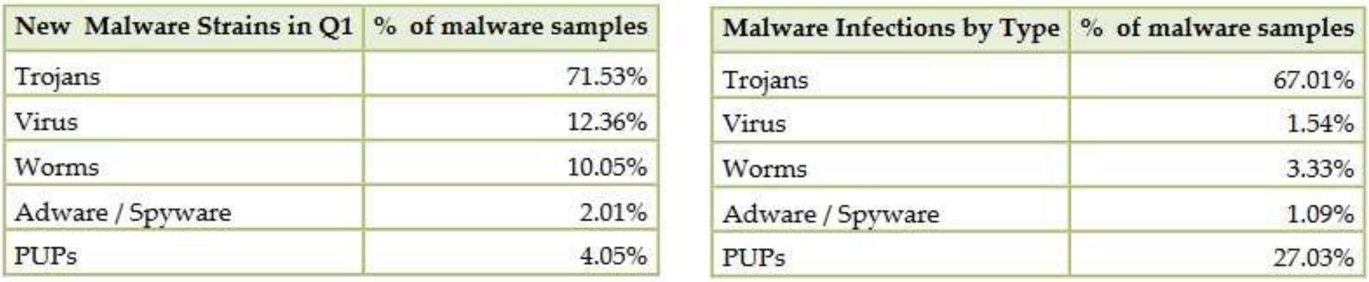


Figure 2 Sector wise data breaches

APWG found 18 million new malware samples in Q2. This is 10 percent lower than in the previous quarter, where 20 million new samples were found. Trojans are broad type of malware.



New Malware Strains in Q1	% of malware samples
Trojans	71.53%
Virus	12.36%
Worms	10.05%
Adware / Spyware	2.01%
PUPs	4.05%

Malware Infections by Type	% of malware samples
Trojans	67.01%
Virus	1.54%
Worms	3.33%
Adware / Spyware	1.09%
PUPs	27.03%

Figure 3 Different types of malware found

As per APWG report, there are many data breaches during January to June.

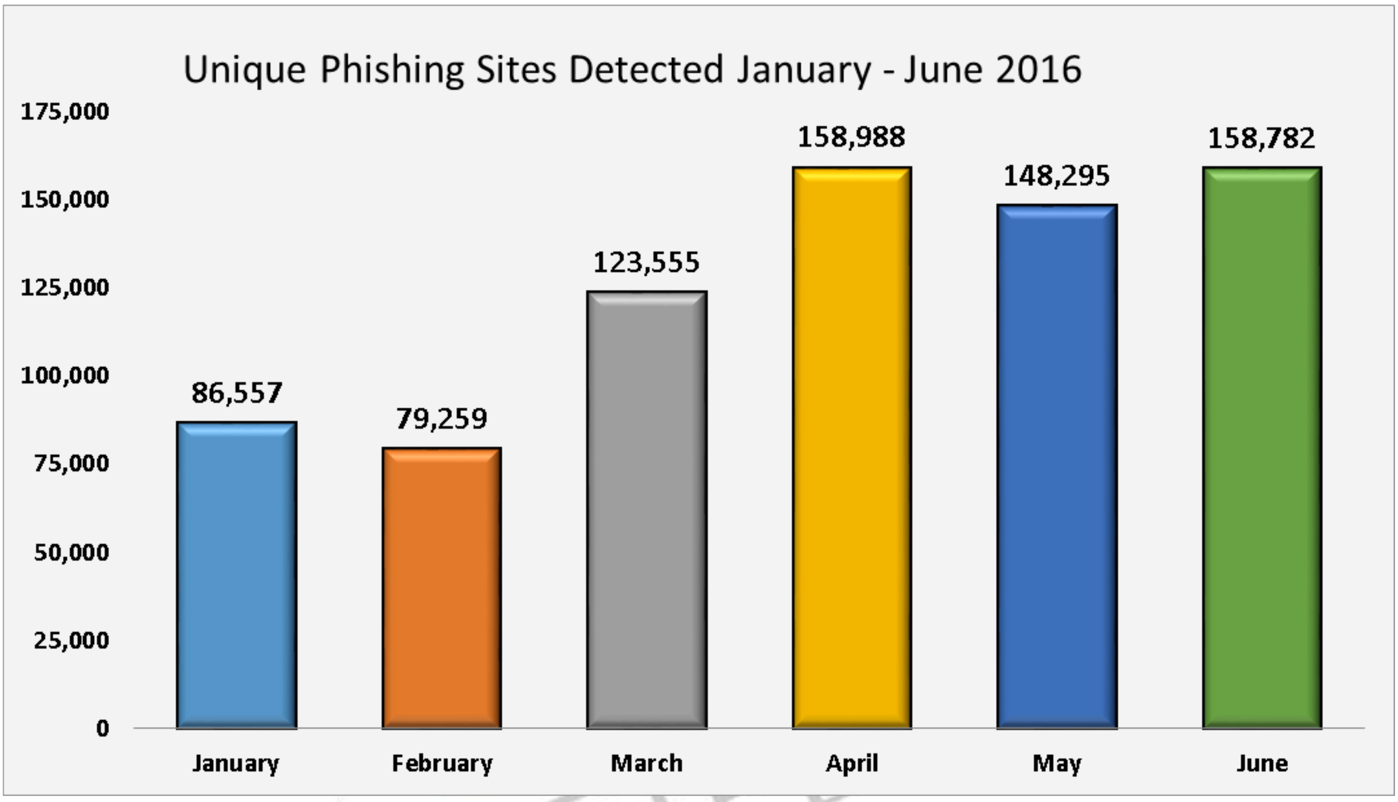


Figure 4 Phishing sites detection in first quarter of 2016

During 2015, there are large number of data breaches. But we must say, companies continue to a good fight against hackers and identifies the theft. In 2016, there are still some of the data breaches happened. Some of them are as follows:

- **FACC- January 25, 2016:** FACC is an Australian aerospace parts manufacturer company announced they fell victim to hackers in January 2016. The criminals approximately steal around $54.5 million U.S. dollars using company's data.
- **University of Central Florida- February 8, 2016:** The University of Central Florida announced a data breach that affected approximately 63,000 current and former students, faculty, and staff at the beginning of February 2016. The cyber criminals compromised the university's computer system and stole a variety of information including Social Security numbers, first and last names, and student/employee ID numbers.
- **U.S. Department of Justice- February 9, 2016:** Hackers were angry about U.S. relations with Israel. They tried to get attention by breaching data of U.S. department of justice. The criminals have stolen information like name, phone number and email address, but they have not stolen important information like social security numbers.
- **Snap Chat- March 3, 2016:** Hackers have stolen 700 current and former snapchat employees' personal information using a phishing scam. As per Snapchat chief executive Evan Spiegel, the attackers simply requested and received sensitive employee information including names, Social Security numbers, and wage/payroll data.
- **Verizon Enterprise Solutions- March 25, 2016:** Verizon enterprise solution is a known IT service providing company and known for data breach assistance to businesses and government sectors around the world. The hackers stole information about 1.5 million consumers.

- **LinkedIn- May 17, 2016:** In 2012, a data breach came to haunt all the LinkedIn user's accounts. The combination of email and password had been stolen by hackers before four years. At the time the breach occurred, members who had been affected were told to reset their passwords. The information then became publicly available in May 2016. Then the password reset not happened.
- **Oracle- August 12, 2016:** Oracle is a very well-known company which has more than 3,30,000 cash registers around the world. Oracle announced data breach in month of August. The breach was uncovered by security expert Brian Krebs.
- **Dropbox- September 2, 2016:** Dropbox is a very popular file hosting service which had a data breach four years before. In 2012, Dropbox helped a small number of users to secure their accounts after some usernames had been stolen. At the end of August 2016, however, it was revealed that more than 68 million Dropbox users had their usernames and passwords compromised in that initial breach.
- **Yahoo!- September 22, 2016:** It may be the most expensive data breach of all time. Yahoo announced that a hacker has stolen information from a minimum of 500 million accounts in late 2014. The hacker stole email addresses, passwords, full usernames, dates of birth, telephone numbers and some of security questions and their answers. Yahoo is still working on the investigation.
- **Weebly- October 20, 2016:** Over 43 million Weebly users were notified about a data breach that happened in February, but was just discovered in October. Stolen data included usernames, passwords, e-mail addresses, and IP information, but Weebly does not believe any type of financial information was stolen because it does not store full credit card numbers on its servers. Hackers were not able to log directly into customer websites because passwords were protected by bcrypt hashing.
- **National Payment Corporation of India- October 20, 2016:** The National Payment Corporation of India (NPCI) was notified by international banks, primarily in the U.S. and China, that some of its customers' debit cards were being used illegally. Experts believe the breach began with a malware attack that originated at an ATM. The NPCI said that 32 lakh debit cards across 19 Indian banks were compromised, but customers were contacted to change the debit card PINs and customers they couldn't reach had their cards canceled and were issued new ones.
- **Cisco- November 3, 2016:** An incorrect security setting on the mobile version of Cisco's "Professional Careers" website created a privacy hole that exposed the personal information of job-seekers. The security vulnerability made sensitive data available between August and September 2015, and again from July to August 2016. That data included names, addresses, e-mails, phone numbers, usernames, passwords, answers to security questions, resumes, cover letters, and voluntary information such as gender, status and disability.

IV. CONCLUSION

This paper gives survey on how and why phishing affects users' personal data. The ways users are attracted to phishing sites and its recorded data throughout year 2016. Several security companies try to collaborate on such attacks and publish data for public to understand and learn. The hackers steal the personal information of companies or users and try to harm them financially.

V. REFERENCES

[1] Marc A. Rader, and Syed (Shawon) M. Rahman, "Exploring historical and emerging phishing techniques and mitigating the associated security risks," IJNSA, vol. 5, no. 4, July 2013.

[2] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson and Filippo Menczer, Social phishing, vol. 50, no. 10, October 2007.

[3] Phishing Activity Trends Report, 2nd quarter, 2016, APWG, published on Oct 3, 2016.

[4] Internet Security Threat Report, Symantec, volume 21, April 2016.

[5] Huajun Huang, Shaohong Zhong, Junshan Tan, "Browser-side Countermeasures for Deceptive Phishing Attack," 2009, IEEE.

[6] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, and Julie Downs, "Who falls for phish? A demographic analysis of phishing suspectibility and effectiveness of interventions", April 10-15, 2010, Atlanta, GA, USA.

[7] Pradeepthi, "Performance study of classification techniques for Phishing URL detection", 2014.

[8] A survey on phishing effects, https://www.identityforce.com/blog/2016-data-breaches.

[9] Xun Dong, John A. Clark, Jeremy L. Jacob, "Defending the weakest link: phishing websites detection by analyzing user behaviors", springer, February 18, 2010.

[10] Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones, "Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones", volume 15, no. 4, fourth quarter 2013.

[11] Ian Fette, Norman Sadeh, Anthony Tomasic, "Learning to Detect Phishing Emails", WWW 2007, May 8–12, 2007, Banff, Alberta, Canada.

[12] Phish Tank, Statistics about phishing activity and phish tank usage. [Online]. Available: http://www.phishtank.com