Volume : 2 | Issue : 3 | Mar 2013 • ISSN No 2277 - 8179

Research Paper

Computer Science

KEYWORDS: Phishing, Mobile Phishing, Clone Phishing, Anti-phishing

Phishing in Mobile Devices: Survey and Prevention Mechanism

Dr. Kuntal Patel — Assistant Professor, CSE Department, Institute of Technology, Nirma University, Ahmedabad

Prof. Parimal Patel — Assistant Professor, Chimanbhai Patel Post Graduate Institute of Computer Application, Ahmedabad

ABSTRACT

Mobile phone becomes essential instrument for our daily routine life. Invention of Smart phone makes our daily business and social activities even more smoothers as we are able to use network or Internet based applications using such smart phones. When we use any networked based application; there is always risks of attacks on our private/ personal network based resources. Various surveys show that phishing is one of the popular attacks now a day to steal the personal information. In this paper we had identified and presented various aspects related to phishing in mobile phones. We had tried to suggest important prevention mechanisms against mobile phishing that can be used to protect our personal information and resources.

II. Introduction to Mobile Phishing

Economists say that continued existence of businesses in the 21st century will depend upon an understanding of and the capability to use current and emerging information technology. One of the buzzword Mobile Technology is already accepted and implemented by many of the businesses to enhance their business performance. As more and more people are using mobile phones for their daily activities, use of mobile phishing technique becomes popular amongst the attackers.

Followings are some of the popular definitions found during literature survey related to mobile phishing:

- Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication [1].
- Phishing is the act of sending an electronic mail (e-mail) to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft [2]. Such e-mail directs the user to visit a Web site where they are asked to update their personal information which later on misused by the attacker.
- SMS phishing occurs when a cell phone receives a SMS (Instant Message or IM) from a fake person or entity [3]. The innocent mobile phone user will reply to a fake SMS and visit a fake URL given in SMS, unintentionally downloading malware and installing malicious programs without the user's knowledge.

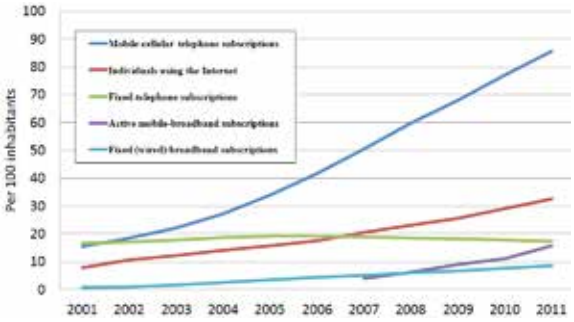
Rapid growth of Mobile technology

Mobile technologies are opening new ways of communication between people, businesses and governments. This instrument offers greater access to data and information for using basic services useful to all in their respective daily operations. No such technology is reached to hand of so many people in the world. This is one of reason behind rapid growth of mobile technology. Now a day cost of basic mobile instrument and cost of service provided by telecom operators are also reduced to great extent. The statistics in figure 1, provided by ITU World Telecommunication clearly indicates the rapid growth of mobile technology [4].

Role of Mobile technology in Society and Industry

Mobile phone communication networks such as 2G and 3G are best known technologies powering our mobile phones. In our daily social life, with the use of 2G and 3G connectivity on our mobile/smart phone and because of the Internet availability, it is possible for us to communicate with our friends. We can communicate through a short written message on an instant messaging application, updates on Facebook or through a video call using Skype.

For the business firms, the mobile based transactions are generating more and more revenues.



(Source: ITU World Telecommunication /ICT Indicators database)

Figure 1: Global ICT development 2001-11

The major categories where mobile based transactions are happening today are as follows: Money transfer using Mobile, Air/ Train/Bus Ticket booking, Content purchase and delivery of goods, Mobile banking, Mobile trading, Auctions, Browsing and many more such types of domains.

Recent statistics show that you save 78% more time shopping online than you do in store along with saving a lot of money in travelling to and from stores [5]. eBay alone, have 300-400 employees working on mobile solutions with reportedly 50% of their sales closing on mobile.

Due to such a vital role of mobile in our society and industry, Mobile phishing becomes important issues now a day's which needs to be tackle carefully to save our resources.

III. Major issues found during literature survey on Mobile Phishing

Lack of knowledge in user about computer and mobile technology: One of the common reasons found during the literature survey about phishing is the lack of proper knowledge of computer and mobile technology. Due to this reason people may click randomly anywhere on the screen and becomes the victim of phishing attack.

Lack of knowledge in user about network security related aspects: Mobile applications are networked based hence network security related basic knowledge is essential for the user performing confidential/financial transaction using mobile phone. Lack of such knowledge indirectly leads to phishing attack.

Trick/Fraud using visual effects: Phishing web sites are created by attackers for forging user personal information. Most of such fake web site has high similarities with the actual web site. Such pages are exactly looks like the real web site. Even Logo's are copied so perfectly and placed on fake web site that for security experts also it is difficult to identify the fraudulent event.

Image as hyper link: Attackers are placing hyperlink behind the normal images. Unknown user may click this image for downloading it, without knowing that on image, there is a hyper link leading to miscellaneous programs/trojan download for phishing purpose.

Lack of security related tools on device: It has been observed that on desktop computers, servers and on laptops generally people install the anti-virus and other security related softwares. But on mobile devices, less number of people is installing security related softwares.

Lack of computing resources on mobile: Many of the mobile instruments offer the software (browser) for browsing web site. But due to limitation of processing and memory power of mobile instruments, it is not possible to implements or executes all cryptographic security related algorithms. This is one of the limitations at present while implementing advanced security related or anti-phishing software on mobile devices.

IV. Types of Mobile Phishing

During literature survey following important types of mobile phishing had been identified. Some the widespread types are listed below:

Deceptive phishing:

Deceptive phishing attacks usually involve the use of e-mail message that appear legitimate, but in reality they are an effort to collect personal data and information [6].

Spear Phishing:

Attacker's attempts directed at specific individuals or organization for collecting information is called spear phishing.

Content-

Injection Phishing means the circumstances where attackers replace part of the content of a genuine site with fake content designed to misdirect the user into giving up their personal information to the attacker.

Clone Phishing:

A type of phishing attack whereby a genuine and earlier delivered, email containing fake link had taken and used to create an almost identical or cloned email. The link within the email is replaced with a malicious program link.

Malware-

Based Phishing refers to scams that involve running malicious software on users' PCs.

Loggers:

Key-loggers and Screen-loggers are types of malware that track keyboard input and send relevant information to the hacker via the Internet.

Web Trojans pop up invisibly when users are attempting to log in.

Hosts File Poisoning:

By "poisoning" or changing the hosts file content, hackers have a bogus address transmitted, taking the user to a fake similar website where their personal information can be easily theft.

Session Hijacking describes an attack where end user's activities are tracked until they sign in to a target account and establish their bona fide credentials.

DNS (Domain Name System) -

Based Phishing: Also known as Pharming, is the term given to hosts file modification or DNS-based phishing. With a this type of attacks, hackers interfere with a hosts files or domain name system of the organization so that requests for fake URLs can be inserted into it.

Man-in-the-Middle Phishing is difficult to detect as it is passive kind of attack. In these attacks hackers simply record the information being transferred between legal users. Later they may mis-use this information.

V. Mobile phishing preventions mechanism

There are various techniques available to fight with phishing. Followings are the important anti-phishing techniques one can use to protect themselves against phishing attacks.

- Use of anti-phishing software: If you are going to perform any payment related transactions on your phone, make sure that it is protected with anti-phishing related softwares. Anti-phishing procedures can be implemented as one of the features embedded along with web browsers as an extensions. Also, anti-virus, anti-spyware and anti-malware softwares should be installed on the smart phones to avoid attacks by miscellaneous programs.
  One of the more popular approaches to avoid phishing is to maintain the record of known phishing sites and to verify websites against such list. Microsoft's IE7 web browser, Mozilla Firefox 2.0, Safari 3.2, and Opera all contain this type of anti-phishing measures.
- Some of the newer browsers like Internet Explorer Version 8 onwards display the entire URL in grey color, with just the domain name with black color; this helps users in identifying fake web site URLs.
- Training people: It is general observation that Users are not reading full security related messages pop-upped by the system, even when it is clearly displayed to them.
  Train individual mobile users, employees and students through seminar, workshops and conferences to make them aware about various types of phishing and security related system messages and their probable prevention mechanisms.
- Browse website through secure connection: Today's browsers offer different functionalities to establish the secure connection. One of such popular method is the use of Secure Socket Layer (SSL) based connection to web site which will reduce the possibilities of attacks on network.
- Check complete URL before pressing Submit button: One should always check the complete web site address (URL) of any web page before clicking on any submit button of that page. Note that it's very easy to replicate the look of any web site but attacker cannot replicate the same web site's domain name for attacking purpose.
- During online form filling process, at any point of time if you fill that such information should not be asked by this web page then immediately stop your transaction and inform the respective authorities regarding the same. For example, during online banking transaction, bank site may ask your mobile number for sending one time password(OTP), but if your mobile's IMEI number is asked then it can be the case related to phishing attacks because mobile's IMEI number can be used for cloning your mobile phone.
- Avoid remember my password utility of the browser while performing your online banking/finance related transactions.
- Phishing email filters: Dedicated spam e-mail filters can reduce the number of phishing e-mails coming to our inboxes. Set proper filter parameters to eliminate known phishing related keywords.

VI. Conclusion

It is fact that there is no such software that can provide us absolutely secure environment over the mobile network/Internet based applications. Also, some of the technology used by mobile/smart phones are relatively novel. So it is the responsibility of researchers and businesses to make mobile users aware about such phishing attacks and its probable phishing avoidance security mechanisms. The mobile applications developer and implementer must provide some solid security mechanisms so that businesses and customer can make use of such mobile networked based applications without fear. This paper is one of the steps towards invoking awareness about the mobile phishing attacks and its prevention mechanisms.

REFERENCE

[1]. Wikipedia, the free encyclopedia. Retrieved February 10, 2013, from http://en.wikipedia.org/wiki/Phishing [2]. Retrieved January 12, 2013, from http://www.webopedia.com/TERM/P/phishing.html [3]. Retrieved February 13, 2013, from http://www.techopedia.com/definition/24898/sms-phishing [4]. ITU - International Telecommunication Union. Retrieved February 15, 2013, from http://www.itu.int/ITU-D/ict/statistics/material/excel/20112/ictwebsite/ Global_ICT_Dev_01-11.xls [5]. Retrieved February 15, 2013, from http://socialmediatoday.com/gloople/1002941/importance-mobile-commerce [6]. Retrieved February 16, 2013, from http://www.pcworld.com/article/135293/article.html