[Chapter: Spam]

[Overview: This chapter starts with a general introduction to what Spam is, what Spammers aim to achieve, how they achieve it and what is the role of a user in a spam related attack. It will mainly focus on Phishing threats.]

1]

The general definition of Spam is “unsolicited messages” which are sent to users usually in a digital format and are also known as ‘junk mail’. This type of messages often contain advertisements for ‘special’ offers on a variety of products and services, other times they contain information about certain events on a news topic or a made up story that aims to urge the user to check it out also known as click-bait.

Some of the popular types of frauds spread by spam e-mails:

- The Nigerian prince / 419 Fraud: Help transfer money from a foreign bank account by paying transaction fees where a reward is promised in return.
- Work at home jobs that offered high paying salary that requires minimal labour and usually no experience.
- Revolutionary weight loss pills or other remedies.
- Foreign lottery : Claiming that you have won the lottery and then requesting personal details in order to claim the prize
- Travelling: Winning trips to foreign locations. In order to retrieve tickets the message would request personal details.
- Issue with a personal account that requires immediate action. most likely bank account.

Spam is spread by:

1. **E-mails**
2. **Instant messaging applications** [**SPIM**]
3. **Voice over IP** services (calls that take place over the internet) [**SPIT**]
4. **SMS** (Short Message Service) **messages**.
5. Other forms of messaging or communication (including **Social media and websites**)

A website called SecureList, run in part by members of Kaspersky Lab, reported information from their (security) products where on average spam took up approximately 70% of the e-mail traffic in the 3rd quarter of 2014. The amount of spam in previous years has reached similar if not greater percentage of the e-mail traffic.

Spam can contain malicious software that corrupt or steal data and even damage the computer system. These types of software are known as malware. [http://techterms.com/definition/malware]

Spammers aim to collect as many active e-mail addresses as possible in every way and any way they can. Some of the ways that they collect and maintain addresses are:

- By purchasing information from databases or accessing information from leaked databases (Illegal)
- Search the internet for e-mail address that are publicly available
- Generating e-mail address by using words from a dictionary and checking whether a service considers them as valid. This is called a brute force attack (trial and error attack) and is usually used to decrypt cipher text (encrypted messages).
- People that open spam e-mails or click on links in those e-mails.

On Android devices spam can appear in the form of notifications in a user's notification bar (push notification ads) or in the form of many pop up advertisements and in the form of application shortcuts on a user's screen (icon ads)[http://google.about.com/od/androidtipscategory/qt/Avoiding-Android-Spam.htm]. Android developers have attempted many times to get users to click on advertisements as they can profit by advertisement traffic. One of the ways is changing the location of the close/dismiss button on advertisement and another is to create spam notifications even when the applications is running in the background and they might have nothing to do with the application itself.

References

- Simon Hill. (2015). Digital Trends, How to shut off Android notifications (Updated for Android 5.0). Available at: http://www.digitaltrends.com/mobile/how-to-deal-with-android-notification-spam/ [Last Accessed on March 14th 2015]
- K. T. Bradford. (2011). GottaBeMobile, Getting Spam Or Mysterious Alerts In Your Android Notification Bar? Here's How **to Get Rid of** Them**. Available at:** http://www.gottabemobile.com/2011/12/20/spam-in-your-notification-bar/ [Last Accessed on March 14th 2015]
- Marziah Karch. About.com, Avoiding Android Spam. Available at: http://google.about.com/od/androidtipscategory/qt/Avoiding-Android-Spam.htm[Last Accessed on March 14th 2015]
- Click-bait definition. (2015). Oxford University Press, Oxford Dictionaries. Available at: http://www.oxforddictionaries.com/definition/english/clickbait **[Last Accessed on March 14th 2015]**

- Federal Bureau of Investigation, Internet Fraud. Available at: http://www.fbi.gov/scams-safety/fraud/internet_fraud **[Last Accessed on March 14th 2015]**
- Andy Walker. (2008). Que Publishing, Spam: Unwanted Email from Hell. Available at: http://www.quepublishing.com/articles/article.aspx?p=1234199&seqNum=6 **[Last Accessed on March 14th 2015]**
- Panda Security, Types of Malware, Spam: Unsolicited email messages . Available at: http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/ **[Last Accessed on March 14th 2015]**
- Chris Hoffman**. (2014). How-To Geek, HTG Explains: How Do Spammers Get Your Email Address? Available at: http://www.howtogeek.com/180477/htg-explains-how-do-spammers-get-your-email-address/ [Last Accessed on March 14th 2015]**
- Tatyana Shcherbakova, Maria Vergelis, Nadezhda Demidova. (2014). SecureList, Spam and phishing in the Q3 of 2014. Available at: **http://securelist.com/analysis/quarterly-spam-reports/67851/spam-and-phishing-in-the-q3-of-2014/** [Last Accessed on March 14th 2015]

2]

Phishing is a form of spam where the purpose of the message is to gather sensitive information from potential victims such as username, password or credit card details by deceiving users into handing over information. The people that send this type of message want to exploit this information in order to gain profit by charging the user or in general by stealing a user's identity. They usually look like a legitimate letters from a service, which usually redirects users to a website that imitates that service's website. It can start by urging users to take immediate action on reviewing some unusual activity on their account or by asking users confirm account details or other sensitive information.

Clone Phishing: This form of phishing attack creates a cloned version of a delivered e-mail that contained attachments. The attachments are replaced with malicious code and the message is resent to the original e-mail addresses, making it look like the original sender was the one sending it.

Spear Phishing: This is a form of phishing is more focused; it uses some knowledge about you and your internet usage. This can include:

- Contacts (Friends or Family)
- Websites that you have visited
- Services that you have used
- Information that you have shared on different social media platforms

This information is used in order to attempt to access your accounts and other sensitive information.

Whaling: This form of phishing attack is a variation of spear phishing that mainly focuses on people of a higher profile/status such as celebrities, politicians etc.

DNS-Based: This form of phishing attack uses a router where a public WiFi access point is set up to attract users. The attackers DNS and phishing server is used to trick the victim (user) into entering personal/account details on fake web pages that imitate an official website's pages. (Also known as a form of man in the middle attack)

Smishing: This form of phishing attacks takes place on a mobile device through SMS messages that usually request information or include malware infested website links.

Phishing attacks can also make a user subscribe to premium rate text messaging services or take the form of bogus security software/applications such as an antivirus. Malware that can be spread through these attacks can also be used to gain access to certain information on devices or even spy on users.

On Android devices phishing attacks can take the form of an application that imitates a legitimate application in the android market or the android market application itself. An application of this type may manipulate a user's browser or simply record sensitive information. Recently there was a report of a smishing (SMS phishing) attack on android devices where a message from a bank told users to install some kind of security application. However the link would download a malicious application (malware) that would either uninstall legitimate bank applications or would force the user to do it through a modified android market (google play) application. It would then replace the bank applications with altered applications of the uninstalled bank applications that would send data to a remote server. Similar attacks have been observed with popular applications where cloned applications that contained malware would show up in the android market. Applications like these can make a user subscribe to premium rate text messaging services. or take the form of bogus security software/applications such as an antivirus.

References

- Carlos Castillo. (2013). McAfee Labs, Phishing Attack Replaces Android Banking Apps with Malware. Available at: https://blogs.mcafee.com/mcafee-

labs/phishing-attack-replaces-android-banking-apps-with-malware **[Last Accessed on March 14th 2015]**

- **Michael Mimoso**. (2014). Thread Post, Cloned Android Banking App Hides Phishing Scheme. Available at: https://threatpost.com/cloned-android-banking-app-hides-phishing-scheme/106867**[Last Accessed on March 14th 2015]**
- Phishing.org, **Phishing and Identity Theft**. Available at: http://www.phishing.org/resources/phishing-identity-theft/**[Last Accessed on March 14th 2015]**
- (2014). Crimewales, Clone Phishing definition. Available at: https://www.ecrimewales.com/en/archive/clone-phishing **[Last Accessed on March 14th 2015]**
- Symantec Corporation, Spear Phishing: Scam, Not Sport. Available at: http://uk.norton.com/spear-phishing-scam-not-sport/article **[Last Accessed on March 14th 2015]**
- Margaret Rouse. (2014). WhatIs.com, Whaling definition. Available at: http://searchsecurity.techtarget.com/definition/whaling **[Last Accessed on March 14th 2015]**
- John. 101Hacker.com, DNS-Based Phishing Attack in Public Hotspot. Available at: http://www.exploit-db.com/wp-content/themes/exploit/docs/20875.pdf **[Last Accessed on March 14th 2015]**
- Tom Fox-Brewster. (2014). The Guardian, Check the permissions: Android flashlight apps criticised over privacy. Available at: http://www.theguardian.com/technology/2014/oct/03/android-flashlight-apps-permissions-privacy **[Last Accessed on March 14th 2015]**
- (2014). Computero, How Not to Go Phishing. Available at: https://computerobz.wordpress.com/tag/clone-phishing/ **[Last Accessed on March 14th 2015]**

- Linda Musthaler. (2013). Network World, **How to avoid becoming a victim of SMiShing (SMS phishing).** Available at: http://www.networkworld.com/article/2164211/infrastructure-management/how-to-avoid-becoming-a-victim-of-smishing-sms-phishing.html **[Last Accessed on March 14th 2015]**
- T-Mobile, Privacy & Security Resources. Available at: http://www.t-mobile.com/company/privacyresources.aspx?tp=abt_tab_phishingsmishing **[Last Accessed on March 14th 2015]**
- (2013). Kaspersky Lab, THE EVOLUTION OF PHISHING ATTACKS: 2011-2013. Available at: http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf **[Last Accessed on March 14th 2015]**

3]

Android permission system involves what actions an application can perform. A list of permissions is shown before installation where it requests the user to grant them in order to install the application. If the user does not want to grant these permissions then they are unable to install the application. Permissions are split into groups such as SMS (where an application is granted permission to read, receive and send SMS messages), Location (where an application can keep track of approximate or precise location) and Contacts (where an application can read or modify contacts on a device).

Users can often agree to an application's permissions without considering the possibility that an application can abuse them. Recently there were reports of top-rated flashlight applications in the android market that were requesting a lot more of permissions than they required. Applications like these required permissions such Location, Identity, Microphone etc. The problem with this is that applications like could record information that has nothing to do with the application functionality and can quite possibly be used to spy on users (Spyware). Some people however could argue that installing an application like this is optional and the user has the power to grant the permissions. When updating applications they can request for new permissions before updating and if they are not granted, the user cannot acquire the latest update. This might be a problem with security as older versions might be more vulnerable to attacks.

In the paper "**Android SMS Malware: Vulnerability and Mitigation**" by Khodor Hamandi, Ali Chehab, Imad H. Elhajj and Ayman Kayssi there is a study that talks about malware that use a device's SMS services and how privileges that were granted by a user can be abused and still remain undetected by security software. It stresses the fact that privileges that have been granted before installation can become dangerous, as they remain unmodified. Android's broadcast service, which distributes data to services/applications that request them, does not guarantee that all applications will receive the original/unmodified data. Malicious software can be registered with top priority, which means that they would receive the data first and therefore can modify the data.

This software, with the malicious code can suppress notifications of misuse and can continue to drain a user's credit without them noticing. In order to test the a scenario like this an application has been developed by the team in order to act as the malicious application where it will be suppressing notifications, sending messages and removing them from the local messages database so that a user will not have a history of these events. The application that was implemented in such a way that it would re-run services that have been terminated and it will continue with its malpractice.

It has been tested between two devices one of which being an Android smartphone. When anti-malware applications were run, this application was not detected and it was even successfully published to the official android market. Finally the study suggested solutions to

this problem such as: not allow applications to set their own priority (and possibly assigning a trusted application as the highest that will be in control), always inform a user when with the receipt of a SMS message and request permission each time a SMS message is sent.

References

- Chris Hoffman**. (2014). How-To Geek, Android's Permissions System Is Broken and Google Just Made It Worse**. Available at: http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/ **[Last Accessed on March 15th 2015]**
- Google Support, Review app permissions. Available at: https://support.google.com/googleplay/answer/6014972?hl=en-GB**[Last Accessed on March 15th 2015]**
- Chris Hoffman**. (2012)** . MakeUseOf, How App Permissions Work & Why You Should Care [Android]. Available at: http://www.makeuseof.com/tag/app-permissions-work-care-android/**[Last Accessed on March 15th 2015]**
- Hamandi, K.; Chehab, A.; Elhajj, I.H.; Kayssi, A., "Android SMS Malware: Vulnerability and Mitigation," *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* , vol., no., pp.1004,1009, 25-28 March 2013
  doi: 10.1109/WAINA.2013.134
  URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6550526&isnumber=6550285 **[Last Accessed on March 15th 2015]**

4]

Spam Detection

Spam filter is software that filters incoming messages in order to block incoming spam. Messages are classified by the filter based on certain rules and algorithms. If a message is marked as spam, it usually ends up in the junk/spam folder. If a message does not show any signs of being spam or it is from a trusted sender then it is added to the user's inbox folder.

According multiple online sources on spam, there are many tricks used in order to fool spam filters into thinking that the message is a legit message and therefore avoid detection. Here are some of the techniques used by spammers:

- Line breaks at unexpected parts of a message
- Adding spaces between characters in words
- Replace spaces with a specific character
- Use of characters from foreign languages that look like English characters
- Switching around some letters in words
- Use of HTML code in various was such as encoding characters or adding tiny letters between letters in words, which cannot be noticed by a user.
- Use of JavaScript to hide messages

- Using multiple ‘zombie’ computers to send spam since IP addresses can be added to block lists
- In order to fool spam filter algorithms more sentences are added in order to pass the algorithms’ threshold. These additional sentences can be the same colour with the background of a message so that a user does not notice them.
- Use IP addresses with neutral or positive reputation
- Using tiny URLs instead of full length URLs
- Using encoded URLs
- Use HTML to fool recipient by adding a malicious link on a legitimate service’s URL
- Splitting URLs in different parts and showing how the user can attach the parts to get the original URL

Spammers study how spam filters work so that they can try to exploit their algorithms in order to bypass detection. Spam filters need to be regularly updated with alternative detecting techniques and improved algorithms. As the detection algorithms advance, some problems that can appear are false positive classifications where legitimate messages are marked as spam. Email services such as GMAIL by Google try to improve their algorithms in order to reduce the number of false positive detections by either using familiarity such as adding an e-mail address to an approved senders list (contacts) or allowing users to create their own filters.

There are numerous of patterns that filters tend to look at and there are many websites that help legitimate users avoid spam classification by following some rules in order to improve their message’s quality score. Some of the rules that are mentioned online are:

- Do not use of words such as ‘free’, ’urgent’, ‘click here’, ’once in a lifetime’ or characters such as $$, XXX
- Do not focus mainly on transactions.
- Avoid excessive use of caps lock
- Avoid excessive amount of images or links with not enough text
- Do not use of bright colours and irregular font size (too small)
- Avoid attachment of files of these formats: exe, bat, com etc.
- Claiming that is a legitimate e-mail might trigger a filter into thinking that it is spam
- Use well known mailers such as GMAIL, Hotmail, Yahoo etc.
- Timing : frequent e-mails from an address can be marked as spam

References

- Vivian. (2015). Google support, Anti-virus scanning attachments**. Available at: https://support.google.com/mail/answer/25760?hl=en** [Last Accessed on March 15th 2015]

- Margaret Rouse. (2014). WhatIs.com, Spam Filter definition. Available at: http://searchmidmarketsecurity.techtarget.com/definition/spam-filter**[Last Accessed on March 15th 2015]**
- John Graham-Cumming. (2004). "Hakin9" Magazine, Wydawnictwo Software, Tricks of the Spammer's Trade. Available at: http://www.windowsecurity.com/uplarticle/anti-spam/Spammer_tricks.pdf**[Last Accessed on March 15th 2015]**
- **Google Postini Services, How do I prevent good messages from getting filtered out as spam? (false positives)**. Available at: http://www.google.com/support/enterprise/static/postini/docs/admin/en/troubleshooting_spe/faq_spam_falsepositives.html**[Last Accessed on March 15th 2015]**

- Vivian. Google Support, Legitimate mail is marked as spam. Available at: https://support.google.com/mail/answer/9008?hl=en**[Last Accessed on March 15th 2015]**
- Process Software, Common Spammer Tricks - White Paper. Available at: http://www.process.com/psc/fileadmin/user_upload/whitepapers/pmas/common_spammer_tricks.pdf**[Last Accessed on March 15th 2015]**
- **(2009). IT News Africa, 10 tricks used by spammers to get into your inbox**. Available at: http://www.itnewsafrica.com/2009/11/10-tricks-used-by-spammers-to-get-into-your-inbox/**[Last Accessed on March 15th 2015]**
- CETS Answers, **How can I avoid having my mail blocked by spam filters?** Available at: http://www.seas.upenn.edu/cets/answers/spamblock-false.html**[Last Accessed on March 15th 2015]**
- CETS Answers, **Sending "Prohibited" Attachments.** Available at: http://www.seas.upenn.edu/cets/answers/send-prohibited-attachments.html**[Last Accessed on March 15th 2015]**
- **Mail Chimp , How to Avoid Spam Filters**. Available at: http://mailchimp.com/resources/guides/how-to-avoid-spam-filters/html/**[Last Accessed on March 15th 2015]**

- Sofia Woods. (2012). THE DAILY EGG, 8 Little Known Ways to Avoid The Email Spam Filter. Available at: http://blog.crazyegg.com/2012/06/26/avoid-email-spam-filter/**[Last Accessed on March 15th 2015]**
- **Jeff. (2012). the Email Admin, 5 Tricks Spammers Use to Get Past Your Filter**. Available at: http://www.theemailadmin.com/2012/03/5-tricks-spammers-use-to-get-past-your-filter/ **[Last Accessed on March 15th 2015]**

- Panda Security, Types of Malware, Spam: Unsolicited email messages . Available at: http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/ **[Last Accessed on March 15th 2015]**
- David Greiner**. (2006). Campaign Monitor, What are some good methods for avoiding spam filters?** Available at: https://www.campaignmonitor.com/blog/post/1971/what-are-some-good-methods-for **[Last Accessed on March 15th 2015]**

5] How to stay safe

"Better safe than sorry" is a popular saying that is used in situations where it is important to stay safe and avoid any risks even if the situation might not seem very risky. This is often true when it comes to reading digital messages, even if it might not seem as something that might harm you, it can. Companies can rely on their reputation and productivity in order to be successful. Spam can have a negative effect on a worker's time and productivity; it can also cost a company or an individual a significant amount of money to repair the damages that it might inflict due to the possibility of malware infections or loss of information. Identity theft can damage an individual's credit score by adding a significant amount of debt or even accuse an individual of illegal activity since their name appears in the databases. These are some of the reasons of why it is important to respond appropriately in order to defend against spam.

Spam often-present ideal situations to their potential victims whether it is a job opportunity or a great offer on certain products/services and the saying that comes to mind is "if something is too good to be true, it probably is". One of the first things to look out for is these messages that present ideal situations that are unrealistic. The general rule is to not open spam messages, some of these messages might be detectable from the subject of the message but a lot of them either prefer to leave it blank or ambiguous in order to tempt a user into opening it. If the message that you have received is from an unknown or unfamiliar sender then do not open it.

A message may look very legitimate as spammers can make messages look like they are from a trusted sender by adding the company's logo and creating a similar if not identical layout. However, services in general do not request account details to

be confirmed or shared via e-mail. The best thing to do is to contact the service via telephone to confirm or report the message.

As mentioned above spam can often keep the message as general as possible, not using a user's name or any specific detail about the user. If the message looks suspicious, avoid replying to it and avoid clicking on any link in the e-mail content. If you are unsure type the link into your browser (do not click to open the website) or hover over the link and try to look for any unusual patterns or do some research to find the official link to the service's website and see if they match. Spam often includes an 'Unsubscribe' link in their message that does nothing but confirm that the e-mail address that they used to contact you is active. As an extra security measure, disable the preview pane and loading of images in your mailing software.

Finally, it is highly recommended that antivirus software and filtering software are used and are regularly updated. Some email services such as GMAIL use antivirus software to scan attachments of incoming and outgoing messages for malware. If malware are detected then attachments are made unavailable for download to the receiver or notify the user/sender that the message cannot be sent until the infected attachment is removed.

References

- ELIZABETH KNOWLES. "something sounds too good to be true, it probably is, if." The Oxford Dictionary of Phrase and Fable. 2006. Retrieved March 16, 2015 from Encyclopedia.com:http://www.encyclopedia.com/doc/1O214-smthngsndstgdtbtrtprbblys.html **[Last Accessed on March 15th 2015]**
- Definition of better safe than sorry from the Cambridge Advanced Learners Dictionary & Thesaurus © Cambridge University Press. Available at: http://dictionary.cambridge.org/dictionary/british/better-safe-than-sorry **[Last Accessed on March 15th 2015]**
- Telstra, PROTECTING AGAINST SCAMS AND PHISHING CYBER SAFETY TIPS. Available at: http://www.telstra.com.au/consumer-advice/download/document/cyber-safety-consumer-phishing.pdf **[Last Accessed on March 15th 2015]**
- Kaspersky Lab, Staying Safe Online. Available at: http://www.kaspersky.com/downloads/pdf/staying_safe_online_home_guide.pdf **[Last Accessed on March 15th 2015]**
- StaySafeOnline.org, SPAM & PHISHING . Available at: https://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing **[Last Accessed on March 15th 2015]**
- GCF Learn Free, I**nternet Safety: Email Tips for Scams and Spam**. Available at: http://www.gcflearnfree.org/internetsafety/4.2**[Last Accessed on March 15th 2015]**

- (2014). Air-IT, **Staying Safe from Spam and Phishing Emails**. Available at: http://www.air-it.co.uk/2014/09/staying-safe-spam-phishing-emails/ **[Last Accessed on March 15th 2015]**

- iKeepSafe, How Can I Avoid Spam and Phishing Scams. Available at: http://www.ikeepsafe.org/be-a-pro/online-security/how-can-i-avoid-spam-and-phishing-scams/**[Last Accessed on March 15th 2015]**

- Panda Security, Types of Malware, Spam: Unsolicited email messages . Available at: http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/ **[Last Accessed on March 15th 2015]**

Quiz [random order of quizzes]

Pass mark: 50

Essay type questions

1. Give 5 tricks spammers have used to bypass spam filtering software
2. What is clone phishing?
3. Explain the dangers of identity theft
4. Explain ways to avoid spam/phishing attacks

True/False questions

5. Phishing messages try to sell products to users
6. Phishing messages in general try to obtain information from users either by a response or fake website
7. Spam messages take up most of the e-mail traffic
8. Whaling is a form of phishing where legitimate messages are taken and the links or attachments are changed
9. Spear phishing is a form of phishing that uses information about a user to create a more focused attack
10. Spam filtering software can block all incoming spam
11. It is safe to open all spam as long as you do not click any links
12. Phishing message do not look exactly like legitimate messages

Multiple-choice questions

13. Phishing message do not look exactly like legitimate messages
    - E-mail
    - SMS
    - Mobile Applicatons
    - Instant Message
    - Social Media
    - All of the aboce
    - None of the above

14. Spammers obtain list of e-mails from:
    - Leaked Databases
    - Black market
    - Brute force attacks
    - Social media accounts
    - All of the above
    - None of the above

15. Which one of these is not a phishing form:
    - Spear
    - Whaling
    - Clone
    - Smishing
    - Harvesting

16. Phishing attacks can appear
    - E-mails only
    - Advertisements only
    - E-mails and Advertisements only
    - E-mails and Websites only
    - Advertisements and Websites only
    - E-mails, Websites and Advertisements
    - None of the above