**Spam** can generally be defined as unsolicited messages sent to users usually in a digital format, also referred to as ‘junk mail’. These messages often contain advertisements for ‘special’ offers on a variety of products or services, sometimes they contain information about certain events on a particular topic and other times they request personal details.

Some of the popular types of scams that were spread in the form of spam are:

* The Nigerian prince – 419 Fraud : Help transfer money from a bank account by paying transaction fees where there was a promise of reward
* Work at home jobs that offered high salary and required minimal labour
* 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
* Problems with your an account that you own, most likely bank account.

Spam can be contain malicious software that was designed to corrupt and/or damage computer system, also known as malware. [ <http://techterms.com/definition/malware> ]

Spam is commonly spread via:

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.

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.

**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.

Bibliography

<https://blogs.mcafee.com/mcafee-labs/phishing-attack-replaces-android-banking-apps-with-malware>

<https://threatpost.com/cloned-android-banking-app-hides-phishing-scheme/106867>

http://www.digitaltrends.com/mobile/how-to-deal-with-android-notification-spam/

http://www.gottabemobile.com/2011/12/20/5-tips-for-picking-a-great-smartphone-or-tablet-case/

http://google.about.com/od/androidtipscategory/qt/Avoiding-Android-