Cyber Threats to Mobile Technology Services

Rita Mendes de Azevedo

Lusófona do Porto University, Portugal
ritamendesazevedo@gmail.com

Abstract. With the evolution of technology, we started to see an increase in the usage of mobile technology daily, which for many has become an obligation or necessity due to their work or studies. Consequently, mobile device users over the years started using them more frequently for personal use or work. There are different types of mobile technology like cell phones, tablets, computers, or other devices we can find in companies. Despite the security methods provided by the creators of the operating systems, like android and iOS, they are not enough to protect the users from all the threats that come up daily, such as malicious websites or even emails intended to steal user data.

The emergence of the COVID-19 virus in the year 2020 led most countries to confinement. COVID-19 virus caused mobile technology users to use their mobile devices even more often, consequently, all the attacks and threats became more frequent, but we don't know if our knowledge is necessary to prevent ourselves.

In this paper, will be possible to find the necessary tips to help users protect themselves from these cyber threats and help the readers to learn more about specific threats.

The threats can have different environments and not only is it important to know how to protect our mobile devices from all kinds of threats and attacks but for companies becomes even more important because the damage can be more catastrophic.

Keywords: Mobile Technology, Mobile Technology Services, Cyber Threats, Threats, Mobile Threats, Phishing, Malware, DoS, DDoS, Mobile Security, Tips

1 Introduction

Cyber Threats are one of the biggest problems for mobile device users today. The present group of devices can be of various types like our mobile phones, tablets, laptops, and other devices we use daily.

Cyber threats to mobile devices can include various types of threats and theft, such as the security of our personal data, for example, banking data, privacy, and disrupting our mobile device, whether for personal use, like a mobile phone or tablet of the company we work for. By cyber threats, we mean different types of hacker attacks, as well attacks that can insert malicious code into our devices or even, have the objective of attacking the network we are connected to, and malicious messages with a suspicious link sent to our email or by message to our cell phone.

According to [1] Android devices are the most used and then iOS devices. According to their studies, access to Android devices has been increasing, leading users to need to be more careful.

Consequently, in 2020 the COVID-19 virus appeared, which caused several health problems to the world population, which forced the government of each country to take measures to protect the population while laboratories studied the virus. One of the solutions adopted was confinement, which gave online classes to students and workers working at home. Without the opportunity to leave the house except to buy essential goods, the population was forced to use their electronic devices often, whether for entertainment or to communicate with their family and friends or even for work, thereby, the use of mobile devices increased as also online shopping. With this increase in the use of electronic devices, hackers saw more opportunities to fraud the deceive users and, cyber threats became more frequent.

Sometime later the pandemic started, vaccines against COVID-19 from different laboratories began to be created, and with the vaccination, was created platforms and messages started to be sent for citizens to get vaccinated, according to [2] resulted in a Malware target, and the mobile device's users received fake messages.

Moreover, companies that use mobile devices can also be affected by cyber threats. Although the use of security measures is not inevitable, as any user within the company is connected to the network and takes some action that compromises the network and its data, that's why it's important to have a basic understanding of where certain threats can arise, and especially to avoid the use of company's devices or network for personal use.

In this paper about cyber threats to mobile technology services, different topics will be covered. The topic, Most popular cyber threats, talking about the threats that most affect mobile users' devices and give tips on how to prevent them, the topic, Types of Mobile Threats, talking about the different "environments" from which cyber threats can arise and the topic, How to protect Mobile Technology from Threats, where tips are provided on how to protect both personal and corporate mobile devices.

2 Most Popular Cyber Threats

The various threats to mobile devices mainly occur in the form of malicious code distribution that exploits the operating system and application vulnerabilities. These threats mostly appear by email or message on users' devices.

In this topic, we will see some of the ones that most affect mobile device users and give some tips on how to prevent them.

2.1 Phishing

A current case that catches many people even possibly our friends and family. A phishing attack is done in the form of a message or an email, containing a link for the

victim to open, in which the attackers pretend to be an entity they aren't to make the attack credible.

These attackers usually steal victims' sensitive data such as credit card details or login credentials. This happens when the victim clicks on any link sent by the attacker who takes the form of a genuine entity.[3]

Typically, the most common data stolen by attackers are bank account numbers, usernames, and passwords, credit card details, internet banking details.[4]

Below is an example of a phishing message, where we can see a message received from a personal number, to let me know they have my order waiting for delivery and, to access the link to know more details. In the warning found above with the alert icon, the system is asking if the message received is spam and, if I want to set the number as "Not Spam". The sender's telephone number is usually a personal number, in some cases the message received is already given as a spam alert as seen in the example. This alert occurs due to the user's complaint, in this case, the device presented is an android phone, this helps other users to be careful when receiving the message. Whenever a suspicious message is received it is possible to report the mobile number.

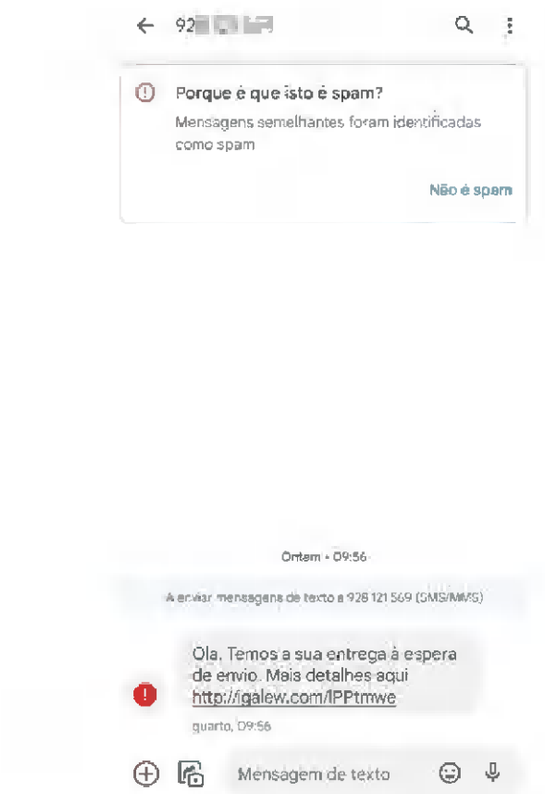

Fig. 1: Phishing message received on an Android phone

2.1.1 Phishing in Portugal

With the pandemic and the increase in online shopping, more phishing attacks emerged, where attackers claimed to be legitimate companies. One of the most frequent mobile device threats that possibly many of us suffered in Portugal, was receiving messages on our mobile phones indicating that our order was in customs and, for dispatch was necessarily accessing the link to pay if we wanted to receive the package, in some cases the user of the device had not even placed any order. For some people with less knowledge about Phishing, people looked for help on social media.

According to [5], phishing was one of the most recorded events. Consequently, one of the cases, the most frequent crime based on the registration of complaints to the PGR Cybercrime Office is fraud in the use of MBWAY, with phishing in 2nd place.

2.1.2 Phishing life cycle

A phishing attack is made up of a cycle with several steps.

The first step is planning, the attacker starts by planning the attack, identifying the victims, the target information, and the technique to use in the attack. Following, the attacker starts the "collection" step, as soon as the victim takes an action making him susceptible to information theft, he is then urged to submit his credentials through a trustworthy-looking webpage. Normally, the fake website is hosted on a compromised server, which has been exploited by the attacker for this purpose. The last step is given by "Fraud", finally, and once the attacker has achieved his goal, he then becomes involved in fraud by impersonating the victim.[6]

2.1.3 How to prevent phishing

In the case of receiving e-mails, it is necessary to pay attention if the e-mail address corresponds to the real company/entity, sometimes attackers create accounts with a similar e-mail address, changing insignificantly for users not to notice.

As for the phishing attempt by receiving a message on the mobile phone, it's necessary to pay attention to the address of the link sent, for most people it is easy to notice that it does not a legitimate link, in case of doubt, the attempted attack is almost always made by a personal mobile number of an operator. It's recommendable searching for the contact on google you can find information and comments about the contact on specific websites.

To test your knowledge of recognizing phishing attempts you can consult sites like phishingquiz.withgoogle.com, it will help you to increase knowledge about phishing.

2.1.4 Simulate phishing with Microsoft Defender

Although building a phishing website is a time-consuming and complicated process, it is possible to find phishing attack simulators to test your companies' policies and practices.

One of the most suitable is the Microsoft simulator, to have access you must have the Microsoft Defender for Office 365 plan 2.[7]

It is possible to select different techniques such as credential harvest (attempts to collect credentials), malware attachment, link in attachment, kink to malware, drive-by URL. The malicious URL in the message takes the user to a familiar-looking website that silently runs and/or installs code on the user's device.[7]

In each one, when selecting the desired one, first the name and description of the simulation are defined, then on the "payload" page, it is possible to define the language and view information such as the number of people who clicked on the link. For this same simulation, it is possible to determine specific users and groups for which it is intended and to carry out and simulate training in order to test the employees' knowledge.[7]

2.2 Malware

Malware is a contraction of malicious software, is designed to destroy computer systems and programs. It has many forms such as virus, worm, Trojan, and spyware. Malware can attack personal and organizational computer systems.[8]

2.2.1 Trojan

Given as a type of malware, Trojan is a program in which the code contained is harmful or data that takes control and its chosen form of damage, such as ruining or erasing data on the hard drive. A Trojan can cause massive harm to computer systems and may turn a system into a killing machine as well.[9]

2.2.2 Worm

Given as a type of malware, Worm is a program that self-propagates across a network exploiting security or policy flaws in widely used services.[10]

For a worm to infect a machine, it must first discover that the machine exists. There are several techniques for discovering multiple machines such as pre-generated target lists.[11]

2.2.3 Spyware

Given as a type of malware, Spyware is a type of software that can install itself or run on a user's computer without providing notice, consent, or control to the user. Usually hidden among other programs or can be unwittingly downloaded to a user's system when specific websites are visited.[12]

2.2.4 How to prevent Malware

As [13] says, we can prevent Malware in the following ways:

- Keep your computer's current software up to date. The operating system and anti-virus application must be updated regularly.
- Always think before you install something. You don't know if the lengthy license agreement that you normally don't read, area waring you are about to install Spyware.
- Only download updates from reputable sources.
- Install and use a firewall.

2.3 Application Vulnerability

According to [14] application vulnerability is threats that perform malicious actions such as elevation of privileges by using the vulnerability of the developed application.

2.3.1 How to Prevent Application Vulnerability

This threat is aimed at programmers, according to [15], to protect applications some of the needs are, developing secure code, input validation, hotspot protection, output validation, and vulnerability detection.

2.4 DoS (Denial of service attack) and DDoS (Distributed Denial of service)

According to [16] denial of service (DoS) attack occurs when users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Affected services may include for example e-mail, web-sites, online accounts, or other services that are dependent on the affected computer or network. While DDoS attack occurs when multiple machines are operating together to attack one target.

2.4.1 Attack Symptoms

Both DoS attack and DDoS have the same symptoms, these are slow network, Unavailability of a particular website, or an inability to access any website. [16]

2.4.2 What to do if you are experiencing a DoS or DDoS attack

Most likely this type of attack happens in companies, but it is not inevitable that it also occurs in our home network when we are experiencing a DoS or DDoS attack it is possible to take some measures.

When we are targets of DoS and DDoS attacks, we can contact our network administrator to confirm whether the service outage is due to maintenance or an in-house network issue and contact our ISP to ask if there is an outage on their end or even if their network is the target of the attack and you are an indirect victim. [16]

3 Types of Mobile Threats

Threats to mobile devices can arise in several ways, as mentioned in the previous topic, in addition to cyber threats made by hackers, threats can be of other categories.

3.1 Physical Threats

Physical attacks can, as the name says, be practiced at the physical level by the attacker. Under these circumstances, it is easier to carry out a physical attack on a mobile device than on a computer, for example, our mobile phone despite being constantly with us, is more difficult to perceive its absence than a computer and it is faster for us to notice that disappeared due to its size.

The attacker can, through physical access to a mobile device, perform malicious actions, such displaying as flashing it with a malicious system image, that is connected to a computer to install malicious software or conduct data extraction. So, it is important not to leave devices unattended so that this type of threat does not occur. In addition, device authentication and encryption need to be applied to secure mobile devices against unauthorized access.[17]

3.2 Network-based Threats

You've probably read or heard cases of attacks on corporate networks on the news, so it's important to be careful when using a wi-fi network or even with whom you connect to your home/business network and, in addition to using Wi-Fi, be careful also when using Bluetooth connection.

Wi-Fi and Bluetooth interfaces have their own vulnerabilities and are susceptible to wireless eavesdropping attempts, using readily available tools like Wifite or Aircrack-ng Suite. [17]

3.2.1 Basic tips when using and with our Wi-Fi network

When using Wi-Fi networks and letting guests use our network, there are precautions that users can take to better protect our network and mobile device, these being basic tips for any user:

- Avoid connecting to public Wi-Fi networks, instead use mobile data or search for a more secure network.
- Keep the device's Wi-Fi turned off when you don't need to use it.
- At home, to protect the Wi-Fi network, you can create a guest account and keep the router in a barely visible place in case of visitors, change the predefined password and in case of doubt, install a specific program such as Nmap to check if there are open ports so there are no intruders.

3.3 System-based Threats

Manufacturers can sometimes introduce vulnerabilities into their devices unintentionally. Sometimes these incidences need to perform timely updates of mobile devices to mitigate system issues.[17]

3.4 Application-based Threats

Even if software updates are available, users may not update applications on their mobile devices promptly. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with this software. Malicious applications, also known as malware, mentioned earlier in this paper what this type of attack is.[17]

4 How to protect Mobile Technology from Threats

To protect mobile devices, besides basic knowledge about mobile threats, it is important to know how to protect mobile devices while using them.

The devices may include our personal data as well from the company we own or work for, so it is important to know what procedures the users should take, in order to make devices safe to use and protect them from the use of third parties.

An example applied could be, a friend of the mobile device user asks to consult his/her e-mail address, the user, when letting the friend use the device, does not know if he/she has sufficient knowledge about mobile threats, for example, phishing and may end up opening a malicious email that compromises personal data or the device.

Hence, it is important to take the necessary precautions to protect these same devices and that's why it's important to know if that person has the basic knowledge, before letting them access certain applications on their mobile device.

4.1 For individual users

The following measures indicated by Kaspersky [1] for individual users are intended for users of android mobile devices, namely:

- Protect your devices with secure passwords, it helps to prevent attackers from accessing personal data by stealing your device and brute-forcing the password.
- Never enable the option that enables apps from third-party sources to be installed on the device, the best is always to keep it turned disabled.
- It's recommendable using the apps that antivirus software developers often create applications designed to test devices for unclosed vulnerabilities. Such applications are regularly updated to include data on newly discovered vulnerabilities.
- Use a security solution on your device and make sure it scans files as they are downloaded and protects the device from other types of Internet attacks.
- When making bank payments, always use 2-factor authentication.

- Use encryption if you have any valuable information (financial, personal, or work-related) on your device.
- If you believe that you may have fallen victim to or witnessed a cybercrime, do not hesitate to contact law enforcement as soon as possible.

4.2 For Corporations

The following measures indicated by Kaspersky [1] for corporation users are namely:

- The Bring Your Own Device approach, which allows employees to use their personal devices for work, can expose your company to virtually all 'consumer' IT security risks: sensitive corporate data stored on an employee's personal phone could be a valuable find for cybercriminals. A security solution with Mobile Device Management capabilities, including encryption and remotely wiping data from smartphones, will help you to keep your sensitive business-related information secure.
- If employees' companies are not aware of simple IT security rules, this is likely to cause security incidents. Training people to handle their mobile devices appropriately will be a worthwhile investment.

5 Conclusion

Cyber threats are one of the factors that most affect mobile device users, and it is necessary to take precautions to make the use of mobile devices safe, one of the possible consequences if the user is a victim of a threat is the theft of personal data.

To understand what these types of attacks are, it was defined each one was given and tips on how to prevent them. It was possible to observe phishing, malware, application vulnerability, DoS, and DDoS attacks.

About phishing attacks was also talked about the effects that the pandemic caused in Portugal regarding cyber threats, the life cycle of a phishing attack and the Microsoft phishing simulator was presented. About Malware, it was possible to discover that there are several types of attacks, each with a different objective.

Although most attacks have the involvement of a hacker, threats can be of different types, as seen above these can be physical threats, network-based, system-based, and application-based. As seen, all related to device software attack, but physical attacks are simply given by physical access to the device compromising its software as well.[17]

While it's important to learn how to protect our devices and data, it's also important to protect our company from employees' misuse of mobile devices by taking extra care and providing the necessary training.[1]

In a future paper, more cyber threats that affect mobile device users may be included and examples of how some of the threats are carried out along with statistics, helping further to appeal how dangerous it can be or the damage it can cause without due care in the use of mobile devices.

10

References

1. Kaspersky and INTERPOL Joint Report," Mobile Cyber Threats" 2014 https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf
2. McAffe, "McAffe Mobile Threat Report" 2021 https://www.mcafee.com/content/dam/global/infographics/McAfeeMobileThreatReport2021.pdf
3. Antonette R. Muntode and Sandeep S. Parwe, "An Overview on Phishing- its types and Countermeasures" 2019 https://www.researchgate.net/publication/342118299_An_Overview_on_Phishing-_its_types_and_Countermeasures/link/5ee2d851299bf1faac4e66b2/download
4. Muhammet Baykara and Zahit Ziya Gurel, "Detection of Phishing Attacks," ISDFS, 2018
5. National Cybersecurity Center Portugal, Cybersecurity Observatory, "Cybersecurity in Portugal" 2021 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_riscos_conflitos2021.pdf
6. Rami M. Mohammad,Fadi Thabtah and Lee McCluskey, "Tutorial and Critical Analysis of Phishing Websites Methods" (last access December 2021) https://core.ac.uk/download/pdf/206070797.pdf
7. Microsoft contributors, "Simulate a phishing attack in Defender for Office 365" (last access December 2021) https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide
8. Mariwan Ahmad, "Malware in Computer Systems: Problems and Solutions" 2020 https://www.researchgate.net/publication/340770783_Malware_in_Computer_Systems_Problems_and_Solutions
9. Ghossoon M. Waleed and Hilal Mohammed Yousif Al-Bayatti, "A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems" 2011 https://www.researchgate.net/publication/51891535_A_Comparison_of_Trojan_Virus_Behavior_in_Linux_and_Windows_OperatingSystems
10. Mark Eichin and Jon Rochlis. With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. In IEEE Computer Society Symposium on Security and Privacy, 1989
11. Robert K. Cunningham, Nicholas Weaver, Vern Paxson and Stuart Staniford, "A taxonomy of computer worms" 2003 https://www.researchgate.net/publication/220796741_A_taxonomy_of_computer_worms
12. D Anil Kumar, Sisira Kumar Kapat, Susanta Kumar Das and Satya Narayan Tripathy, "Classification of Spyware Affected files using Data Mining Techniques" 2019 https://www.ijrte.org/wp-content/uploads/papers/v8i2S6/B10880782S619.pdf
13. Robert Moir, "Defining Malware: FAQ" 2009 https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN
14. Kim Hee Wan, "A Study on the Mobile Application Security Threats and Vulnerability Analysis Cases" 2020 http://koreascience.or.kr/article/JAKO202034465346164.pdf
15. Nuno Antunes and Marco Vieira, " Defending against Web Application Vulnerabilities" 2012 https://eden.dei.uc.pt/~mvieira/2012_Computer_DefendWeb.pdf
16. Cybersecurity&Infrastructure Security Agency, "Security Tip (ST04-015) Understanding Denial-of-Service Attacks" 2009 https://us-cert.cisa.gov/ncas/tips/ST04-015
17. Pang Jian Hao Jeffrey, Chua Chee Leong, Chan Guan Huat and Lim Seh Leng, "Challenges in Mobile Security" 2016 https://www.dsta.gov.sg/docs/default-source/dsta-about/challenges-in-mobile-security.pdf?sfvrsn=2