Table of content

Mobile Phone Security: Protecting Your Device and Data in the Digital Age

Abstract

With the increase in mobile phone users and the creation of various applications, people use mobile phones for social networking, mobile payment, shopping transfers, etc., and the importance of mobile phones in people's lives is becoming more and more obvious. But at the same time, the risk of cyberattacks, data breaches, and identity theft is increasing, making mobile security a hot topic and a fundamental issue. This article aims to explore the current state of mobile security, including various common and unusual threats, attack principles, cases, and how to prevent them. It will also examine emerging trends and technologies in the field of mobile security, such as biometric authentication and secure software development practices, and how these technologies can best help different populations. The paper is aimed at a wide range of people, including individuals, businesses, and will provide insight into the security risks associated with mobile devices. It aims to let professionals or non-professionals understand mobile phone security more comprehensively and help them use mobile phones safely in daily life.

Introduction

Twenty years ago, the main function of a mobile phone was communication; people mainly used it to make phone calls or send text messages. Ten years ago, smart phones began to emerge. Mobile phones added functions at the software level so that people could use them for entertainment, photography, video, and social networking. Around 2009, smart phones began to popularize and gain applications. It is worth mentioning that the iPhone 4 was officially released on June 8, 2010, symbolizing the official opening of the smart phone era. Going back to the present, as of November 15, 2022, according to the data, the world population had reached 8 billion. According to Statista, by 2023, the number of smartphone users in the world today will be 6.92 billion, which means 86.29 percent of the global population will have a smartphone. That's up sharply from 2016, when there were 3.668 billion users, or 49.40 percent of the world's population that year.

However, as the use of mobile devices and the valuable information they contain increase, so does the risk of cyberattacks, data breaches, and identity theft. Mobile devices now account for more than 60% of digital fraud, from phishing attacks to password hacks (Reader's Digest, 2023). At the same time, criminals are increasingly focused on penetrating banking apps (cyber security intelligence, 2022). Randy Pargman, senior director at cybersecurity firm Binary Defense, said: “The more you rely on your phone for everyday tasks, the greater your loss if your device is compromised." (Reader's Digest, 2023). Fortunately, mobile phone attacks are not unavoidable. By understanding mobile phone vulnerabilities and attack methods, we can regulate their use in our daily lives. Our actions can prevent certain attacks, reduce threats, and ensure the security of assets on mobile phones.

Identify your mobile asset

Having a good understanding of your mobile assets can help you behave better in the future and be more aware of threats. When we talk about the value of mobile phones, people's first reaction may be to ask how much I paid for my mobile phone. An interesting phenomenon: if I could give you the same price you paid for your phone plus $200, would you give me your phone? I think most people would say no, because the loss of photos, contacts, and apps on your phone, even if you could import them again, would be a lot more cumbersome than $200. So in this case, I'm going to call that $200 your phone's hidden assets. In fact, the hidden assets of your phone are much more than $200. Criminals can use your information or your confidential data to cause much more damage. Depending on the user, the potential damage is much higher than imagined.

Here we will identify the mobile asset analysis of general users, enterprise users, and government users, who share common hidden assets and become more valuable or more confidential depending on their identity and position. At the same time, explore the hidden assets stolen after the possible loss:

- Personal data: There will be personal data in some software or notepad, including all personal information like name, address, date of birth, and social security number. After such data is stolen, it may be sold through telecommunications fraud or phishing. If attacked, it is usually the user who suffers directly.
- Photos and videos: For general users, mainly life photos, which have commemorative value. For enterprise users, photos contain images of work sites, record project progress, or record important meetings, which have commercial value. For government users, it may contain state secrets, strategic information, intelligence collection, and decision-making that is very important to national or institutional interests.
- Contacts: Contacts can be said to be a very important asset on your phone. Contacts include the user's friends, family, colleagues, and other important people to keep in touch with. Specific information includes personal information such as names, phone numbers, email addresses, and social media profiles. Criminals can use contact information for fraud, spear phishing attacks, and whale phishing attacks against enterprise or government users. These technical terms for attacks will be explained in detail later.
- Banking and payment applications: Mobile phones are increasingly used for mobile banking and payment services. There may be two or more mobile banking or payment applications on each user's mobile phone for usual transfer and payment servicesmore mobile banking or payment applications on each user's mobile phone for usual transfer and payment services. General users, enterprise users, and government users are not distinguished here. What we need to understand here is that if there are multiple banks or payment software in your mobile phone and the amount in it is large, you need to pay more attention to the security of your mobile phone.
- Various information: This refers to various historical information contained in mobile phones, usually containing commemorative and historical value. Specific content includes text messages, social media apps, personal notes, passwords, memos, and more. Criminals may not try to find confidential and valuable information from the mass text messages and memos of general users, but for enterprise users and government users, if criminals launch targeted attacks, your various information may also become the source of criminals causing losses to you.

In this section, we will not discuss too much about attack methods and how criminals use these hidden assets. The purpose is to let non-technical users or users who had no such awareness before think about it after reading this part and identify the assets in their mo-

bile phones so that they can pay more attention to mobile phone security and protect their mobile phone assets.

Unsafe mobile phone use behavior

Now we have realized how important the intangible assets in our mobile phones are. Successful cyberattacks usually require finding vulnerabilities. It also includes people's unsafe behavior. According to the study from IBM, human error is responsible for the success of 95% of cyberattacks involving data breaches. In other words, mobile phone manufacturers and software security measures have done a good job. They help users eliminate most of the cyber threats, and if human error can be eliminated, the vast majority of cyber attacks will not be successful (Ahola, 2022).

causes of human error

So what is human error in mobile phone security? The definition of human error is the intentional or unintentional unsafe behavior of the user that leads to the spread or occurrence of harm (Ahola, 2022). For technical users and non-technical users, they have the same unsafe mobile phone behaviors, but the sources of unsafe behaviors are different.

For non-technical users, most of the causes are unintentional behaviors. Due to their lack of professional knowledge or understanding of network security, they may go to phishing websites and click on unknown links because they do not know about this behavior. May be harmful.

For users with a certain computer foundation, they know which behaviors may bring risks, but they still perform unsafe operations. What drives their behavior is more of a related psychological concept: optimism bias and risk-taking. Risky behavior usually refers to taking a risk to obtain some benefit; for example, the risk of jaywalking is the risk of a car accident, but the benefit is less walking. The risk of not adhering to security policies is cyber-attack; the benefit is that no extra work is done (Moustafa et al., 2021). As a result, many technology users do not strictly adhere to complex cybersecurity practices, preferring to risk convenience. Another psychological concept is optimism bias. People often think that the best things will happen to them (Moustafa et al., 2021). They also think that it is difficult for them to be affected by risks, which usually happen to others (Grobler et al., 2021). That is, humans tend to be optimistic and underestimate the likelihood of negative events happening to them (Moustafa et al., 2021).

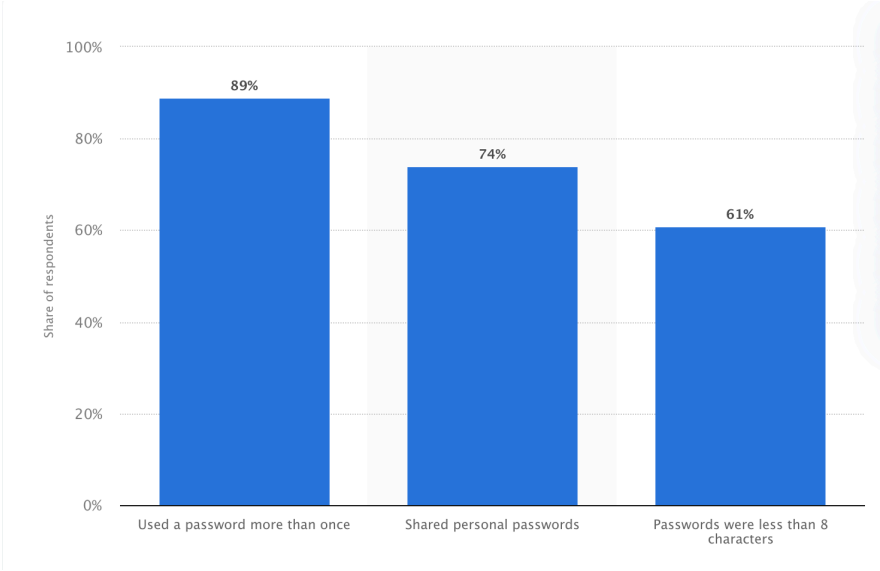
Therefore, even users who are proficient in computers have unsafe use behaviors, while non-technical users have more frequent unsafe behaviors due to a lack of understanding. Therefore, after analyzing the subjective causes of user behavior vulnerabilities, we will identify some vulnerabilities so as to better help non-technical users understand the irregular behaviors at ordinary times, help technical users supplement their computer knowledge, and help to better protect their mobile phone security in the future.

Password problem

First of all, the user's unsafe behavior is reflected in the setting of the password. Most of the time, passwords are used as the first and last line of defense to protect your privacy, but many users mistakenly think that just setting a password will protect their data well. But that’s not the case, with 1 million passwords being stolen every week, according to 2019 breach alerts. 81% of breaches are caused by weak, stolen, or reused passwords (Devon, 2021). Generally, insecure behavior regarding passwords is divided into three parts.

- The first is a weak password. A weak password is one that is too simple, such as having only numbers or a simple combination of numbers and letters. One of the characteristics of weak passwords is that they are easy to guess, i.e., common passwords such as ABC12345. These common passwords are added to the "dictionary". When hackers attack passwords, they usually try to import common passwords into the dictionary.
- The second is using the same password. Many users use the same password across many accounts for easy memory and operation. If hackers crack your password, their usual second step is credential stuffing. Credential stuffing means that after a hacker obtains a password, he then continues to log in to other accounts with the password until a match is found.
- The third is to easily tell others the password. This is mainly for elderly users. Because they are easy to trust others and do not understand current technology, for example, they are afraid of forgetting the password and do not know how to retrieve it, so they usually put the password in an obvious place. location or tell people outside your family.

Common password practices among hacking victims in the United States in 2021



Click unknown link

Links, also known as hyperlinks, are usually a medium for jumping to videos, pictures, websites, apps, etc., which exist in various forms in emails, web pages, apps, and SMS. Common forms of links include text links, URL links, and image links, which means that whenever you click on more than one form of link, you will be directed to the destination the designer wants you to reach.

Links are also classified by destination as normal hyperlinks, jumping to a specific web page; download links, which start downloading the target file or application; and email links, which are used to link to an email. So when a user clicks on an unknown link, especially if we don't know where the link goes, there is a possibility that risks may occur. Risks include:

- Directed to phishing websites, guided to steal personal information, or a fake payment interface to steal bank account information
- Download malicious software, which may steal all kinds of private information from users' mobile phones.
- May result in unnecessary charges on users' mobile bills, such as paying for SMS services via subscription.

People have too much faith in the security of the Internet, believing that links simply take them somewhere else to read something. And the psychology that drives this behavior, in addition to the optimism bias and risk-taking that we talked about earlier, also includes curiosity. In one study, FAU researchers investigated user behavior when unknown messages are received online. About 1,700 FAU students were sent emails or Facebook messages containing phishing links, and 45 percent and 25 percent, respectively, clicked on the links. "When asked why they clicked on the link, the vast majority of participants said it was out of curiosity about the content of the photo or the identity of the sender," said Zinaida Benenson, who led the study.

Connect to public Wi-Fi
Many users connect to unsecured wifi hotspots in public places such as airports, coffee shops, hotels, or plazas. Although this approach has been shown to have certain risks, in today's busy world, convenience seems to outweigh consequences, especially in the way people use mobile devices (Luke Bencie, 2017). There was an interesting experiment conducted at the 2016 Republican and Democratic National Conventions, where private entities offered visitors free public Wi-Fi for social science purposes at every convention, and it turned out that about 70 percent of people were connected to unsecured Wi-Fi networks.

So most of the time, even if people have a mobile data network, they still connect to unknown wifi for convenience. But this is indeed unsafe behavior. On the surface, it is just connecting and using this wifi for network operations. In fact, about $50 can buy the tools needed to crack the data transmitted by the wireless network, as well as decrypt and view the data on networked devices (Uy, 2022). In addition, there are various other Wi-Fi-based attacks, such as man-in-the-middle, twinning, combining phishing websites, etc. These attacks can be launched after users connect to unknown public WiFi.

Jailbreaking
The iOS operating system has a lot of features:
- **Safe boot**: Apple uses a technique called "safe boot" to ensure that the operating system and firmware on its devices have not been tampered with. This includes verifying the digital signature of each component during boot.
- **Sandbox**: Apple uses a technique called "sandboxing" to isolate apps from each other, with each app having its own "sandbox" to run in, which limits its access to system resources and other apps.
- **Encryption**: all data stored on the device by default is encrypted.
- **Two-factor authentication**: Apple provides two-factor authentication to help prevent unauthorized access to user accounts. For example, if a user logs in to an app account on a new Macbook or iPhone, he or she needs to obtain the verification code and click consent on the mobile phone or laptop that has logged in to the app account.

This behavior mainly exists in the younger generation of users because Apple's built-in security settings lead to certain restrictions on the use of download control and other files

and functions, but this restriction is definitely beneficial and protects user safety to a very large extent. To put it simply, jailbreaking is to increase the user's control over their mobile phone and reduce their requirements for external software, websites, and security certificate audits.

Some users choose to jailbreak in order to pursue more flexible use. Jailbreak may be able to install third-party applications, switch operators, and have more flexible functions, such as beautiful wallpapers. But what we need to know are the risks that come with it:

- **Download malware**: Apple will review all programs and games in the App Store. After jailbreaking, software from other markets does not have the same strict review as that from the Apple Store. We don't know which apps are genuine right now, and we can't tell the difference between cleverly disguised adware and other types of malware under the same icon. Worst of all, jailbreaking opens up the root directory of the operating system, and when attacked through malware or other means, control of the phone may have been handed over to a stranger (Cruz & Turner, 2023).
- **No more downloads of system updates or patch updates**: Once a user jailbreaks their phone or tablet, they forgo access to any future OS updates. Whenever Apple improves its security or Android responds to some new digital threats, jailbroken users are excluded (Cruz & Turner, 2023).
- **Compromise the integrity of the phone**: Jailbreaking has the potential to introduce certain misconfigurations that can lead to a whole new set of problems. For example, some built-in programs cannot run normally, some files cannot be parsed, and so on. Comparing the configuration of an Apple mobile phone to a beautiful house, jailbreaking is like forcibly remodeling the structure of the house. If the user forcibly remodels the structure, it will inevitably affect other places and cause new problems.

Behavior in a bad state

Many times, people are prone to making wrong behaviors or decisions in a bad state, but they usually mistakenly think that they can make right decisions as usual. Mental bad states include decision fatigue, multitasking, and a bad mood (Frick et al., 2019). Decision-making fatigue refers to the fact that after a day of fatigue, the accuracy of decision-making decreases due to fatigue. Multitasking refers to a state of distraction caused by juggling too much work at once. Dysmoods are extremes of emotion that cause us to lose our minds, such as during peak moments of anger and joy, and can hinder our ability to make good decisions (Frick et al., 2019). As for the physical state, it includes fatigue, illness, drunkenness, and so on. The losses caused by these bad behaviors can also occur in mobile security, such as transferring the wrong account when tired or drunk and losing the ability to judge malware and phishing software. Therefore, if users are in a bad state of mind or body, they need to reduce the number of decisions about mobile assets or not make important decisions, which can help reduce the losses caused by human errors and better protect our mobile security.

Finally, regarding this section, the mobile behaviors that lead to people's unsafe behavior can be roughly divided into two groups. The first group is unconscious behavior without understanding mobile security, and the second group has a certain knowledge of mobile security but still performs unsafe behavior. For the second group of people, the main psychological factors involved are optimism bias, risk-taking behavior for convenience, curiosity, excessive trust in others, and the safety of the Internet.

For mobile devices, the harm is digital, unpredictable, and immeasurable (Bencie, 2017). Every time an unsafe mobile phone behavior is like throwing a dart, it is only a matter of

time before the dart is thrown in the middle, and according to the current mobile phone security status, even if it is thrown within the 9th or 8th ring, it will suffer losses.

Identify common mobile attacks

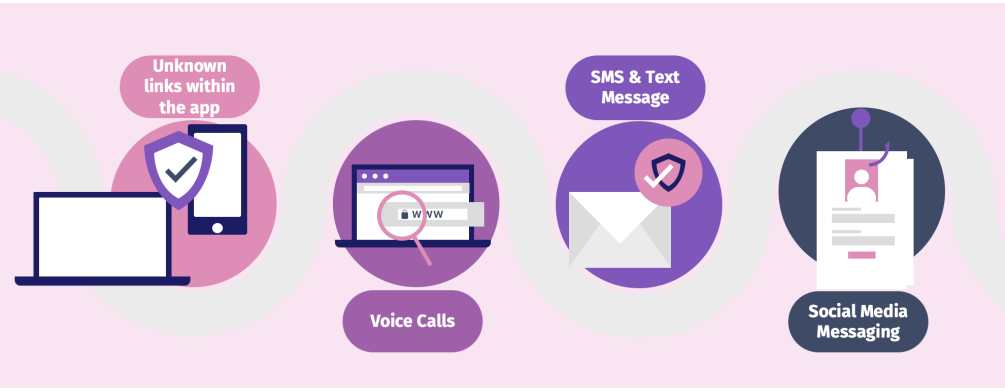
The previous section covered some common vulnerabilities in mobile user behavior, but this section explores some common mobile attacks. As mentioned above, most mobile attacks simply involve the discovery of vulnerabilities and then targeting the vulnerabilities to cause losses to users. Vulnerabilities include behavioral vulnerabilities of users, such as clicking on unidentified links and connecting to public Wi-Fi, as well as technical vulnerabilities of mobile phones, such as software backdoors and unqualified penetration reviews.

Behavioral vulnerabilities can be avoided after users receive education or understand relevant knowledge, but mobile technology vulnerabilities seem to be impossible for ordinary users to defend against in real time and can only rely on the technology of mobile phone manufacturers or mobile application security personnel. But fortunately, while we cannot technically defend in real time, we can understand the relevant response or preventive measures. The purpose of this section is to give all mobile users a better understanding of how mobile attacks combine with user behavior described in the previous section and how to prevent and respond to the technical aspects of mobile attacks to minimize or avoid losses.

Mobile phishing attack

Let's start with one of the most destructive attacks today: phishing attacks. A phishing attack is an attempt to steal medical privacy, account passwords, personal money, or other important data. Attackers pose as reputable sources to trick victims into filling out forms or downloading malware. Traditional phishing attacks are based on computers, in which the attacker usually sends an email and puts a text link or picture link inside a Web page, and then directs the victim to the phishing site. However, nowadays, hackers are more likely to develop phishing attacks on mobile devices because people spend more time on mobile phones than ever before and still use mobile phones to surf the Internet even if they can use computers (Eperjesi, 2023). Mobile phishing attacks have become more diverse than traditional attacks. The following section will identify mobile phishing attacks:

The main channels of phishing attacks on mobile terminals include advertisements and image links in applications, phone scams, text messages containing phishing links and false information, and a large number of phishing messages, links, and malware posted on social media applications.



The attack process is usually combined with social engineering. Phishing attacks need to mobilize users' extreme emotions to reduce their thinking time. The more time they spend thinking, the less they believe in the authenticity of phishing attacks. For example, some text messages tell users that they have won the prize or that their family members are out in an accident. People are extremely excited or worried, and they will click the link without hesitation or send money directly to the criminals.

Meanwhile, a new method of phishing, called ‘positive’ phishing, has recently emerged (Katz, N.A.). The attacker combined the game and question quiz to carry out phishing, and the user could win prizes by playing the game or answering the questions. However, this is the most attractive way to conduct phishing attacks. No matter what the answer is or what the result of the game is, the prize will be obtained. Phishing attacks also increase trust by offering rewards from well-known brands, such as a phone from a well-known brand or a ticket from a well-known airline.

Another common follow-up practice is that after the victim wins the prize, the prompt is required to share with friends or groups within a limited time to get the prize. Through this method, the phishing attack has a larger scope and more victims.

In the end, although the decoys used in mobile phishing vary, what really hurts users is giving out personal information, downloading malware, and transferring money directly.

Password attack

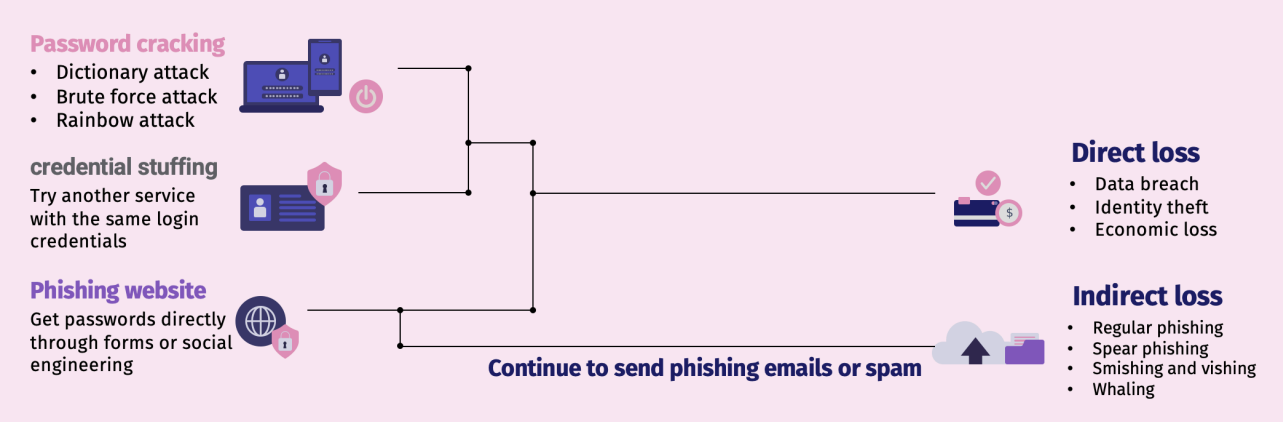
A password attack is an attack on a user's login credentials. Unlike phishing software, a password attack is designed to crack the account and password of an app or website and then steal personal information and money. First of all, hackers obtain the user username through a variety of ways, such as website data leakage. Many users will be affected by this due to temporary needs in some small website registered accounts. When these websites lose maintenance, it is very likely that data leakage will occur because users often use the same account name and password on multiple platforms. So the hacker uses the same username and password to try another site or service. Also, there are social engineering, phishing attacks, guesses, or enumerations to get the user's username.

After the attackers obtained the user's username, they began the attack on the user's password. Some attackers who are familiar with the victim may begin to guess from aspects of the victim's life, such as name, birthday, pet, color, etc., which can be obtained from social media, direct interactions, and deceptive conversations (Miller, 2022). But random password guesses have a low success rate, and for most users, hackers use automated cracking tools and different built-in methods to attack passwords.

- **Dictionary attack**: If the threat actor knows the password length and complexity requirements of the target account, the dictionary can be customized according to the target. In dictionary attacks, the length, character requirements, and word combinations can be customized. More advanced dictionaries include lists of the most commonly used words in passwords. This is a relatively simple method that can be used effectively to guess passwords that are not too complicated.
- **Brute-force attack**: In this way, attackers use tools to try and repeat every possible combination of letters, numbers, and symbols until the password is cracked. A similar method is a reverse brute force attack, in which hackers try a single password for

multiple usernames. But if the password is complex enough, the attack could take more than 30 years.

- **Rainbow table attack**: In a rainbow table attack, the attacker constantly searches for the plaintext password through the tool and rainbow table when the hash value of the password is known.
- **Credential stuffing**: If the password is weak, the attackers may have cracked the user's password after these attacks. The next step is credential stuffing, which essentially uses an automated tool to log in to other services with the same account number and password.
- **Password spraying**: This is an attack similar to credential padding, where hacker use one set of usernames and passwords to continue trying other services. and password spraying is attackers use some common passwords to access multiple usernames.



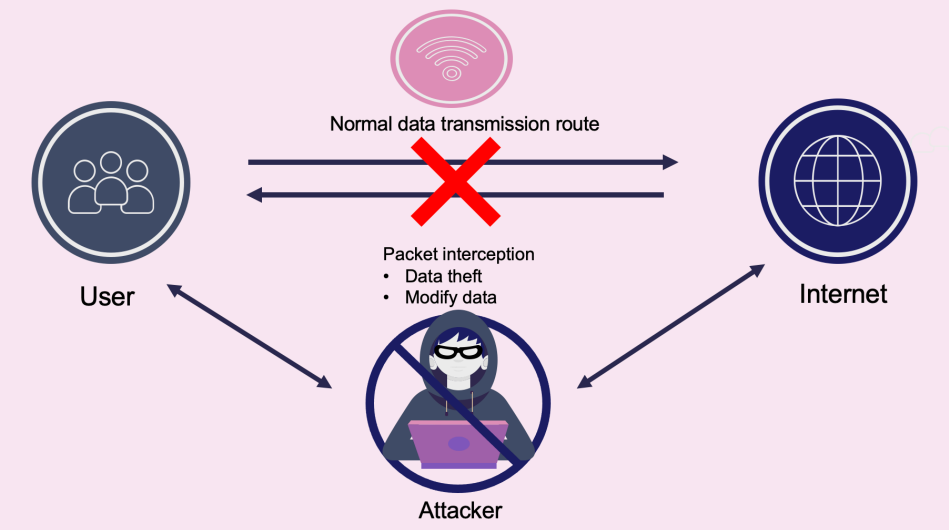
Finally, the countermeasures of security personnel against password attacks include locking the account if the incorrect password is entered too many times, but the subsequent problem is that the attacker may deliberately enter the wrong password, resulting in a large number of accounts locked, affecting the website's operation and user use. Locking accounts at the same time does not work against attempts to use the same password for different usernames (Esheridan, N.A.). The response also involves blocking IP addresses, but attackers have new technology, also known as IP pooling, that allows a computer to switch IP addresses. At present, the most effective defense method is to increase the verification code and the reaction time of the authentication password. As a user, using two-factor authentication and a strong password can prevent most password attacks.

Wi-Fi attack

Many users love free Wi-Fi at airports, coffee shops, or shopping malls, but we need to think about why it's free and who provides it. Of course, some are provided by shopkeepers or public institutions, but many of them are set up by criminals, and any mobile device connected to Wi-Fi without proper security can be hacked. So it's not just the hotspot that's public; it's also the user's data.

A man-in-the-middle (MITM) attack is a Wi-Fi network attack in which the attacker intercepts the transmitted data between the sender and the destination. Because the data transmitted over public Wi-Fi is not encrypted, the attacker can directly see the transmitted plaintext data (Karaymeh, 2019). A man-in-the-middle attack involves a replay attack, in which the attacker monitors the messages sent between the sender and the receiver, gets the data, modifies the packet, and then proceeds to the destination so that the destination does what the attacker sent.

In order to deceive users with a certain awareness of prevention, attackers use the Wi-Fi with the same name as the store Wi-Fi or the Wi-Fi with the name of the official facility. This attack is called "the evil twin'.



Malware and ransomware
Malware is also a common mobile attack in which attackers create malicious scripts or malicious programs that are often built into seemingly normal applications but, once installed, begin stealing data, advertising, and money without the user's consent. And the theft of contacts makes the attack a problem not just for the victim but potentially for everyone the victim knows.

Ransomware is also a type of malware. Ransomware is a popular Trojan that usually exists in third-party applications. For example, some of the targeted users downloaded it via phishing links, fake antivirus software, and links to porn browsers, and then their phones were encrypted within minutes, rendering them unusable. And some ransomware that can gain access to photos and contacts. One example would be to send all of the victim's private photos to all of the victim's contacts if the victim doesn't send money to the attacker. At the same time, the attacker uses the psychology of the victim to set a time limit for payment, and the amount of ransom will increase over time. But the price they charge is sometimes very high, and unfortunately, sometimes even the ransom payment does not always lead to the recovery of the phone and the data. So the best way is to back up important data and have it repaired by a mobile security professional.

In addition to these common attacks, there are many more targeted attack forms and technologies, but for ordinary users, these are no longer what we need to consider; these technical levels of defense require more mobile phone manufacturers, web developers, and application technology-related security personnel to solve and defend. The best defense that ordinary users can do is to avoid the dangerous behaviors that can be avoided and minimize the ways that criminals can attack us.

User safety guide

According to the assets, vulnerabilities, and attacks in the article, users can have a good understanding of the importance of mobile phone security, unsafe mobile phone behaviors, and possible threats. The following chart integrates and complements all the parts mentioned above, aiming to give mobile users a more intuitive understanding of mobile security and give them guidance on mobile security.

Asset

The mobile asset table identifies the assets on the user's phone, and the assets also come in different forms, mainly in the form of data, apps, memos, and in-app money. At the same time, for different types of users, such as general users, enterprise users, and government users, the same asset has different importance to them. As mentioned in the first part of asset identification, enterprise users and government users have private data related to enterprise or government on their mobile phones. Each asset has a corresponding description and number, which plays an associated role with the following tables.

#	assert	owner/steward	type	description	assert importance(low,medium,critical)
A1	Personal data	All users	data	This includes all personal information like name, address, date of birth, and social security number	critical
A2	Contacts	All users	data	Contacts include the user's friends, family, colleagues, and other important people to keep in touch with	critical
A3	Bank and payment application	All users	app	Mobile banking and payment services for money transfers as well as routine payments	critical
A4	Social media application	All users	app	Include account passwords, login details, profiles and chat history	medium
A5	Personal notes	All users	memo	Users use their phones to jot down notes, memos, and to-do lists about their personal lives	low
A6	Photos and videos	general users enterprise users government users	data	Photos and videos of the user's life or work	low critical critical
A7	Confidential documents	enterprise users government users	data	About company or government secrets, such as strategic plans, organizational decisions, financial statements	critical critical
A8	Historical record	general users enterprise users government users	data	This includes text messages, emails, and web browsing history.	low medium critical

vulnerability

The vulnerability table identifies the unsafe movement behaviors of users and classifies and supplements the unsafe behaviors of users mentioned above. possible losses analyzes the mobile phone assets that may be involved in each unsafe behavior and corresponds to the assets in the asset table, enabling users to know the possible consequences of unsafe behavior and describing the content of each unsafe behavior.

#	Unsafe Behavior	Possible losses	Description
V1	Insecure password	A3,A4	Set a weak password, set the same password for different accounts, and share your password with others
V2	Click unknown link	A1,A3,A4,A7	Click on a link in an email, text or social media app and fill in your personal information
V3	Download insecure applications	ALL Assets	Download an app from a third party store or from an unknown link and give the app too many permissions
V4	Connect public wifi	A1,A6,A7,A8	Use public Wi-Fi without VPN, transfer data and private information after connecting to public Wi-Fi
V5	Jailbreaking	ALL Assets	Jailbreak the phone and disable the built-in security Settings
V6	Behavior in bad state	A1,A3,A4	Decisions made under decision fatigue, multitasking, dysmoods, fatigue, illness, and drunk
V7	Giving too many permissions to unknown applications	A1,A2,A6	Allow apps to access unnecessary data, such as giving game apps access to geolocation, photos, contacts
V8	Let strangers operate your phone	ALL Assets	Strangers may use your phone to access third-party payment platforms or install spyware
V9	Scan unsafe QR code	ALL Assets	QR code attacks include redirecting to phishing websites, downloading malware, stealing customer data, and gaining access to users' applications

Risk

The risk table lists common mobile attacks and analyzes the attack routes and how to exploit the user's insecure behavior. The probability of each attack occurring and a brief description of the attack are also listed. At the same time, the control measures or preventive measures for each attack are given, and the danger level of each attack is divided.

#	Attack	router	likehood	description	controls	risk level
R1	Blowing up one' s phone	N/A	low	continuously sending spam text messages and phone calls to a certain mobile phone number	Automatically intercepts unstored numbers	low
R2	Bluetooth Attacks	V4	low	unauthorized access to devices, interception of data, or malicious action	Turn off Bluetooth when not in use, do not connect to unknown devices	Medium
R3	Wi-Fi attack	V4	Medium	steal user data, modify user operations	Do not connect to unknown Wi-Fi, connect to Wi-Fi to ensure that the name is correct	Medium
R4	Password attack	V1	High	steal user accounts and passwords and perform malicious operations	Strong passwords, and enable two-factor authentication	High
R5	Phishing attack	V2,V9	High	steal private information, download and execute malicious software	Do not click on unidentified links sent by anyone unless you are sure it is perfectly safe	High
R6	Spyware	V3,V5,V7,V9	Medium	uses software to monitor a phone's internal data, such as contacts, text messages and emails	Antivirus scanning software, ask professional mobile security personnel	High
R7	Ransomware	V3,V5,V7,V9	Medium	encrypts files and directories, freezes users' phones, and will demand payment to unlock phones	Do not download unknown apps and ask mobile security professionals	High

Safety suggestion

In order to help non-technical users better ensure the security of mobile phones, this table is made by combining common attacks, including technical attacks, psychological attacks, and real-life physical attacks. According to different security controls, different protection areas are divided, such as Wi-Fi security behavior, passwords, and applications. Finally, each security behavior is described so that users can better ensure the security of mobile devices after understanding the security table.

#	Type	Guide
C1	Wi-Fi	Periodically check the Wi-Fi status: an unfamiliar device or IP address, the Wi-Fi password has been changed, and the network speed is slow
C2	Wi-Fi	Do not use public Wi-Fi to shop online, log into your financial institution, or visit other sensitive websites
C3	Wi-Fi	Turn off Wi-Fi and Bluetooth when not in use
C4	Wi-Fi	Connecting to Wi-Fi is to make sure the name is correct
C5	Password	Avoid simple passwords and the same password for multiple important accounts
C6	Password	Enable two-factor authentication
C7	Unknown source	When filling in personal information or account password, make sure it is on the correct website and in a safe situation
C8	Unknown source	Don't scan QR codes of unknown origin
C9	Unknown source	Do not click on unidentified links of any kind
C10	App	Don't give apps unnecessary permissions (photos, cameras, contacts)
C11	App	Don't download apps from unknown sources
C12	App	Don't jailbreak your phone system
C13	physical	Back up important data
C14	physical	Don't let strangers operate your phone

Conclusion

This paper analyzes the current mobile security situation from the perspectives of user psychology, user behavior, and criminal psychology and behavior, with the aim of better protecting our mobile devices and data in the current digital age. With the development of the times, mobile devices and data will To become more diversified, there may be more forms of assets and data. Of course, there will be more different methods of mobile attacks. Finally, I hope that users can pay more attention to mobile security now and in the future and that security professionals can better improve mobile security. This requires the cooperation and collaboration of mobile phone manufacturers, data security personnel, policies, laws, and every mobile phone user.

Reference:

Nelson, B. (2023, April 13). *Top security threats of smartphones (2022)*. Reader's Digest. Retrieved April 22, 2023, from https://www.rd.com/article/mobile-security-threats/

Turner, A. (2023, April 2). *3.12 billion more phones than people in the world!* BankMyCell. Retrieved April 22, 2023, from https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Why human error is #1 cyber security threat to businesses in 2021. The Hacker News. (2021, February 4). Retrieved April 24, 2023, from https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html#:~:text='Human%20error%20was%20a%20major,in%2095%25%20of%20all%20breaches.&text=Mitigation%20of%20human%20error%20must,cyber%20business%20security%20in%202021.

Ahola, M. (2022, June 17). *The role of human error in successful cyber security breaches*. usecure Blog. Retrieved April 24, 2023, from https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Moustafa, A. A., Bello, A., & Maurushat, A. (2021, May 3). *The role of user behaviour in improving cyber security management*. Frontiers. Retrieved April 24, 2023, from https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full

Grobler, M., Gaire, R., & Nepal, S. (2021, January 20). *User, usage and usability: Redefining Human Centric Cyber Security*. Frontiers. Retrieved April 25, 2023, from https://www.frontiersin.org/articles/10.3389/fdata.2021.583723/full

Devon. (2021, January 26). *How much one bad password can cost you*. Cybint. Retrieved April 29, 2023, from https://www.cybintsolutions.com/how-much-one-bad-password-can-cost-you/

Stefan Lueders and The Computer Security Team. (2018, March 2). *Computer security: Curiosity clicks the link*. CERN Document Server. Retrieved April 30, 2023, from https://cds.cern.ch/record/2306520

Bneson, Z. (n.d.). *Black Hat USA 2016*. Black Hat USA 2016 | Briefings. Retrieved April 30, 2023, from https://www.blackhat.com/us-16/briefings.html#exploiting-curiosity-and-context-how-to-make-people-click-on-a-dangerous-link-despite-their-security-awareness

Bencie, L. (2017). Why you really need to stop using public Wi-Fi. *Harvard Business Review*.

Uy, M. (2022, March 25). *Safety issues when connecting to and using an open wireless network*. Lifewire. Retrieved May 1, 2023, from https://www.lifewire.com/is-it-safe-to-use-an-open-wireless-network-2378210

Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. Mobile Information Systems, 2020, 1-15.

Cruz, B., & Turner, G. (2023, February 8). *Should you jailbreak your iphone?* Security.org. Retrieved May 2, 2023, from https://www.security.org/digital-safety/jailbreak-smartphone/

Frick, W., Maxfield, D., & Carucci, R. (2019, September 11). *6 reasons we make bad decisions, and what to do about them*. Harvard Business Review. Retrieved May 5, 2023, from https://hbr.org/2019/08/6-reasons-we-make-bad-decisions-and-what-to-do-about-them

Nylander, S., Lundquist, T., & Brännström, A. (2009, April). At home and with computer access: why and where people use cell phones to access the internet. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 1639-1642).

Eperjesi, A. (2023, February 8). *The rise of mobile phishing and how to handle it*. Swimlane. Retrieved May 6, 2023, from https://swimlane.com/blog/mobile-phishing/

Katz, O. (Ed.). (n.d.). *Research paper | A new era in phishing* . Retrieved May 7, 2023, from https://www.hmtaxes.com/sites/default/files/content/a-new-era-in-phishing-research-paper.pdf

Esheridan. (n.d.). *Blocking brute force attacks*. Blocking Brute Force Attacks | OWASP Foundation. Retrieved May 7, 2023, from https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security*, *6*(03), 206.

Karaymeh, A., Ababneh, M., Qasaimeh, M., & Al-Fayoumi, M. (2019, October). Enhancing data protection provided by VPN connections over open WiFi networks. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-6). IEEE.

Li, Q., & Clark, G. (2013). Mobile security: a look ahead. IEEE Security & Privacy, 11(1), 78-81.