PROJECT REPORT
ON
"CYBER CRIME AND LAWS"

Project work submitted as partial fulfillment of the course for the Award of the degree

BACHELOR OF COMPUTER APPLICATION
OF
BANGALORE UNIVERSITY

SUBMITTED BY

JAY BRATA MANDAL : U03AB21S0014

Under the Guidance Of

(CHARAN)

AVK DEGREE COLLEGE 27th Cross Rd, Banashankari Stage
II, Banashankari, Bengaluru, Karnataka 560070

Mobile security is a constant issue among many enterprises. As companies continue to go digital and offer online and mobile platforms to their consumers, the rate of mobile security threats multiplies by the day.

Having a mobile application is another means of ensuring that the product and services your company offers are readily available for your customers to consume. Connectivity, accessibility, and convenience are among the many factor’s entrepreneurs must prioritize to deliver to establish a good relationship with their market.

However, if you fail to properly secure your mobile application and your company, the risk of having sensitive and vital information compromised will significantly damage your reputation and trust in your brand among consumers.

To help you avoid this, we prepare a comprehensive and in-depth checklist of ways to ensure the utmost security for your mobile application and reduce the probability of encountering external cyber threats penetrating your application.

INDEX

Prepare checklist for configuring security settings in mobile wallet and VIP

Mobile Wallet Security Checklist:

Enable Biometric Authentication:

- ❖ Set up fingerprint or facial recognition authentication for accessing the mobile wallet. Strong Password/PIN:

- ❖ Create a strong and unique password or PIN for the mobile wallet.
- ❖ Avoid using easily guessable information, such as birthdays or common patterns.
- ❖ Two-Factor Authentication (2FA):

- ❖ Enable two-factor authentication for an extra layer of security.
- ❖ Use authentication methods such as SMS codes, app-based authenticators, or biometric verification.

Device Lock Settings:

- ❖ Set a device lock (screen lock) with a password, PIN, or biometric authentication.
- ❖ Configure the device to automatically lock after a short period of inactivity.

Update and Patch Mobile Apps:

- Ensure the mobile wallet app is up-to-date with the latest security patches.
- Regularly update the mobile device's operating system.
- Secure Network Connections:

- Avoid using public Wi-Fi networks for sensitive transactions.
- Use a virtual private network (VPN) when connecting to public Wi-Fi.
- Review App Permissions:

- Review and manage the permissions granted to the mobile wallet app.
- Disable unnecessary permissions that may compromise security.
- Monitor Account Activity:

- Regularly review transaction history and account activity for any unauthorized transactions.
- Set up account notifications for transactions or account changes.
- Logout from Sessions:

- Manually log out from the mobile wallet app when not in use.
- Enable automatic logout after a certain period of inactivity.

VIP Account Security Checklist:

Unique Username and Password:

- Choose a unique and strong username for the VIP account.
- Set a strong and complex password that includes a mix of letters, numbers, and symbols.

Two-Factor Authentication (2FA):

- Enable 2FA for VIP account access.
- Use secure 2FA methods, such as hardware tokens or app-based authentication.

IP Whitelisting:

- Consider implementing IP whitelisting to restrict account access to specific IP addresses.
- Regular Password Updates:

- Set a policy for regular password updates and ensure that VIP account passwords are changed periodically.

Security Questions:

- Configure and regularly update security questions for additional account verification Security Audits:

- Conduct regular security audits on the VIP account to identify and address potential vulnerabilities.

Limit Access Permissions:

- Review and limit access permissions for users associated with the VIP account.
- Grant access only to essential personnel.

Education and Training:

- Provide security awareness training for individuals with access to the VIP account.
- Educate users on phishing and social engineering risks.

Monitoring and Alerts:

Implement real-time monitoring for suspicious activities on the VIP account.

Set up alerts for unauthorized access attempts or unusual account behavior.

Remember to adapt these checklists based on specific platform features, updates, and any additional security measures provided by the mobile wallet or VIP account service. Regularly review and update security settings to stay ahead of potential threats.

Case Study 1: "Biometric Authentication Breach"

Background:

A popular mobile wallet introduced biometric authentication for users to enhance security. Users were encouraged to use fingerprint recognition or facial ID for accessing their accounts.

Challenge:

Several users reported unauthorized transactions even though their biometric authentication was enabled. The mobile wallet's reputation was at stake.

Solution:

Conducted a thorough investigation into the reported breaches.

Identified a vulnerability in the biometric authentication system that allowed attackers to bypass security measures.

Released an emergency patch to fix the vulnerability and updated users on the importance of regular app updates.

Enhanced communication channels to alert users about suspicious activities and encouraged them to enable additional security features.

Outcome:

The swift response and remediation efforts restored user trust. The case highlighted the importance of regularly auditing and updating security features to adapt to emerging threats.

Case Study 2: "VIP Account Compromise"

Background:

A high-profile VIP account, managing sensitive information for a prominent individual, experienced a security breach resulting in unauthorized access.

Challenge:

Confidential data, including personal details and financial information, was compromised, leading to potential reputational damage and financial loss for the VIP.

Solution:

Engaged a cybersecurity firm to conduct a forensic analysis of the breach and identify the entry point.

Implemented immediate measures to secure the compromised account, including resetting passwords, disabling compromised credentials, and initiating 2FA for all users.

Collaborated with law enforcement to track down the perpetrators and take legal action.

Launched a comprehensive security awareness program for VIP account users and staff to prevent future breaches.

Outcome:

Although there was some reputational damage, the swift and comprehensive response helped in minimizing further risks and reinforcing the importance of robust security measures for VIP accounts.

Case Study 3: "Phishing Attack on Mobile Wallet Users"

Background:

Users of a popular mobile wallet started receiving phishing emails and messages, attempting to trick them into revealing their login credentials and other sensitive information.

Challenge:

Phishing attacks were causing financial losses and eroding user confidence in the mobile wallet's security measures.

Solution:

Issued immediate alerts and warnings to all users about the phishing attacks through the mobile app, website, and email.

Enhanced communication channels to educate users on identifying phishing attempts and provided guidance on secure communication.

Collaborated with cybersecurity experts to identify and take down phishing websites and malicious campaigns.

Implemented additional security features such as anti-phishing tools within the mobile app.

Outcome:

The awareness campaign reduced the success rate of phishing attempts, and the additional security measures helped in safeguarding users from further attacks. The case highlighted the importance of user education in the face of evolving cybersecurity threats.

These case studies illustrate the complexity of security challenges in the digital realm and emphasize the need for proactive measures to protect both mobile wallet users and VIP accounts.

The 3 case laws based on cyber crime

ATM Heist (2016):

In 2016, a cybercrime group targeted ATMs in India, exploiting vulnerabilities in the banking system to compromise debit card data. The attackers used malware to steal sensitive information, leading to unauthorized transactions and financial losses.

Yes, that's correct. The ATM Heist in 2016 was a significant cybercrime incident in India that targeted ATMs and led to unauthorized transactions and financial losses for individuals and banks. Here are some additional details about the incident:

In 2016, several banks in India reported a large-scale security breach related to their ATM networks. Cybercriminals had managed to compromise the systems and gain unauthorized access to sensitive financial information, including debit card data.

The attackers used a sophisticated malware strain to infect the systems controlling the ATMs. This malware allowed them to capture sensitive information, such as card numbers and PINs, from individuals using the compromised ATMs.

Once the cybercriminals had obtained the necessary information, they conducted unauthorized transactions, leading to financial losses for both the affected individuals and the banks. The incident highlighted the vulnerabilities in the banking system and raised concerns about the need for improved cybersecurity measures in the financial sector.

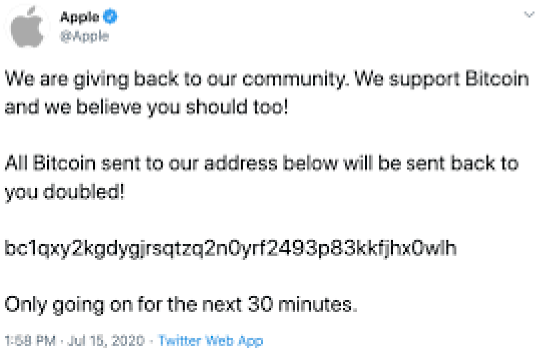
Banks took immediate steps to address the issue, including recalling compromised debit cards, enhancing security protocols, and implementing measures to prevent future cyber-attacks. The incident underscored the importance of robust cybersecurity practices, continuous monitoring, and prompt response to potential security threats in the financial industry.

It's worth noting that cybersecurity is an ongoing challenge, and financial institutions regularly invest in upgrading their security infrastructure to stay ahead of evolving cyber threats.

Twitter Bitcoin Scam (2020):

In July 2020, several high-profile Twitter accounts, including those of prominent personalities and companies, were hacked as part of a Bitcoin scam. The attackers posted tweets urging followers to send Bitcoin to a specified address, promising to send back double the amount.

Yes, that's correct. The Twitter Bitcoin scam in July 2020 was a high-profile incident where the accounts of various prominent individuals, including politicians, celebrities, and companies, were compromised. The attackers used the compromised accounts to post tweets promoting a cryptocurrency scam.



Apple
@Apple

We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for the next 30 minutes.

1:58 PM · Jul 15, 2020 · Twitter Web App

Here are some key details about the Twitter Bitcoin scam:

Scope of the Attack:

The attack targeted a wide range of high-profile Twitter accounts, including those of Barack Obama, Joe Biden, Elon Musk, Bill Gates, Apple, and many others.

The compromised accounts were used to post tweets containing a fraudulent message encouraging followers to send Bitcoin to a specific wallet address. The message falsely claimed that the sender would double the amount of Bitcoin received.

Bitcoin Scam Message:

The fraudulent tweets typically stated that due to the COVID-19 pandemic, the account owner was giving back to the community and would double any Bitcoin sent to the specified wallet address.

Impact:

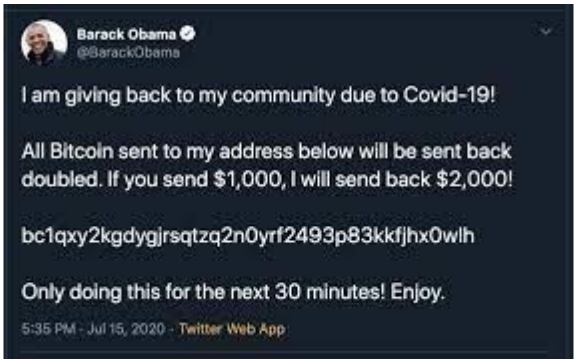
The scam tweets led to confusion among followers and raised concerns about the security of high-profile Twitter accounts.

Some individuals fell victim to the scam and sent Bitcoin to the specified addresses, expecting a return that, of course, never occurred

Response and Investigation:

Twitter quickly responded by taking down the compromised accounts and disabling the ability to tweet or reset passwords for a brief period.

The incident prompted an investigation by law enforcement agencies, and Twitter initiated a thorough review of its security measures to prevent similar incidents in the future.



Barack Obama
@BarackObama

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

5:35 PM · Jul 15, 2020 · Twitter Web App

Security Measures:

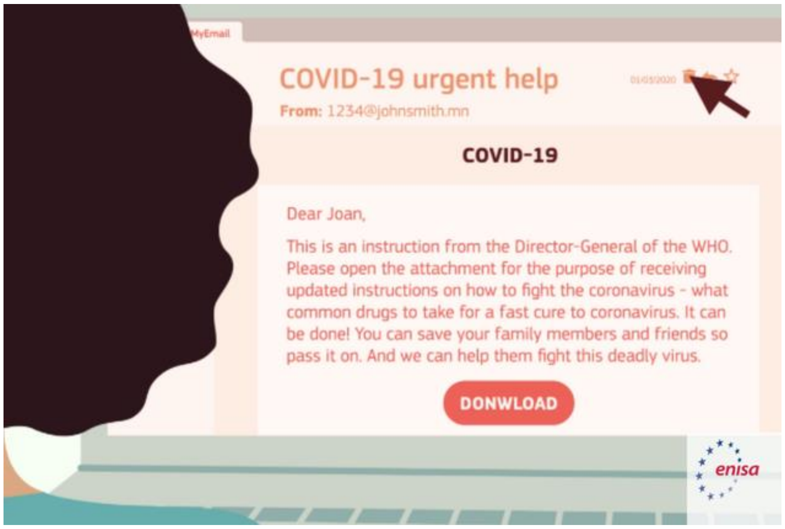
Following the incident, Twitter implemented additional security measures and controls to enhance the protection of high-profile accounts. This included measures to prevent unauthorized access and improve the platform's overall security posture.

The Twitter Bitcoin scam highlighted the vulnerabilities associated with high-profile social media accounts and the potential misuse of such platforms for financial scams. It also emphasized the importance of robust cybersecurity measures and user education to prevent falling victim to social engineering attacks and cryptocurrency scams.

Phishing Attacks During COVID-19 (2020):

With the onset of the COVID-19 pandemic, there was a surge in phishing attacks exploiting the health crisis. Cybercriminals used fake websites and emails related to COVID-19 to trick individuals into revealing personal information or downloading malicious content.

Absolutely correct. The COVID-19 pandemic presented a unique opportunity for cybercriminals to exploit the global health crisis for their malicious activities. Here are some key points about the phishing attacks during the COVID-19 pandemic in 2020



COVID-19 urgent help

From: 1234@johnsmith.mn

COVID-19

Dear Joan,

This is an instruction from the Director-General of the WHO. Please open the attachment for the purpose of receiving updated instructions on how to fight the coronavirus - what common drugs to take for a fast cure to coronavirus. It can be done! You can save your family members and friends so pass it on. And we can help them fight this deadly virus.

Exploiting Fear and Uncertainty:

Cybercriminals took advantage of the fear and uncertainty surrounding the pandemic to launch phishing attacks. They used the urgency of the situation to create scenarios that would prompt individuals to click on malicious links or provide sensitive information.

Fake Websites and Emails:

Phishing attacks often involved the creation of fake websites and emails that appeared to be from reputable health organizations, government agencies, or even healthcare providers.

The emails and websites typically contained false information about COVID-19, vaccine availability, or safety measures, aiming to trick individuals into taking action.

Themes of Phishing Attacks:

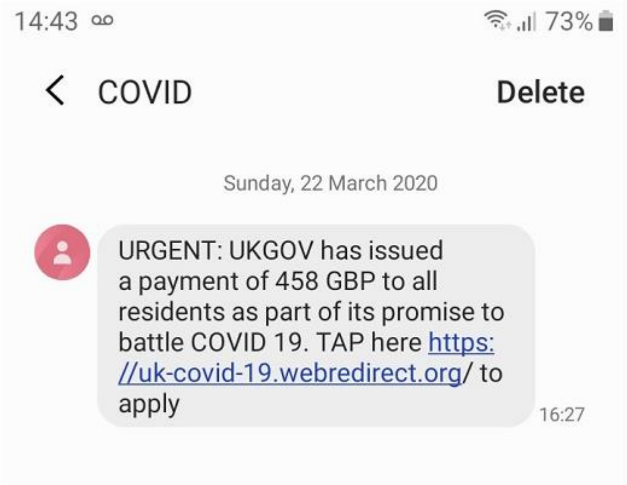
Common themes included fake COVID-19 testing or vaccine registration forms, financial aid applications, and health advice. These were designed to lure individuals into providing personal information, such as names, addresses, financial details, or login credentials.

Malicious Attachments and Downloads:

Some phishing emails included attachments or links claiming to provide important information about the pandemic. Clicking on these links or downloading attachments could lead to the installation of malware on the victim's device.

Targeting Remote Workers:

With the increase in remote work during the pandemic, cybercriminals also targeted individuals working from home. Phishing emails often posed as work-related communications, HR updates, or information about COVID-19 policies within organizations.



Sunday, 22 March 2020

URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply

16:27

Cybersecurity Awareness and Education:

The surge in COVID-19-related phishing attacks highlighted the importance of cybersecurity awareness and education. Individuals and organizations needed to be vigilant and verify the authenticity of emails and websites before clicking on links or providing sensitive information.

Government Warnings:

Governments and cybersecurity agencies worldwide issued warnings and advisories to educate the public about the increased risk of COVID-19-related phishing scams. They provided guidelines on how to identify and avoid falling victim to such attacks.

The phishing attacks during the COVID-19 pandemic underscored the adaptability of cybercriminals to capitalize on global events. It also emphasized the need for individuals and organizations to stay informed, exercise caution, and employ cybersecurity best practices to mitigate the risks associated with phishing and other cyber threats.

Reporting a redressal mechanism for misusing or violating social media.

1. Reporting Mechanism:

a. User-Friendly Reporting Interface:

Develop a user-friendly reporting interface within the social media platform accessible through both desktop and mobile applications.

b. Variety of Violations:

Provide specific reporting categories covering various types of violations, including harassment, hate speech, impersonation, misinformation, and other forms of abuse.

c. Anonymous Reporting:

Allow users to submit reports anonymously to encourage individuals who may fear retaliation to come forward.

d. Attach Evidence:

Enable users to attach evidence such as screenshots, links, or other relevant information to support their reports.

2. Review and Investigation:

a. Dedicated Team:

Establish a dedicated team responsible for reviewing and investigating reported cases promptly.

b. Transparency:

Maintain transparency in the review process by providing updates to the reporter regarding the status of their complaint.

c. Expertise:

Ensure the team possesses expertise in handling various types of violations, including legal considerations and cultural nuances.

d. Collaborate with Law Enforcement:

Collaborate with law enforcement agencies to address cases that involve criminal activities or pose serious threats.

3. Action and Redressal:

a. Graduated Responses:

Implement a system of graduated responses based on the severity of the violation. Responses may include warnings, temporary suspensions, or permanent bans.

b. Appeals Process:

Establish an appeal process for users to challenge decisions made by the review team. Ensure transparency in the appeals process.

c. Communication:

Communicate outcomes and actions taken to both the reporter and the alleged violator, maintaining privacy and security protocols.

d. Continuous Improvement:

Regularly review and update the redressal mechanism based on feedback, emerging trends, and changing online behaviors.

4. Public Awareness and Education:

a. Educational Campaigns:

Conduct educational campaigns to inform users about the reporting mechanism, the importance of responsible online behavior, and potential consequences for violations.

b. Resources and Support:

Provide resources and support for users who have experienced online harassment or abuse, including access to counseling services.

c. Collaboration with NGOs:

Collaborate with non-governmental organizations (NGOs) and advocacy groups to address broader issues related to online safety and digital literacy.

5. Legal Compliance:

a. Compliance with Local Laws:

Ensure that the redressal mechanism complies with local laws and regulations governing online content and user behavior.

b. Cooperation with Authorities:

Cooperate with relevant authorities to address legal issues and facilitate the investigation and prosecution of individuals involved in criminal activities.

Implementing a robust redressal mechanism requires a combination of technological tools, human intervention, and a commitment to fostering a safe and inclusive online community. Regularly evaluate the effectiveness of the mechanism and make necessary adjustments to address evolving challenges in the social media landscape.

6. Data Privacy and Protection:

a. User Consent:

Clearly communicate how user data will be handled within the reporting mechanism.

Obtain explicit consent from users before collecting and processing any personal information.

b. Encryption:

Implement end-to-end encryption for sensitive communications and data shared within the reporting process.

c. Data Retention Policies:

Establish clear and transparent data retention policies, specifying how long the platform will retain user reports and associated data.

d. Regular Audits:

Conduct regular audits of data protection practices to ensure compliance with privacy regulations.

7. Cultural Sensitivity and Diversity:

a. Diverse Review Team:

Ensure diversity within the review team to better understand and address cultural nuances and sensitivities in reported cases.

b. Multilingual Support:

Provide multilingual support for reporting, review, and communication processes to cater to a global user base.

c. Cultural Competency Training:

Offer cultural competency training to review team members to enhance understanding and sensitivity to diverse perspectives.

8. Collaboration with External Entities:

a. Collaboration with Cybersecurity Experts:

Collaborate with external cybersecurity experts to continuously assess and improve the platform's security infrastructure.

b. Collaboration with Research Institutions:

Partner with research institutions to stay updated on emerging trends in online behavior and potential risks associated with new technologies.

c. Industry Collaboration:

Collaborate with other social media platforms, industry associations, and regulatory bodies to share best practices and collectively address challenges.

9. Public Reporting Transparency:

a. Publish Transparency Reports:

Regularly publish transparency reports detailing the number and types of reports received, actions taken, and trends in online abuse.

b. Aggregate Data for Research:

Aggregate and anonymize data for research purposes, contributing to a broader understanding of online behaviors and potential solutions.

c. Periodic External Audits:

Undergo periodic external audits of the redressal mechanism to ensure accountability and adherence to best practices.

10. Accessibility and User Support:

a. Accessible Reporting Tools:

Ensure reporting tools are accessible to users with disabilities, adhering to international accessibility standards.

b. User Support Channels:

Establish dedicated support channels to assist users in understanding the reporting process and addressing concerns.

c. Crisis Response Team:

Form a crisis response team to handle high-profile incidents and coordinate responses with public relations and legal teams.

Enhancing these aspects of the redressal mechanism contributes to a more comprehensive and resilient system for addressing social media misuse. Regularly solicit feedback from users and stakeholders to iterate and improve the system over time.

What is Mobile Application Security?

Mobile app security is a comprehensive mobile security solution for applications on mobile devices such as smartphones, tablets, smartwatches, and the like.

It is like a practice where you ensure that your product is safe from various cyber-attacks, such as malware, reverse engineering, keyloggers, data theft, and other forms of manipulation or interference, by implementing the best mobile application security practices available in the market.

Moreover, it involves examining the structures of mobile applications and how they work. It also involves checking the major areas of the application and analyzing what hackers or any external threats want to accomplish by penetrating your application.

The Common Mobile App Security Threats

To help you better understand security threats towards mobile apps, we listed the most common mobile app security issues and threats and how you can avoid or prevent them from happening to your organization.

Malware

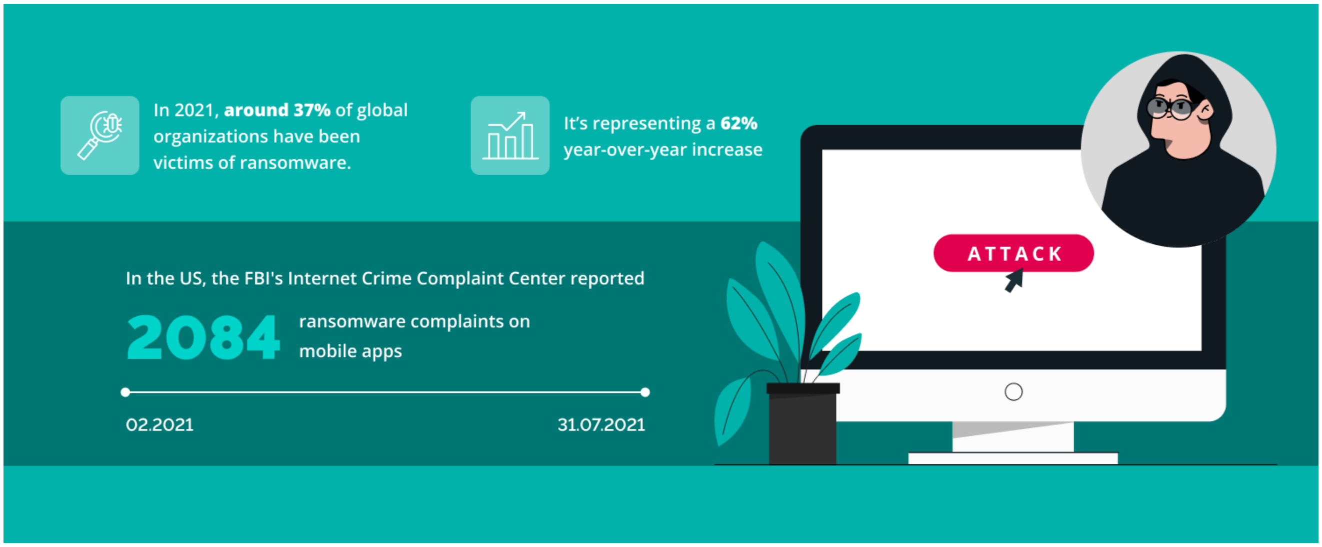
Malware is one of the most common cyber threats that mobile apps face daily. This intrusive software is designed to damage and destroy the internal systems of the user's device or computer. Moreover, it can explore, steal, and conduct various behavior controlled by an attacker.

In a report conducted by Verizon, approximately 86% of users were worried about malware, while 20% were unprepared to defend their devices against it. As technology and digital spaces evolve, malware grows more sophisticated and complex.

Ransomware

Another common threat in the mobile app industry is ransomware. A more specific type of malware, ransomware, is a set of malicious programs that penetrates your device and disables access until you pay a certain amount to the hacker.

In short, ransomware is similar to real-life ransoms, but instead of a person, it is your device that is held hostage by external captors. Such cyber threats are complicated and expensive to remove.



In 2021, **around 37%** of global organizations have been victims of ransomware.

It's representing a **62%** year-over-year increase

In the US, the FBI's Internet Crime Complaint Center reported

2084 ransomware complaints on mobile apps

Ransomware is the most preferred method of cyberattacks. In 2021, around 37% of global organizations have been ransomware victims. In the US, the FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints on mobile apps from January to July 31, 2021, representing a 62% year-over-year increase.

Crypto jacking

Crypto mining and cryptocurrencies are gaining steady popularity worldwide. Businesses, financial institutions, and the like are slowly adopting crypto and its principles. Crypto jacking is another cyber threat that attacks your devices and uses their computing power to mine cryptocurrency.

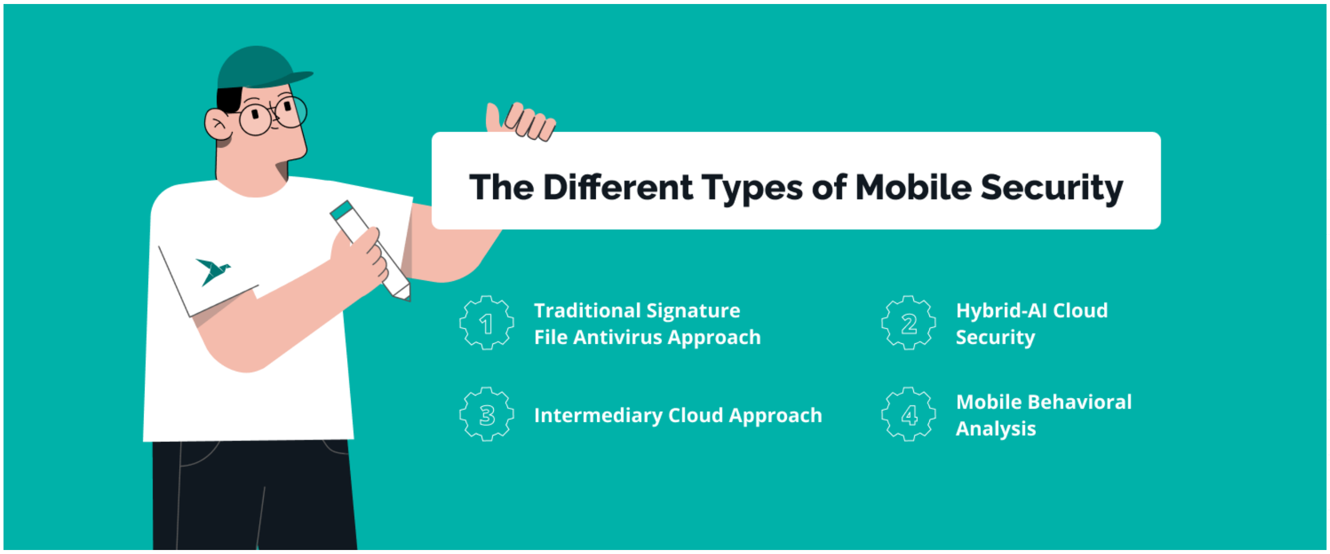
Victims who are attacked by crypto jacking experience rapid battery drain, device downtime, and operational disruption. Around 73% of organizations report concerns about crypto jacking and have experiences with such issues.

Insecure Coding

Failure to apply the best practices of mobile app development. Doing so can leave gaps within your code that can be easily infiltrated by hackers and other cyber threats that want to penetrate your app.

The Different Types of Mobile Security

Let's explore the four types of mobile app security models and how vendors can combine cloud-based threat defense with an on-device mobile security framework.


The Different Types of Mobile Security
1 Traditional Signature File Antivirus Approach
2 Hybrid-AI Cloud Security
3 Intermediary Cloud Approach
4 Mobile Behavioral Analysis

1: Traditional Signature File Antivirus Approach

Traditional antivirus software is a program designed to prevent, detect, and mitigate malware threats and functions. IOS and Android devices are generally void of the need to implement antivirus software, given that their operating system already has one. That said to exploit vulnerabilities and protect mobile apps, incorporating a traditional signature file antivirus is one of the ways vendors prevent malware and other cyber-attacks from reaching their mobile apps.

The traditional signature file antivirus model creates a signature file on the device where all apps and documents are compared. However, as mobile IOS and Android app and devices evolve, the approach's effectiveness has diminished over time.

To ensure that the Traditional Signature File Antivirus approach is fully maximized, it must deliver the following security features:

- High Performance and Intended Function

- Inherent Persistence
- Flexibility
- **2: Hybrid-AI Cloud Security**

Hybrid-AI Cloud Security involves software-defined networking (SDN), virtualization, and application support across all layers of the product or service. This method protects app security data, applications, user devices, and infrastructure associated with IT architecture. It also incorporates workload portability, orchestration, and management across multiple IT environments with at least one private or public cloud.

Implementing hybrid AI cloud security can significantly reduce your data's exposure to cyber threats. An app developer can keep sensitive and vital data away from the public space while taking advantage of the cloud for data with little to no risks.

3: Intermediary Cloud Approach

Through this model, any files users receive, download, and store within their devices are automatically uploaded to a cloud service where the files will be tested and compared. This determines if the files contain – or the file itself – malware or security threats.

This approach is ideal for mobile devices consistently connected to the internet or mobile data. On the other hand, devices with weak and slow networks can suffer or lag in performance. This method has the potential to run fast and extensive processes on high-powered cloud servers, which can eliminate the restrictions of on-device resources.

4: Mobile Behavioral Analysis

The mobile behavioral analysis approach is an AI-based preloaded application that prevents malicious activity within a mobile device by flagging suspicious behavior and intellectual property theft. Although most of its functions happen locally within the device, a part of this approach uses a cloud-based component where the agent occasionally downloads new suspicious behaviors to flag on the device.

This process is one of the best ways to find zero-day exploits, using crowd-sourcing to obtain and test files. However, its process is closer to a behavior-based approach than a simple penetration testing associated with the traditional signature file antivirus approach.

Reference chatgpt