Licel

licelus.com

The state of mobile app security

A third of our waking hours are spent staring at our smartphone screens. We rely on apps so much that for many businesses it's their most valuable asset. And yet collectively we're still not prioritizing mobile app security.

The apps we use every day aren't as secure as we think they are

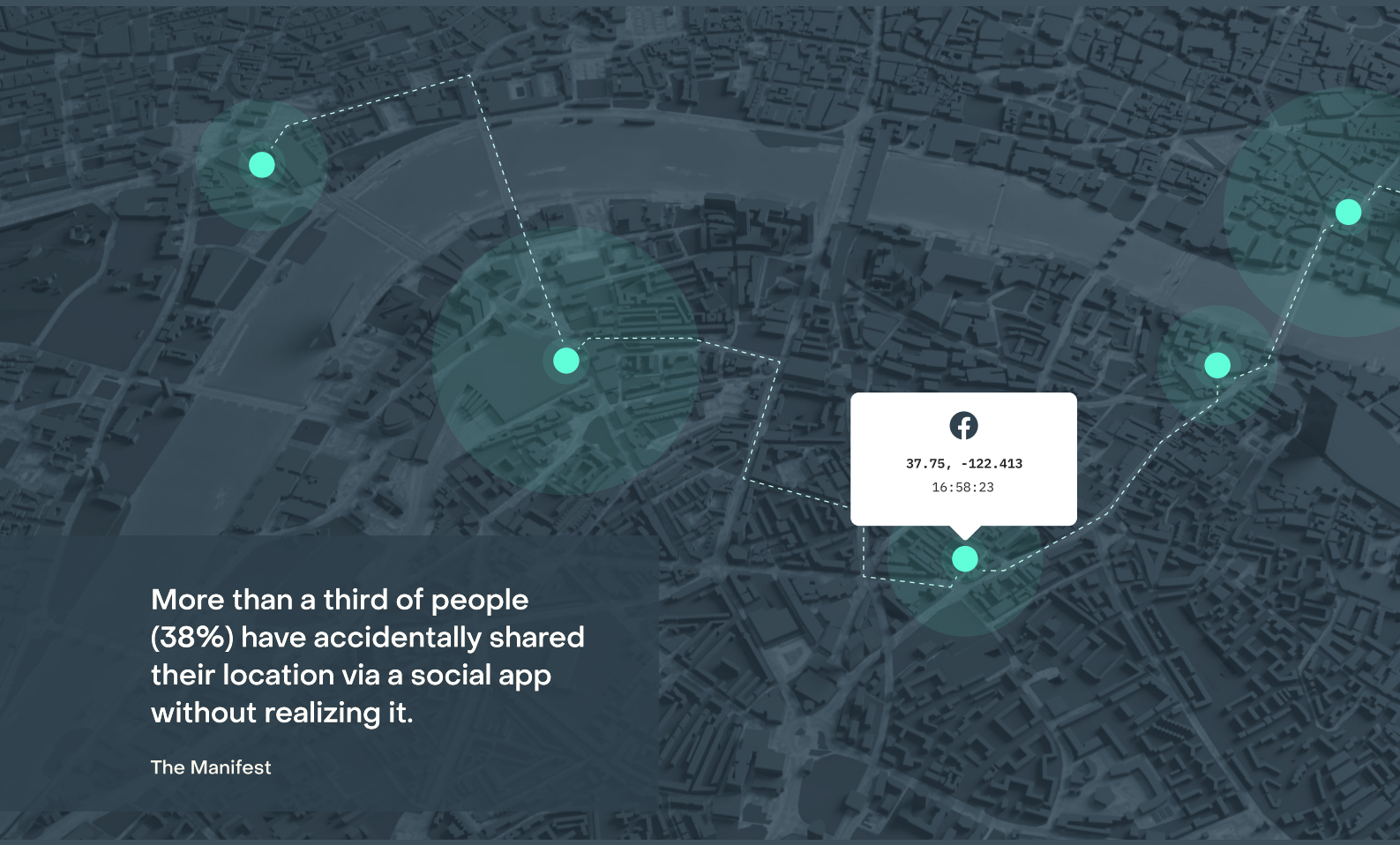
Mobile apps are something of a blind spot in cybersecurity. It's often assumed that if an application is available on an official app store, then it must be safe.

But the truth is that fake versions can end up there for unsuspecting end users to download. And even the genuine ones used by millions often run without the kind of robust protection needed to deter modern attacks.

> There's currently a massive disconnect between the value we place on everyday applications and how robustly they are protected.

It's time we think more carefully about the data apps collect and how attackers look to extract it.

We’re sharing more personal data than ever before



More than a third of people (38%) have accidentally shared their location via a social app without realizing it.

The Manifest

306.4 billion emails were estimated to have been sent and received each day in 2020. This figure is expected to increase to over 376.4 billion daily emails by 2025.

statista.com

3.2 billion images and 720,000 hours of video are shared online daily.

theconversation.com

WhatsApp and Facebook Messenger combine for more than 60 billion messages sent every day.

The Verge

The average person sends 72 messages per day.

Twilio

The phone has transformed from a communication device into a device for everything

Not so long ago your phone collected data like contact numbers and the contents of text messages. Now it collects enough data to tell your entire life story.

Data shared in 2007

Contact numbers
Text messages

Data shared today

Contact numbers
Text messages

Bank details
Health records
Purchase history
Digital IDs
Photos
Social networks
Dating profiles
Fitness logs
Covid certificates
Location tracking
Videos
Mental health logs

A river of data flows to and from our phones every day. The current carries health records, banking credentials, and even details about our dating preferences.

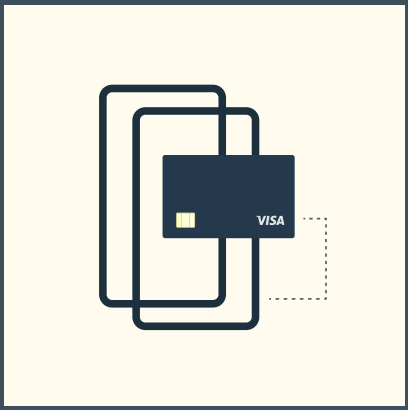
Think about the amount of personal information you share in a given day and it's easy to see why mobile apps are such an attractive target for cybercriminals.

The phone is no longer a device we use. It has become a second home we escape to.

Mobile device usage is evolving. What does this mean for security?

The covid-19 pandemic has given some existing tech trends a push. It has also ushered in others we didn't expect. The end result is that the smartphone is now taking on tasks it was never designed to carry out. And some of them have big cybersecurity implications.

/ The rise of cashless payments



The demise of cash was on the cards long before covid. What the pandemic did was to push cash closer toward the precipice. The phone has filled the gap - cementing its role as our go-to device for digital payments. But are the mobile banking apps we use every day secure?

- Cash payments plunged by 35% in the UK in 2020
- There was a 28% YoY increase in finance app downloads worldwide in 2021 to 5.9B.
- By the end of 2025, close to 40 million US adults will hold accounts at digital-only banks.

Sources: The FT, Statista, eMarketer

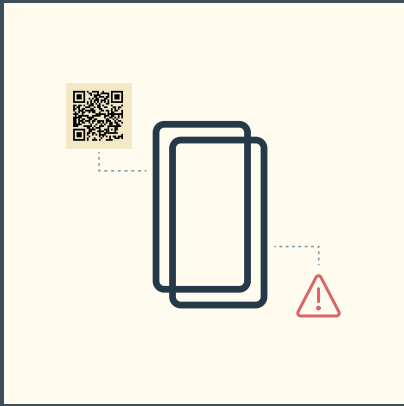
In no time at all the phone has become our de-facto wallet. But recent attacks illustrate that the finance apps we rely on aren't as secure as we'd like them to be.

Risks

Financial apps have become the holy grail for hackers. And that helps to explain why their attacks have become increasingly sophisticated and brazen in recent months. The more we rely on mobile apps to manage our money, the more we need to be aware of a changing threat landscape.

- Malware capable of capturing user credentials
- Fake banking apps designed to trick customers
- Man-in-the-middle attacks to intercept sensitive info

/ The comeback of the QR code



The QR code is the most striking example of the covid pandemic causing a shift in our digital behavior. The perfect tool to help us return to the lives we knew while keeping a safe distance, it seems they're back for good. But should we be so trusting of them?

- There was a 94% growth in the number of QR code interactions from 2018-2020.

- The number of US smartphone users scanning a QR code will increase from 83.4 million in 2022 to 99.5 million in 2025.

Sources: BlueBite, eMarketer

During the 2022 SuperBowl, Coinbase ran an advert in which a QR code moved around people's TV screens. Without thinking, millions reached for their phones.

Is there a danger that we're normalizing the act of randomly scanning QR codes?

Risks

People have gotten used to being suspicious of URLs. But there's a general feeling that all QR codes are safe - potentially as they're often associated with official documents like boarding passes and covid certificates. The problem is that QR codes are everywhere these days. And they're easy for a bad actor to manipulate.

- Redirecting someone to a bogus network.
- Sending somebody's location to an app.
- Malicious link to a site where users are tricked into downloading a fake app with malware embedded.

/ Health and tracking

The phone and smart wearable devices have become daily trackers of our health, our fitness, our moods, and our desires. We're actively encouraged to check in regularly and share information about ourselves. Yet we don't tend to question how secure that information is.

- The Global IoT in Healthcare Market size is forecast to grow from USD 60.83 billion in 2019 to USD 260.75 billion by 2027.
- Global spending on mobile mental health applications is set to reach close to US$500 million in 2022.
- The global wellness market is estimated to be worth more than $1.5 trillion, with annual growth of 5 to 10 percent.

Sources: Biospace, Deloitte, McKinsey

"I go to a lot of cybersecurity conferences like Black Hat, Def Con, and I meet executives from all over. Except healthcare. I've never met a healthcare exec at these conferences. They're the only industry I don't see."

Alex Balan, Security Research Director at Bitdefender

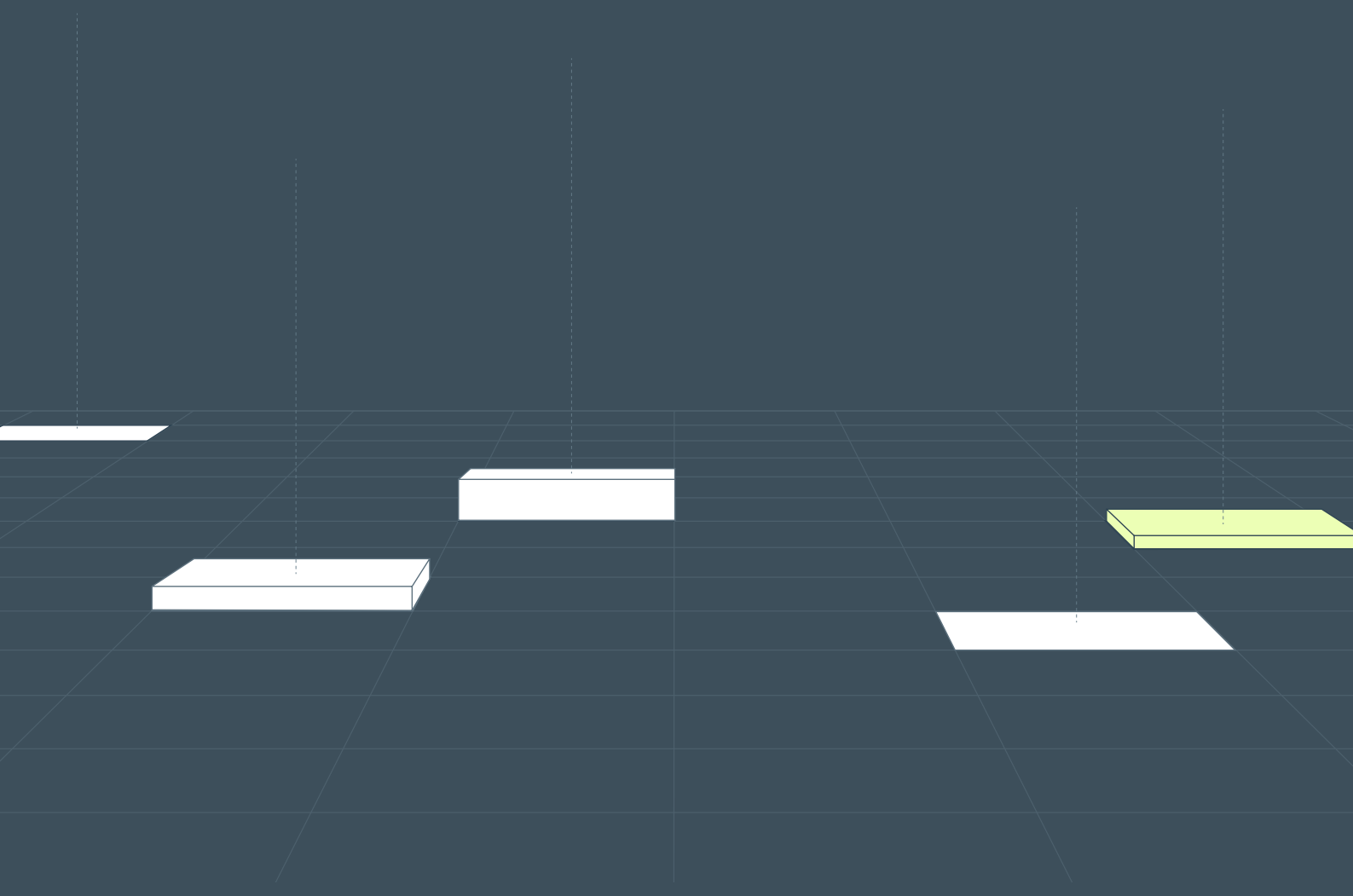
Risks

The main worry for the health, fitness, and wellness sectors is they haven't traditionally had to worry much about cybersecurity. So, they often don't have the security infrastructure in place that other industries do. This helps to explain why they've been targeted so much during the pandemic.

- Vulnerabilities unique to IoT devices.
- Medical records stored unprotected.
- Insufficient security knowledge and outdated sytems.

Mobile app security threats

Attacks against mobile apps are becoming normalized due to a lack of protection. In the UK alone, bank transfer fraud victims lost £28,000 per hour between 2019 and 2021.



Tampering

Bad actors often try to tamper with the code and logic within an app after it has been handed over for publication on an app store. In a completely unprotected app, hackers don't need any dynamic tools to do so. As well as tampering with the app's core functionalities, attackers can also override security measures.

Malware

Malware often arrives on a user's phone via a seemingly legitimate text message. It can then hide within an app that users may have forgotten is even on their device before waking up at just the right time – such as when a banking app is opened. Then the malware uses fake screens to steal a user's credentials.

App cloning

Bad actors can decompile a genuine app before releasing their own fake version in the hope that an end user will download it. It's an easy mistake to make. Once the cloned, bogus application is downloaded, any information a user shares – login details, passwords, or financial data – can be harvested by the attacker.

Key logging and screen recording

Attackers can log tapped keys and record the phone's screen to capture a user's in-app activities. Typically this takes place when someone is entering their login details via a user interface. In both cases the user is completely unaware of anything untoward happening on their device.

Man-in-the-middle attacks

Man-in-the-middle attacks happen when cybercriminals exploit weaknesses in network connections to hijack the communication between an app and the server. By doing so, bad actors make it so that sensitive details shared in an application arrive at their malicious server instead of the genuine one.

Injection of malicious logic

Here, a bad actor attempts to access the app and either inject some malicious code or modify the app's logic. The main goal is to manipulate the contents of the app somehow so that the attacker has control over it and can override security mechanisms.

Software supply chain attacks

Attackers can include malicious code inside otherwise useful, open source libraries. Developers may then incorporate these as dependencies, completely unaware of the danger to their app and its users.

Digital rights management violations

Piracy is a huge and evolving threat. And mobile applications are now a big part of it. Attacks are often designed to gain a competitive advantage over rivals, sell intellectual property secrets, or simply consume content without paying a subscription fee.

Static and dynamic analysis

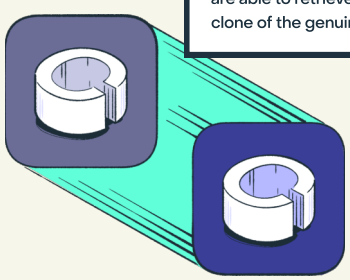
Attacks often start with code analysis. Static analysis is the simpler of the two as it involves a bad actor reading the files within an app. If these files are obfuscated, then static analysis is almost impossible. Dynamic analysis is more complex and involves hackers creating a special environment to run the app in.

> Understanding how apps are at risk is the first step in protecting them. But a lot of companies don't carry out this vital threat analysis.

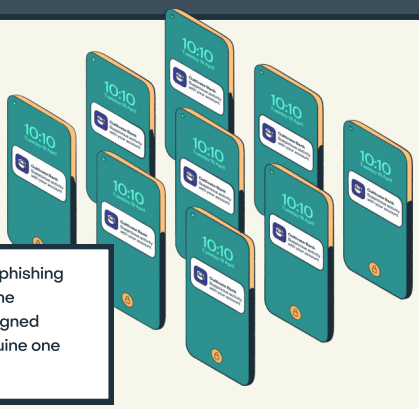
How attacks can happen

Understanding how attacks can happen is a crucial step in being able to prevent them. The following example shows how cybercriminals create a fake app and how they convince people to download it.

Bad actors carry out either a static or dynamic analysis on a banking application to scope it out. They're looking for weaknesses here – like some code that hasn't been encrypted or obfuscated.

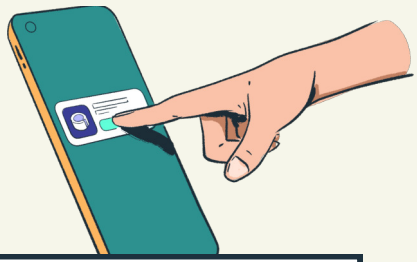


With the code and logic the attackers are able to retrieve, they prepare a clone of the genuine banking app.

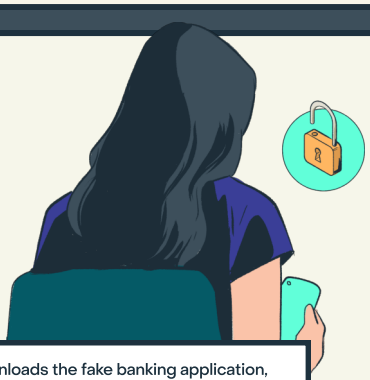


They then prepare and send a phishing message to thousands of phone numbers. The message is designed meticulously to look like a genuine one from the user's bank.

This message uses social engineering techniques to convince the user to click on a link. Often it refers to something urgent that needs to be investigated or fixed by the user. One example is to warn them that an unknown payee has been added to their account.



The user clicks on the link in the SMS and is taken to a page where they're encouraged to download an updated version of their mobile banking app. But in reality this is the fake version the attackers created using code extracted from the genuine app.



Once the user downloads the fake banking application, they enter their credentials which are stolen by the attackers. The bad actors then use these in the genuine app to log in and transfer funds to their account.

SMS phishing messages work because attackers know that we behave differently on our phones. We're more at ease. Our guard is down.

Platform security alone isn't enough to protect against modern attacks

It's quite common for people to think that the iOS and Android ecosystems already keep apps secure. But the truth is that while Apple and Google security is better than it has ever been, it isn't enough on its own to block modern attacks.

Android is an open, fragmented ecosystem with multiple vendors. The majority of its users run outdated versions that don't get security updates.

Apple's walled-garden approach to security means it does a better job at blocking threats. But it's still vulnerable to more dynamic attacks.

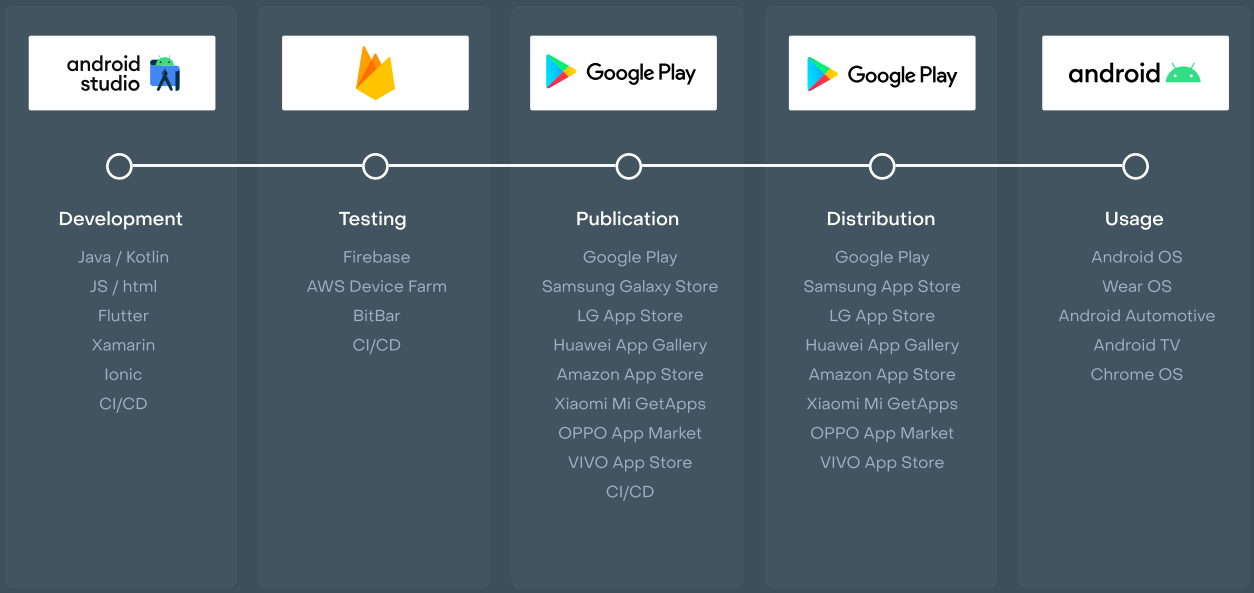
Multiple layers of security are needed to stop modern, sophisticated cyber threats. You can't rely on Apple and Google alone.

Android

Android's open nature allows for plenty of freedom and customization. But a large proportion of devices are running legacy versions with security gaps attackers can exploit.

- 2.5 billion users in 2022
- Only 37% of global Android users were using the latest version at the start of 2022. [statcounter.com]
- In 2021, security researchers discovered that 13 popular Android apps exposed the personal data of up to 100 million users.

The Android ecosystem



How Android helps to secure apps

By default

- Personal information protection such as phone numbers and hardware identifiers (provided you're running the latest version of the OS).
- Permission control.

Optional / needs to be configured

- Regular OS security updates (not everyone receives them due to problems with legacy devices).
- Limited network security aimed at stopping man-in-the-middle attacks.
- Overlay attack protection.
- Google SafetyNet - designed to protect Google Play services.
- Google Play Protect - designed to check the app's environment.
- Antivirus protection sometimes comes preinstalled on Android devices.
- Bootloader protection available with certain vendors.

Recommendations for enhanced security

Defense against:

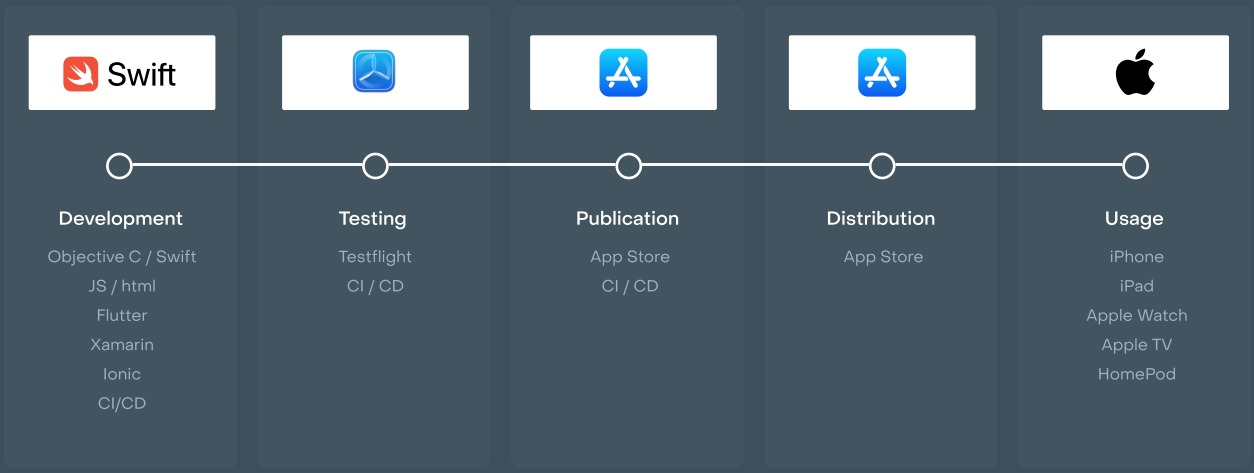
- Application-level digital rights management.
- Permission control.
- App cloning.
- Injection of malicious logic.
- Static and dynamic attacks.
- Malware.
- Key logging, screen capture, and screen recording.
- Tampering of an application.
- Digital rights management violations.
- Software supply chain attacks.

iOS

The centralized nature of Apple and its streamlined update process makes iOS a more secure platform than Android. That said, it can still be vulnerable to more sophisticated, dynamic attacks.

- Over a billion users in 2022.
- A zero day flaw in 2021 took advantage of a weakness in Apple's iMessage, exposing 900 million active users.

The iOS ecosystem



How iOS helps to secure apps

- Personal information protection.
- Permission control.
- Process isolation.
- Digital rights management.
- Limited protection against app cloning.
- Limited protection against tampering.
- Limited protection against static analysis.
- Extensive (but not total) protection against malware.

Recommendations for enhanced security

Defense against:

- Injection of malicious logic.
- Dynamic analysis.
- Malware.
- Key logging /screen capture / screen recording.
- Tampering.
- Network communication interception.
- IP theft.
- Sensitive Data / Key material Exfiltration.

Threats to the ecosystem

Attacks against mobile apps can take place across the entire lifecycle - from early-stage development through to everyday use.

Development

/ Malicious source code injection
/ Vulnerable dependencies
/ Compromised CI / CD
/ Compromised package repository

Testing

/ Vulnerable dependencies
/ Compromised CI / CD
/ Compromised package repository
/ Upload of malicious artifact

Publication

/ Tampering
/ Malicious code injection

Distribution

/ Tampering
/ Malicious code injection
/ DRM violation
/ App cloning
/ Static and dynamic analysis

Usage

/ Tampering

/ Malicious code injection

/ DRM violation

/ App cloning

/ Malware

/ Screen recording and keylogging

/ Man-in-the-middle attacks

/ Static and dynamic analysis

Right now it's impossible for the major platforms to protect all of their legacy devices from cyber threats.

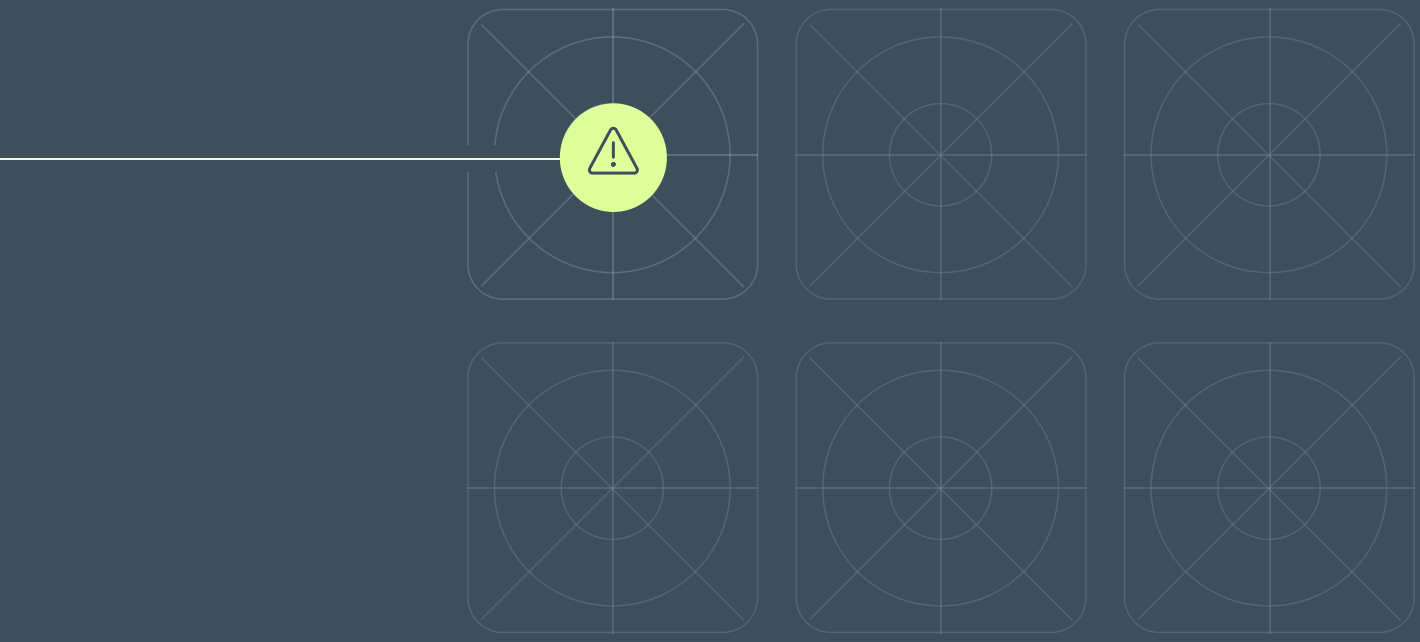
The threat landscape for mobile apps is shifting all the time. This is a big challenge because while Google does support some legacy versions that are up to two years old, there's a limit to how far back their security can stretch.

> Apps are at risk from mobile security threats if they rely only on the protection offered by Android and iOS.

Businesses aren’t taking mobile app security seriously enough

We recently analyzed the mobile app security used by some of the world's biggest banks. The findings are shocking and suggest a lax approach to app protection currently permeates the industry.

This isn’t just a problem for banks. Most of the apps people rely on every day don’t have full-scope protection. They run with unlocked doors that hackers can easily push open to take a look around.



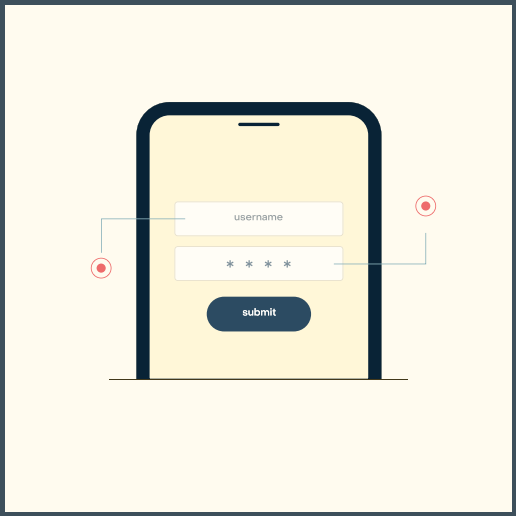
The 4 essential protection mechanisms below are curiously absent from all of the mobile banking apps we analyzed.

Keylogger detection

Hardly a day goes by without a news story about a new form of mobile banking malware exploiting Android's Accessibility Services.

This vulnerability allows the malware to log taps, keystrokes, and touches of a smartphone screen. Specifically, when the user is inputting sensitive data such as login credentials or card details.

Keylogger detection stops this vital information from being leaked.

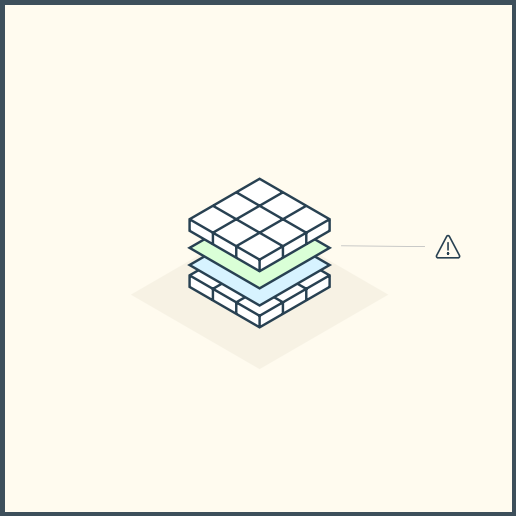


Tampering detection

An application can be tampered with after developers hand it over for publication on an app store.

Parts of it can be modified or removed. Attackers can inject it with malicious code. Or it can even be resigned and redistributed illegally elsewhere.

Without tampering detection - which confirms that the code and logic within the app is exactly the same as before - banks simply have to hope for the best.

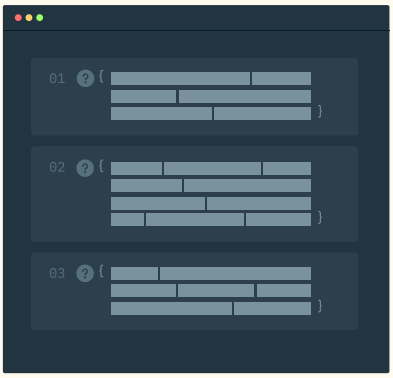


Debugging and hooking detection

Debugging and hooking frameworks are a hacker's best friend. They enable them to analyze an app and understand how it works.

Obfuscation of the code within your app is useless if you don't also protect against these frameworks. That's because they enable attackers to bypass the app's security controls.

Given how fundamental this activity is for bad actors, not being able to detect it is a massive oversight.

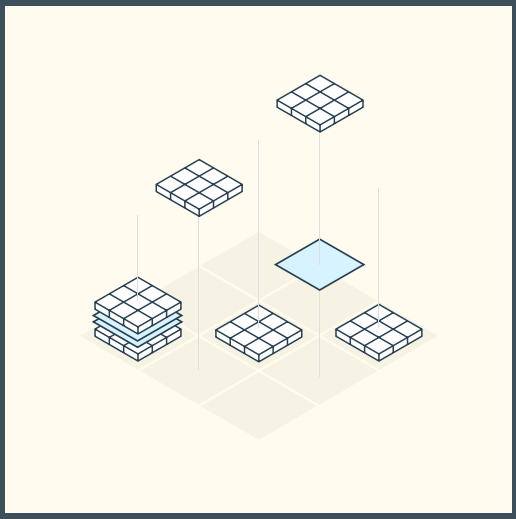


Runtime data protection

Banking apps deal with a fast-flowing stream of sensitive information and cryptographic operations. Every bit of code and data gets mapped and recorded in the memory.

That's why the app's memory is such a common target for cybercriminals.

Without app memory protection, hackers can find all the information they need there. This includes individual customers' processed banking credentials.



Banks are in danger of permanently losing the trust of their customers.

The four mobile app protection mechanisms above are just some of the vital barriers to attack that are currently being ignored by respected global banks.

What makes this study particularly shocking is that banking apps are increasingly viewed by banks as their most important asset. Oftentimes the app is the only interaction a customer will have with the brand. In the event of a loss of customer data or money, the long-term hit on reputation would be difficult to recover from.

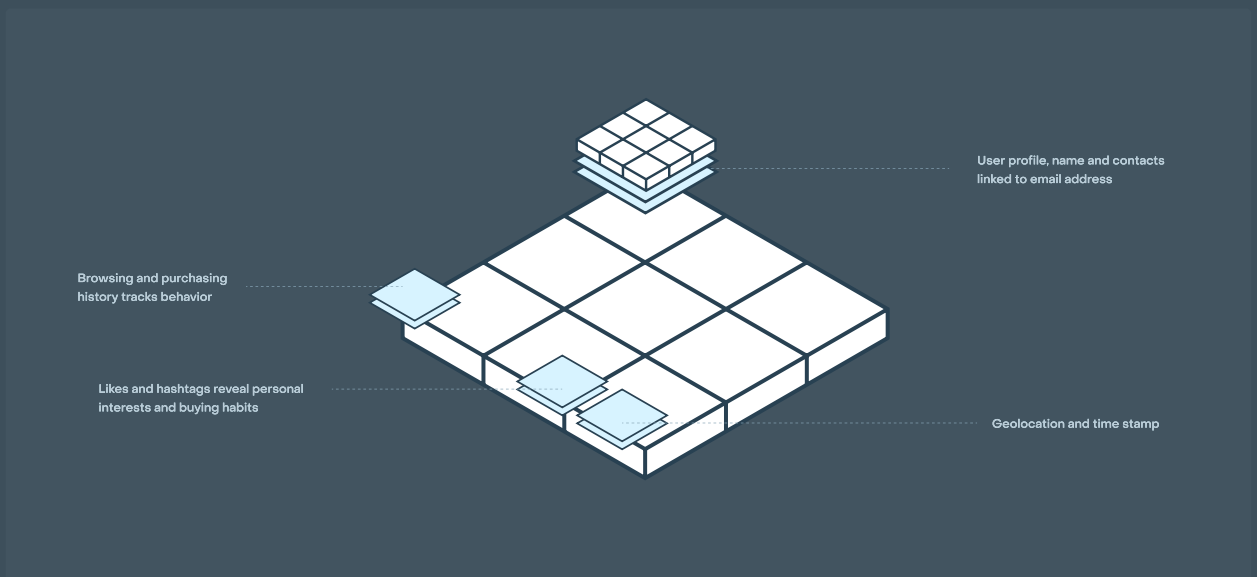
> Security advice from banks to customers is meaningless if they don't protect their own app from damaging attacks.

App protection is a trust enabler

When attacks against mobile apps take place, there are typically two victims: individuals and businesses.

The impact on individuals really can't be overstated. If you asked a friend whether she'd rather lose her wallet or her phone, she'd almost certainly choose her wallet. That's because of the amount of highly-personal information that exists on our phones. We feel an emotional connection to the device as we associate it with friends, family, and shared memories.

Often, individuals would be able to claim their money back if a banking application were hacked. But this isn't the case with other attacks. Think of health records, for example. Once they're gone, they're gone.



Customers are placing their trust in businesses to look after their personal data.

For businesses, it's trust more than anything else that they stand to lose. And this is a big problem at a time when trust is valued by customers above and beyond any other metric.

The amount of phishing messages pinging on phones during the pandemic brought cybersecurity to the forefront of people's minds. There's a realization now among end users that the device they carry around with them is a target for bad actors.

> Customers will increasingly expect the companies behind the apps they rely on to make sure they're secure from attacks.

Businesses are more transparent than they've ever been, which is great. But advice about passwords, multi-factor authentication, and how to spot phishing attacks will appear hollow if companies don't also invest in protecting their applications.

Compliance and regulations

Aside from the reputational fallout from an attack, businesses can also expect fines and penalties related to compliance violations.

Regulations like Payment Service Directive 2 (PSD2), Payment Card Industry Data Security Standard (PCI DSS), and the Federal Financial Institutions Examinations Council (FFIEC) have been introduced in the financial sector. These make strong mobile app security a must-have for banks.

For a long time the focus has been more on recovery rather than mitigation. Instead of equipping an app with the defensive tools to stop an attack, businesses have invested in insurance to soften the blow of one. But in the coming years this simply won't be a viable option. Not only because insurance premiums are on the rise, but because this approach does nothing to stop the hit on a company's reputation with customers.

What can we do to improve mobile app security?

A common theme in this report is that mobile app security isn't being prioritized enough given the tasks we demand from apps and the complex threats they face.

Right now it feels a little bit like hackers have a head start. They know people tend to be more relaxed – and therefore more vulnerable – on their phones. They know that platform security alone isn't up to the task of protecting mobile apps. And they know that developers and businesses often don't protect their mobile applications as robustly as they should do.

Together we can make apps safer

Collectively we can rebalance the scales so that security is given as much weight as speed and convenience. Together – end users, mobile ecosystems, and businesses – we can make it so that it's simply not worth the effort for bad actors to attack mobile apps.

What individuals can do

While mobile app security is much more of a business responsibility than it is for individual app users, there are things we can all do to make our mobile devices safer.

Chief among them is being more suspicious. This might sound like a sad piece of advice to give when using a device that you associate with family, friends, and fun. But it's a vital trait for the modern digital world.

If you see a message from your bank or elsewhere that looks a little bit suspect, stop for a moment. What is the message asking of you? Is it reasonable? If you're even a little unsure, contact the company directly and query it.

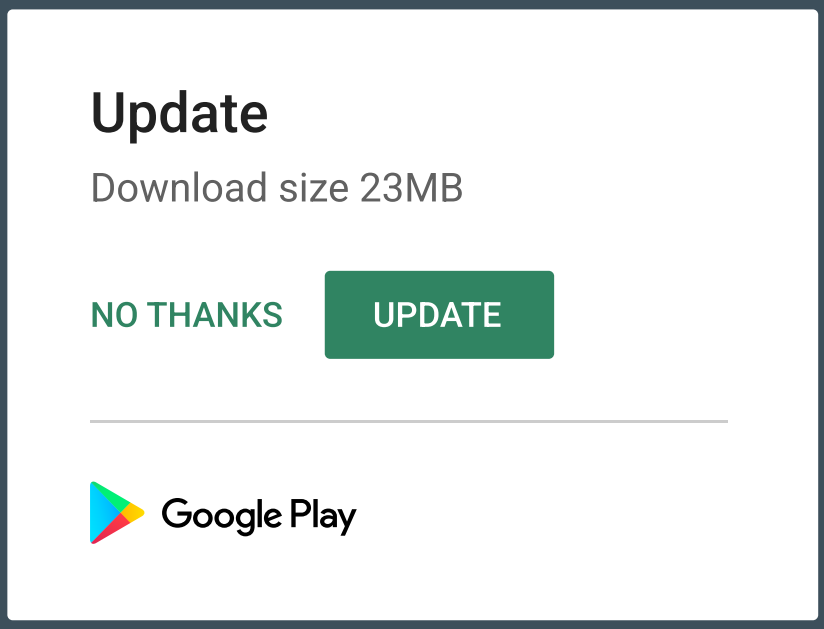
- Use multifactor authentication.
- Make sure you're using the latest version of the OS.
- Be wary of untrusted networks.
- Know the data that you're sharing.
- Don't install mobile apps from untrusted places.
- Don't root or jailbreak your phone.
- Use strong passwords and biometric data.
- Always keep your apps up to date.
- Use an anti-malware solution.

What Google and Apple can do

The big two mobile platforms have done a lot in recent years to improve the privacy and security of their ecosystems. But this is a massive challenge and very tricky for them to fix in one go. Particularly as attack techniques are evolving and new attack vectors emerging almost constantly.

One key objective for both has to be the prevention of dynamic analysis. We've seen countless examples in recent months of malware being successfully published to the Play Store in particular. Apple isn't immune from this, either, though.

For Google specifically, a key challenge is to solve the problem of fragmentation across vendors and manufacturers. Too many Android users don't receive security updates because they're running legacy devices. Google should consider embedding a security component into applications to offset this vulnerability.

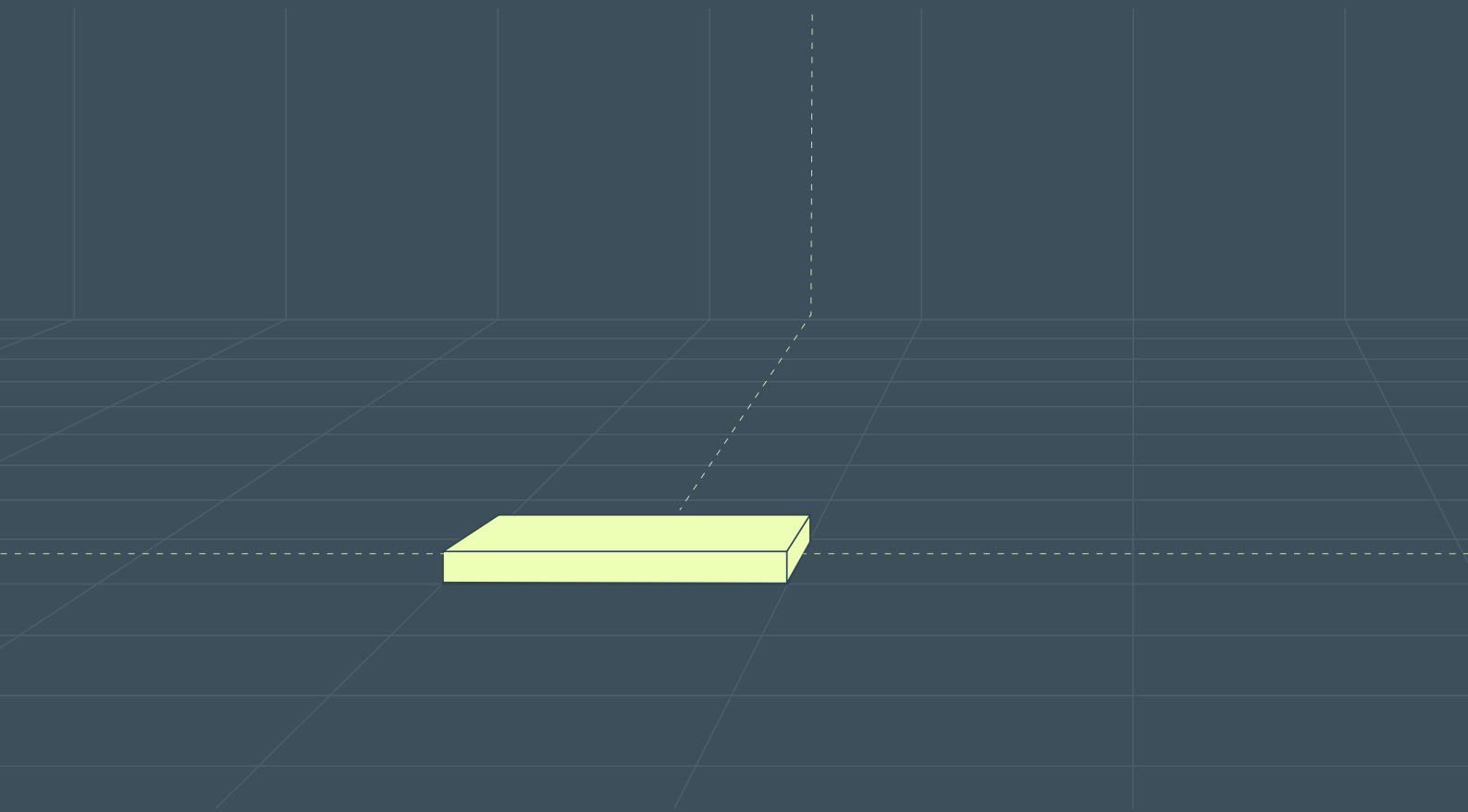


What businesses can do

Our research into banking security earlier in this report highlighted that businesses have a lot to do to make their apps more secure. Right now they're making it far too easy for bad actors to take a look around and exploit weaknesses.

The first step in making their mobile apps more secure is for companies to think about security differently. Protection can't just be a last minute consideration at the end of the app development process. Instead, it needs to be holistic, consistent, and continuous.

This is particularly vital in the zero-trust world we're living in. A world where businesses have no idea about the environment their mobile apps will be used in. It simply isn't an option anymore to publish an app unprotected into this world and hope for the best.



What are our mobile app security essentials? Aside from embracing security by design processes as outlined above, businesses should be implementing the following protection measures:

Code hardening

At the very least you need to harden your mobile application to make it more difficult for an attacker to read its code and logic. This means using robust encryption and obfuscation techniques that can help to prevent static analysis.

Anti-tampering

Your app's integrity is its most important factor. You need to make sure that nothing has changed in its code between handing it over to be published on an app store and it being downloaded by your end user. That's where integrity checks come in.

Runtime checks

Runtime checks are there to make sure that your app isn't being run on a rooting or debugging framework and that it isn't being used on a jailbroken device. These checks can prevent dynamic analysis by causing the app to crash and not function.

Network protection

As well as security built into your application, you need to safeguard the communication between the app and the server. By hardening this network you help to stop man-in-the-middle attacks and ensure that hackers can't hijack your user's credentials.

User interface protection

A big part of malware attacks is using fake screens to trick users into entering their details there and recording them as they do so. User interface protection stops this attack from succeeding by preventing screen capturing.

A trusted execution environment

If your application processes sensitive operations such as financial transactions or cryptographic operations, then you should consider using a trusted execution environment. This is a protected space within the app that bad actors can't access.

How we can help

DexProtector is our no-code mobile app security solution. It protects more than 10 billion instances of mobile applications and saves businesses both their resources and their reputation with end users.

Visit licelus.com to learn more