The Developers Guide To Mobile App Security

a guide by

APP SOLID.

The development period of a new mobile application is an exciting time. After months or even years of preparation, your vision is on track to go live, and you couldn't be more invested in its long-term success. However, amidst all the decisions involved in developing a new app, many developers tend to neglect one of the most critical elements, namely security. For all the ingenuity and forethought put into the functionality and marketing rollout of a given app, it's alarming that security doesn't receive nearly the attention it deserves, especially considering the monstrous price your app may be forced to pay without an effective security strategy.

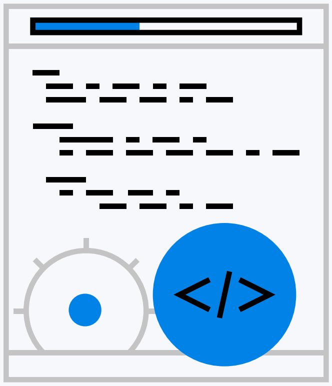
As mobile technology has grown in prominence, hackers have accordingly stepped up their efforts to infiltrate these apps, often making an attack more of an inevitability than a question. In fact, research shows that 75% of mobile apps already lack the most basic form of security. Since apps frequently handle sensitive user data, a malicious hack could wreak havoc on your business. Your reputation and sales will inevitably suffer, as your intellectual property falls into the wrong hands. Developers could even be open to legal issues, and all that only marks the beginning of the consequences an app may face without proper security measures in place. Thankfully, AppSolid presents a one-stop guide to understanding the truth about mobile app security and how you can guard against hackers.

Debunking the Myths

So much has been said about mobile apps in recent years, but we're willing to bet that some of what you think you know is based on misconceptions and falsehoods. Let's break down some of the most common myths about launching a mobile app and unveil the truth at last.

Coding languages:

In many cases, developers may wind up having to incorporate as many as 10 different coding languages and frameworks into their app. You can streamline this by using app platforms that enable you to use a preferred coding language, but be sure to do your due diligence when it comes to deciding on which platform best fits your needs and your security standards.

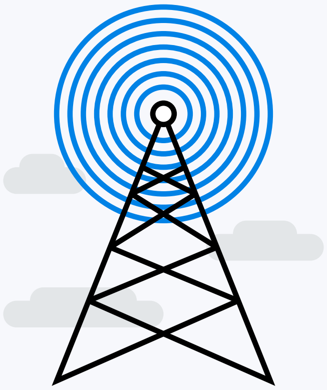


The development process:

Common belief is that businesses take a minimum of six months to develop new apps, but in actuality, that all depends on the mobile platform involved. Oftentimes, developers reuse code and back-end services to expedite the process. While this makes sense from a time standpoint, it may open the door for security vulnerabilities if the right measures are not taken.

Data transmission:

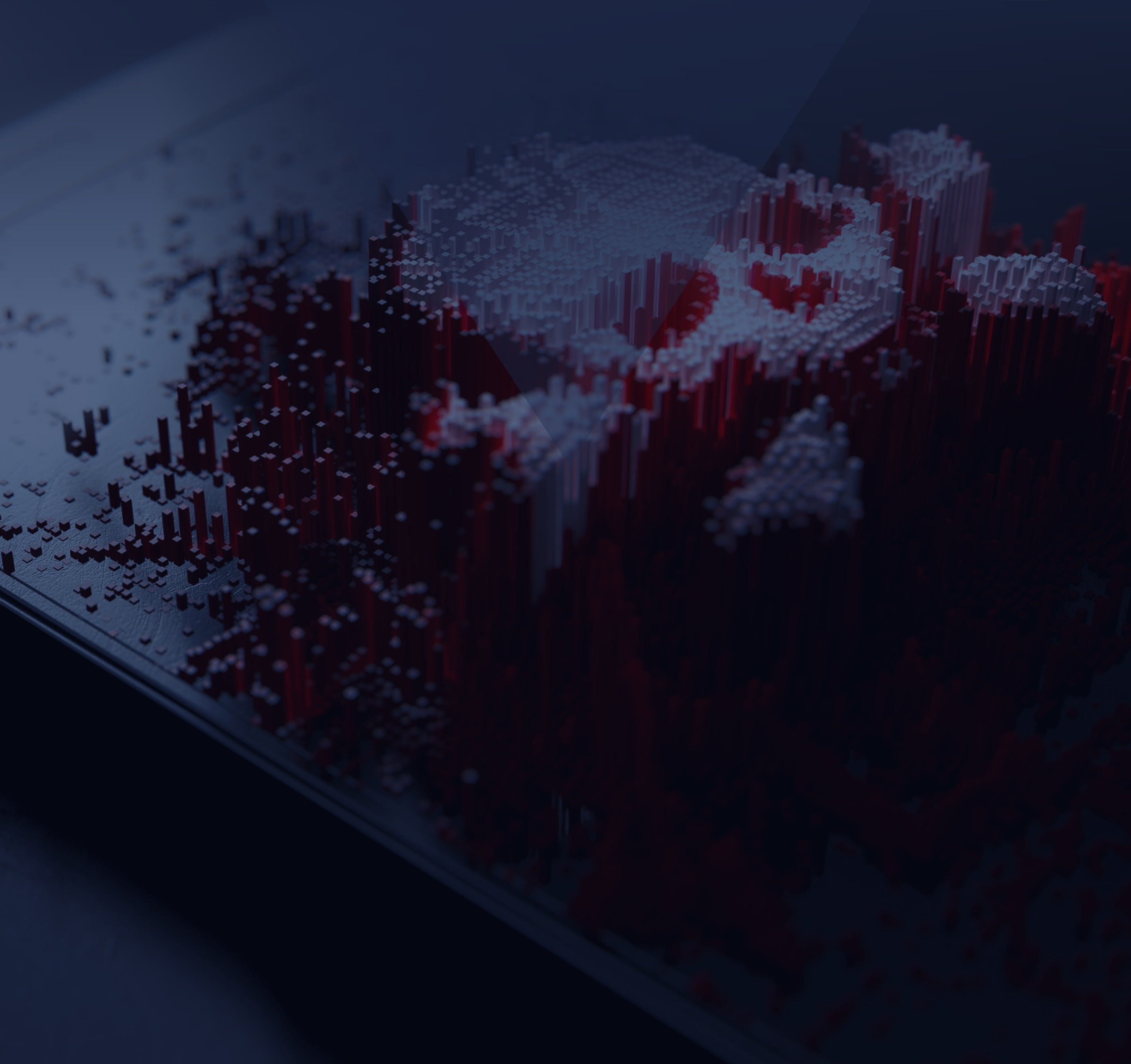
While apps are frequently assumed to be extraordinarily heavy on data, this actually depends on your mobile platform. Data usage is, in fact, on the rise, but you can mitigate this by opting for a platform that transmits a smaller data set. Not only does this approach reduce overall data transmission, but it also maximizes your app's ability to maintain protection, since hackers can intercept transmitted data.



Leadership:

Once upon a time, a single team member may have been equipped to single-handedly oversee app development for a given company, but with the proliferation of mobile apps, that is certainly no longer the case. In order to stay on top of this ever-evolving aspect of business, you need an entire team of specialized personnel to keep your app running smoothly and, yes, maintaining the highest level of security.

The Danger of Hackers



So you're ready to take the steps of modernizing your app's security. But first, let's review exactly what you're up against. As we've alluded, hackers are a tenacious bunch, and they have identified countless techniques to break into an app. Some are as simple as guessing passwords or abusing the access of an open network, while others involve more complicated methods such as email phishing, implanted malware, and server scans for existing vulnerabilities. No matter how hackers launch an attack, the need for ample security to address these perceived vulnerabilities has never been stronger, especially when you ponder the consequences that would arise should they gain access to your app.

In nearly every case, hackers have one of two motives. After they gain access, they intend to steal sensitive data from within your app -- either the code itself or your user data, often both -- or take over the device itself by connecting it to a malicious network of private computers known as a botnet. As you might imagine, the rise of mobile technology has made protection more difficult than ever, with users readily moving from one network to another and oftentimes saving sensitive data in a single repository. Millions of devices are infected every year, leaving hackers with countless entry points and a fountain of information that was never meant for their eyes. In today's world, it's an absolute must to invest in security measures for your app. Only then will you be able to identify your app's vulnerable points early enough to act.

Hackers have a number of tricks up their sleeve. In greater detail, here are a few of the greatest threats you're likely to come up against in your battle to keep your app and its users safe:

Unencrypted code:

It may sound like common sense, but you'd be surprised just how many developers fail to effectively include encryption as part of their coding. This is the first line of defense against hackers, and a strong encryption framework should serve as the foundation of your security strategy.

Easy access:

Leaving your mobile app open to interaction with the back-end might be convenient, but it could leave your app vulnerable to hackers. Only provide access to authorized personnel, and consider incorporating location, time or action as additional restrictions. These simple measures may go a long way toward keeping malicious users away or, at the very least, will discourage them from tampering with your app.

Not enough storage:

Apps that don’t offer enough storage often leave users no choice but to save sensitive information on their devices. This makes it easier for hackers to gain access to any passwords, payment information or other personal data. Rather than concealing them behind the encryption of your app, they are made readily available to prying eyes.

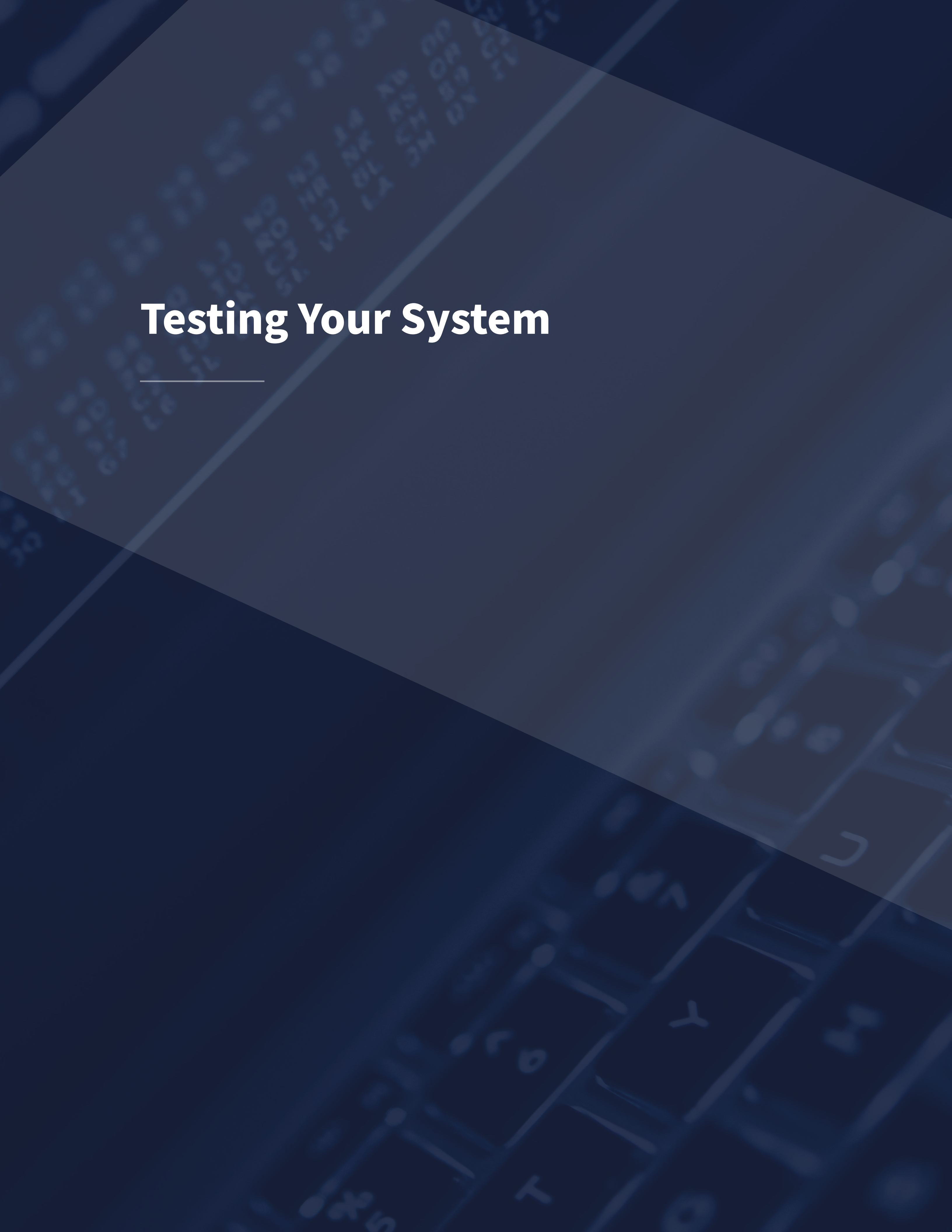
Malware:

We’ve already briefly mentioned malware, but seeing as it is such an essential tool in the hands of hackers, it bears repeating. We’ve all seen them, whether in the form of a pop-up ad, a game or a cryptic yet critical message. Malware often tricks users into downloading it, and without security to guard against it, your app may be an easy target.

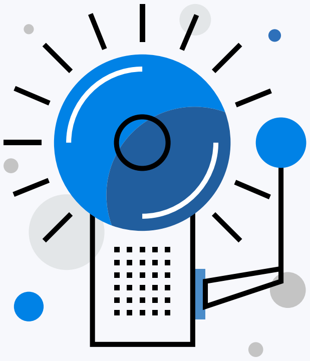
Reverse engineering:

This act is when a hacker accesses and changes central elements of your app’s code, granting them full control of your app and any devices associated with it. In some cases, hackers may wind up impersonating the developer and passing off the altered app as the real deal.

Testing Your System



By now, we imagine that you're wondering whether your app has already fallen prey to one or more of the tactics discussed above. Quite often, developers remain completely in the dark when this does happen, as hackers have gotten increasingly better at covering their tracks. Because of this, we encourage you to maintain testing of your app long after launch has passed.



In fact, security testing should be ongoing as long as your app remains active. Nowadays, countless services -- including ours -- offer a simple, fast ability to scan your app for any vulnerabilities so that you know what aspects of your app need to be addressed immediately. After all, hackers will have a much easier time attacking an app that features outdated or non-existent security measures.

To better prepare you for testing your system's vulnerabilities, here are some key tools that you can use for your app:

OWASP Zed Attack Proxy Product:

Few resources are as updated or tested as this one, which relies on international volunteers to stay current. A free program, it's open-source design makes it a cinch to evaluate security threats.

Smart Phones Dumb Apps:

Apple and Android users can use this program to test their source code and identify any vulnerabilities that may result from a weak code. Moreover, it provides a static code analyzer (SCA) that can scan on Java-based Android apps.

Wireshark:

Monitor network traffic with this open source option, featuring updated stable downloads. It’s the perfect choice for apps that pay no mind to a device’s proxy settings but doesn’t work for apps that fail to gain any network traffic.

APP SOLID.

Naturally, our solution offers the ability to scan your app as well as protection and monitoring services. Our full-service app vulnerability analysis can even identify vulnerabilities that may provide hackers with the opportunity for reverse engineering.

Neopwn:

While this program only runs on some Android devices, its ample features -- using a Linux operating system and customer software -- make up for that fact. It was also the first company to release a mobile security auditing distribution service.

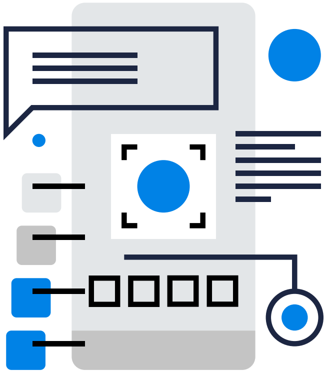
Android Debug Bridge:

Part of the Android Development Kit, this tool lets developers connect to emulators, install programs or debug them with ease. Identifying security vulnerabilities has rarely been this simple, as it deftly explores Android file systems.

HP Enterprise Software:

Supporting nearly every major format, this tool offers a flexibility that many of its contemporaries lack. With it, developers can test security, perform dynamic scans, detect defects within an app and analyze static resources.

In addition to scanning your app for vulnerabilities regularly, we advise you to stay updated on all the security standards that pertain to your industry. Resources like the Open Web Application Security Project (OWASP) can inform you of the latest vulnerabilities out there and guide your coding as well as your regular updates accordingly.



With this knowledge in mind, you can "test" your app's stability and ensure that you're ready for any imminent attacks on your code before they ever occur. As important as having sound security lined up for your app truly is, it's perhaps even more vital to remain vigilant to rising threats. There's much more to mobile app security than simply setting it up and moving on, as we're making abundantly clear.

How to Secure Your App

Securing your app is indeed an active process, but rather than be intimidated by the damage hackers can do, take action. After all, there are many ways in which you can protect your app against attackers. Start with the following:

Encrypt your data:

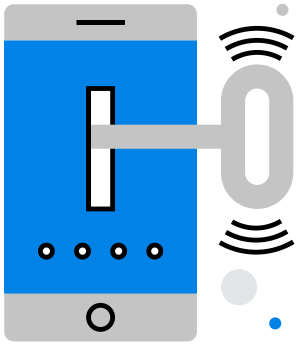
We've already name-dropped encryption as a cornerstone of mobile app security, but be sure to do more than just talk about it. Encrypted data is far more difficult for hackers to crack, making the sensitive information therein far less vulnerable. There's no better way to counteract the many threats your app will face.
In particular, you'll want to ensure that your source code is adequately encrypted (more on that later).

Enable single sign-on:

One tactic that has been steadily growing in popularity is the integrated authentication method commonly known as single sign-on. Using two-factor authentication (typically a password and PIN), this system allows users to easily move from one connected device to another, ensuring that access is limited to authorized users and under the watchful eye of your app's security system at all times.

Application and device management:

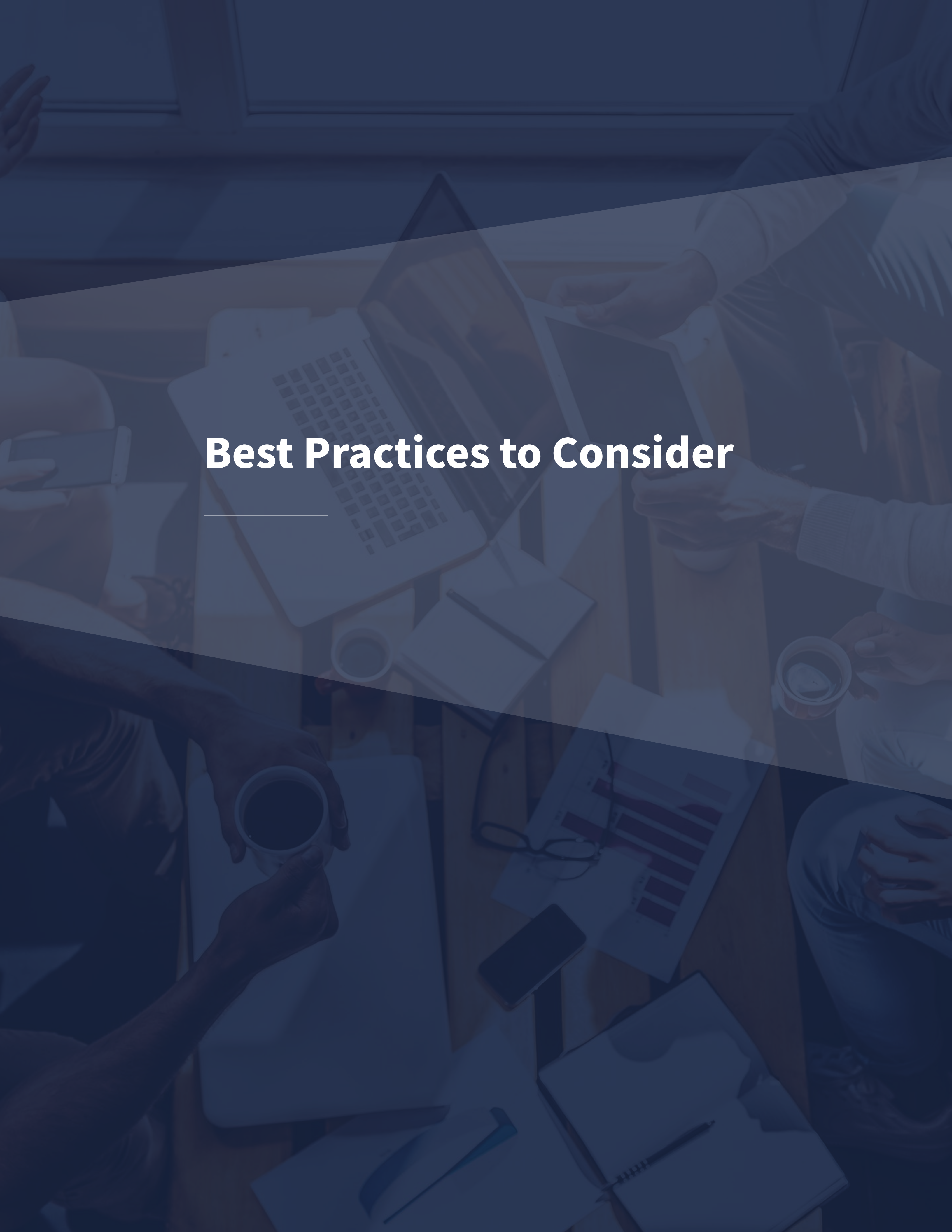
You may have noticed how access is key in keeping your app secure. That also extends to the other mobile apps that may engage with it as well as the devices users may operate to interact with your app. A mobile application management system handles the former, while risk assessment functionality can protect user data or action based on the device used for access.



Protect the Source

Your source code should always be paramount among your security concerns. Because it governs everything your app is and does, even the slightest change to this code can greatly affect your app. As such, hackers are often targeting it directly, hoping to gain access so that they can manipulate your hard work and exploit it. More than simply threatening irreparable damage to your coding, this can set off a chain reaction that can cost you your entire business and earn the mistrust and wrath of your once-loyal users, whose sensitive data will now be made available to the highest bidder.

Regardless of how they gain access, hackers may incorporate weaknesses into your app or even take control of it altogether, often using your trusted brand to dupe consumers into offering up their information for some nefarious reason. As you shape (or re-evaluate) your mobile app security strategy, bear in mind the essential role of your source code and take necessary precautions to keep it encrypted and prevent a terrible fate from befalling your app and your users. If you wait to do until a later date, it may be too late to guard against an impending attack.



Best Practices to Consider

As you move forward with your mobile app security strategy, here are some best practices to guide you in creating the safest, most comprehensive and up-to-date environment for your users:

Develop with security in mind:

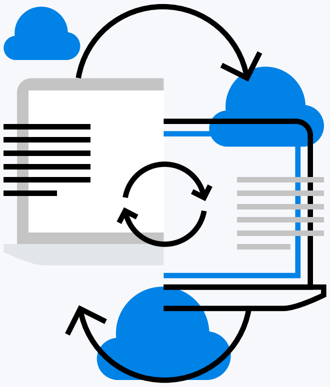
For all the tips and details we've discussed, one point should emerge very clearly: security is most effective when it is considered a key part of your app's design. Though it may be too late to take this approach with your current app(s), be sure to consider it with any subsequent ones you may choose to develop.

Give encryption the attention it deserves:

Since this section serves essentially as a review of key points, we'll take one more chance here to emphasize encryption as a fundamental part of your app's security. Without it, any data your app handles may wind up in the hands of malicious users.

Keep a close eye on data permissions:

Of course, another way to prevent data from falling into the wrong hands is to restrict data access in the first place. When your app interacts with another app, you open up the possibility for data leaks. So only allow this when it's absolutely necessary.



Authenticate and de-authenticate:

Two-factor authentication is a must for your users, since it helps determine their identity with far more accuracy than a traditional password. Every individual who attempts to log in needs to be verified, making it more difficult for hackers to break into your app. Likewise, remember to de-identify user data before it exits your app. In this way, you'll protect your users from any potential harm.

Secure from the application layer:

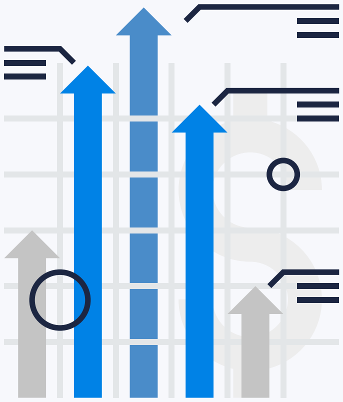
Encrypting data from the transport layer may be important, but don’t neglect the application layer. This ultimately provides greater protection for your users. Just be sure to educate your users regarding the settings they can adjust to customize their experience.

Test, analyze and execute:

Once your app goes live, your security remains a living entity. You still need to continue consistent testing and keep a close eye on analytics. Both will inform you of how your users are interacting with your app as well as what improvements you can make to boost security and performance. Naturally, you’ll want to incorporate these findings into regular updates to ensure that your app is operating at the very highest level.

The Right Solution for Your Needs

With mobile technology expected to only increase in popularity in the coming years, the marketplace has become more and more crowded with app security software options. Still, with so many tools to choose from, it's important that you carefully evaluate the features each one offers. More than anything, you need to ensure that your app receives consistent, around-the-clock coverage across its entire operation.



In addition, such a tool should have the ability to track progress and produce relevant reporting as a result. Only then can you rest assured that your app's security is in good hands and prepared for anything that might occur. Risk prevention and monitoring are the name of the game when it comes to mobile app security. It may seem simple, but this objective often gets lost amid the big picture.

That’s why AppSolid keeps the process as streamlined as possible, consisting of three major components: Scan, Protect and Track. Though the names may give away what part of your app’s security they are concerned with, the intricacies of our system ensure that it runs at the highest level of performance, neutralizing any existing threats before safeguarding against new ones.

Perhaps best of all, the tracking element of our system provides you with real-time coverage of any suspicious activity that might arise, alerting you when and if the time comes. We, of course, realize that AppSolid is but one of many app security software systems out there, but we humbly hope to earn the honor of your business in the near future.

Scan

Analyze security vulnerabilities

Protect

Apply binary protection

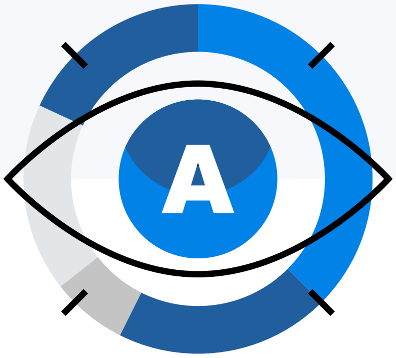
Track

Monitor the real-time security status

Safe or Sorry?

Without mobile app security, your app may be doomed to encounter a damaging attack. In today's world wherein hackers are more determined than ever before, it's bound to happen at some point. After all, the sad reality is that those with malicious intent will always evolve along with technology, and it certainly doesn't appear that mobile apps are going away anytime soon. So, rather than bemoan the necessity of thorough security measures, why not embrace it and ensure that your app is protected from all those who may wish to cause harm. With all the effort you've put in throughout the development process, security is one area which, if overlooked, could jeopardize all you've worked so hard to build. Even if you already have the desire to beef up security, you may not know where to start. That's where we come in.

Since SEWORKS launched AppSolid in 2016, AppSolid has made your app's security its highest priority. We use a simple three-step process to ensure that your app and its users remain shielded from hackers. First, we rapidly (and regularly) scan your app to diagnose any lingering vulnerabilities, and then we apply the binary protection you need to keep dangerous users at bay. Finally, our state-of-the-art system provides real-time monitoring so that you can quickly act whenever any suspicious activity hits your app. Your team and your users deserve the highest level protection on the market, and AppSolid humbly has you covered. Through our effective process and the use of obfuscation -- a practice which conceals your code from hackers -- we offer the complete package you need to bring your mobile app security up to industry standards and beyond.



We know that you take your app's security seriously, and for this very reason, we're offering you the chance to discover what AppSolid can do for yourself. Contact us today to scan your app for free and determine if your data is currently at risk. Every moment you wait presents another opportunity for hackers to strike. Don't leave your app open to attack.

Secure Your App
With AppSolid

Start Now

APP SOLID

help@appsolid.net