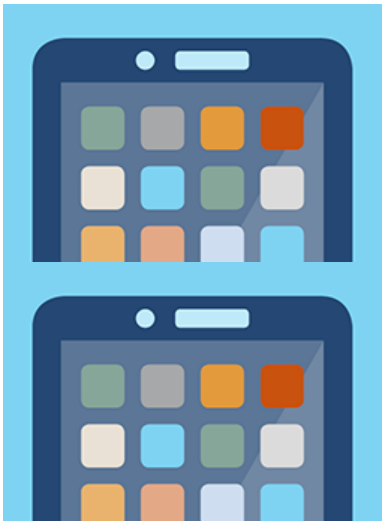
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

App Developers: Start with Security

Tags: spyware and malware | Privacy and Security | Consumer Privacy | Data Security | Tech



More than a thousand new apps are hitting the market each day. In this fast-moving era of entrepreneurship and creativity, is security keeping up? Apps and devices often rely on consumer data — including contact information, photos, and location to name a few — and can be vulnerable to digital snoops, data breaches, and real-world thieves. The Federal Trade Commission (FTC), the nation's consumer protection agency, offers these tips to help developers approach app and software security.

Aim for reasonable data security

There is no checklist for securing all apps. Different apps have different security needs. For example, an alarm clock app that collects little or no data will likely raise fewer security considerations than a location-based social network. Apps that are more complex may rely on remote servers for storing and manipulating users' data, meaning that developers must be familiar with securing software, securing transmissions of data, *and* securing servers. Adding to the challenge: Security threats and best practices evolve quickly.

The FTC expects app developers to adopt and maintain reasonable data security practices and doesn't prescribe a one-size-fits-all approach. This brochure offers a starting point to help you provide a secure experience for your users. If applied thoughtfully and consistently, these tips can help protect you, your users, and the reputation of your app.

Before you start, evaluate the ecosystem

The mobile and Internet of Things ecosystem present developers with both challenges and opportunities. Before getting into the nuts and bolts of data security, consider the landscape:

- App developers can code quickly with the support of powerful software development kits (SDKs). However, a rush to release may result in dangerous security oversights.
- Popular app stores can introduce apps to millions of users, and can lead to overnight popularity. But the bigger the user base and the more sensitive the information, the greater the need for strong security. Is your app ready?
- Ready-made software libraries and cross-platform toolkits can provide a head start in the development process. However, as a developer, you are your app's last line of defense, determining what goes in it and how it performs.
- Mobile and Internet-connected devices offer an array of exciting technologies. GPS receivers, cameras, and sensors let you create a unique experience for users. But threats — like loss, theft, and users who rely on unsecure Wi-Fi networks — raise the security stakes. Balance these features and risks to protect users' personal information and your own business reputation.

Getting your product working and accepted by an app store are two key milestones. But there's a critical third step: Anticipating and preventing potential security glitches.

Tips for app security

Make someone responsible for security.

Your team should include at least one person responsible for considering security at every stage of your app's development. If you're running a solo operation, that person is you. It's easy to assume someone else is handling security — whether that someone is a mobile operating system provider, a device manufacturer, or another member of the development team. It's true that everyone has a role to play, but as the developer, you're the final line of defense.

Take stock of the data you collect and retain.

Don't collect or keep data you don't need. For example, if your photo-editing app doesn't require access to a user's contact info, don't ask for it. Simply put, data you don't collect is data you don't need to worry about protecting. Avoid keeping data longer than you need to. For example, if you offer a location-based mobile game, get rid of the location data when it's no longer relevant.

Understand differences between platforms.

Research the platforms you work with and make sure you enable proper configurations. Each mobile operating system uses different application programming interface (APIs), provides you with different security-related features, and handles permissions its own way. Don't expect that one platform works exactly like another. Do your research and adapt your code accordingly.

Don't rely on a platform alone to protect your users.

Platforms often provide helpful security features. But it's your job to understand those features (and their limitations), implement them properly, and take other measures necessary to protect your users. In addition, while platform-based permissions might be helpful in conveying security information to your customers, they're no substitute for your own effective communication. Talk to your users in your own words.

Generate credentials securely.

If you create credentials for your users (like usernames and passwords), create them securely. For example, a short number string might be an appropriate token for authenticating a user on a game score board, but the same credential wouldn't be appropriate for a social networking app.

Don't store passwords in plaintext.

Don't store passwords in plaintext on your server. Instead, consider using an iterated cryptographic hash function to hash users' passwords and then verify against these hash values. (Your users can simply reset their passwords if they forget.) That way, if your server suffers a data breach, passwords aren't left completely exposed.

Use transit encryption for usernames, passwords, and other important data.

Anytime your app transmits usernames, passwords, API keys, or other types of important data, use transit encryption. Mobile and Internet-connected devices commonly rely on open Wi-Fi access points at coffee shops, airports, and the like — and it's easy for troublemakers to snoop and intercept data.

To protect users, developers often deploy TLS in the form of HTTPS. Consider using HTTPS or another industry-standard method. There's no need to reinvent the wheel. If you use HTTPS, use a digital certificate and ensure your app checks it properly. A no-frills digital certificate from a reputable vendor is inexpensive and helps your customers ensure they're communicating with your servers, and not someone else's. But standards change, so keep an eye on current technologies, and make sure you're using the latest and greatest security features.

Use due diligence on libraries and other third-party code.

Before using someone else's code to build or augment your app, do your research. Does this library or SDK have known security vulnerabilities? Has it been tested in real-world settings? Have other developers reported problems? Third-party libraries can save time, but make sure you stay accountable for your app.

Consider protecting data you store on a user's device.

If your app handles personal information, consider protecting or obscuring the data — for example, by using encryption. Some platforms have special storage schemes for sensitive data like passwords and keys. Use them if they're available. This helps protect your users in the event of viruses, malware, or a lost device.

Protect your servers, too.

If you maintain a server that communicates with your app, take appropriate security measures to protect it. If you rely on a commercial cloud provider, understand the divisions of responsibility for securing and updating software on the server. While some commercial services will monitor and update your servers' security, others leave you in control.

Server security is its own complex topic, so do some research. Take steps to protect yourself from common vulnerabilities, including injection attacks, cross-site scripting, and other threats.

You're not done once you release your app. Stay aware and communicate with your users.

Even after you ship your app, stay involved. New vulnerabilities arise daily, and even the most reputable software libraries require security updates. Follow general and library-specific mailing lists and have a plan for shipping security updates if needed.

Check your inbox, too. User feedback can help you spot and fix security vulnerabilities. When they discover vulnerabilities, researchers often try to resolve the issue with developers before publishing their findings. It's best to be part of that discussion early on.

If you're dealing with financial data, health data, or kids' data, make sure you understand applicable standards and regulations.

If your app deals with kids' data, health data, or financial data, ensure you're complying with relevant rules and regulations, which are more complex. See *Additional Resources* for more detail.

Additional Resources

- Children's Privacy
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Health Breach Notification Rule

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. For free information, visit the BCP Business Center, business.ftc.gov. To file a complaint, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, How to File a Complaint, to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

May 2017

spyware and malware