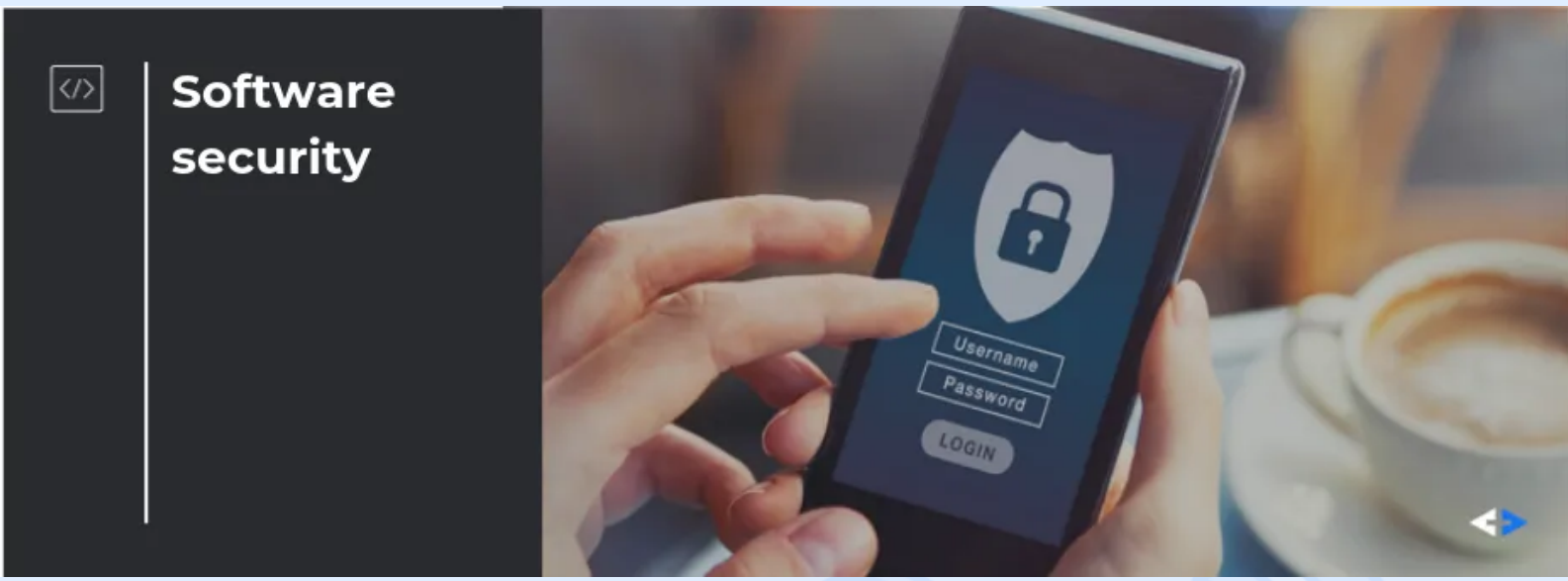
magora



How to Protect an App

App security is becoming a major software development trend in 2019.

In 2018-2019 the number of unauthorised access attempts and the prevalence of app-hacking are significantly increasing along with the growing volume of online purchases and the use of websites and mobile apps for private and business purposes. This disturbing statistic creates a growing demand for the development of more secure technologies, sophisticated authentication algorithms and data encryption methods.

In this article we discuss the key risks your app can face and how to mitigate them.

What is Cybersecurity?

magora

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

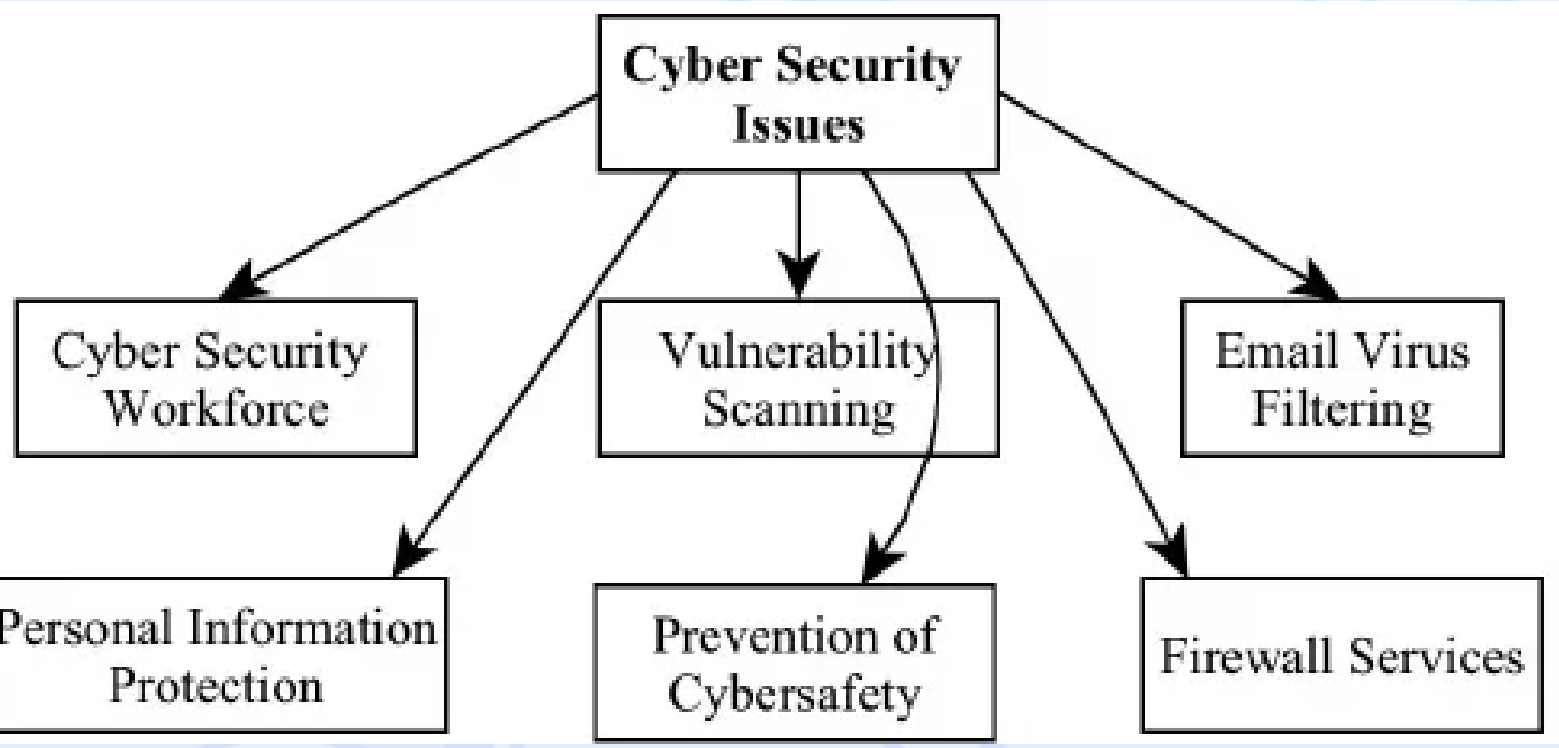
Cybersecurity refers to the implementation of special measures to protect networks, systems and software applications from digital intrusion. Such attacks are aimed at obtaining access to confidential information, its destruction or modification, at soliciting money from users or at disrupting the normal operation of companies.

Professional software development must be implemented in compliance with international standards and security regulations. For the European market additional requirements concerning personal data protection were put in force in May 2018 (the GDPR).

Expert IT agency areas of competence include the following types of software security:

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk



Technology Security

Technology security focuses on technological problems, such as:

- Intrusion detection
- Viruses, worms, crimeware
- Network security
- System hardening
- Engineering and Encryption

Data Security

The main focus of data security is business problems:

- Risk management
- Intellectual property
- Regulatory compliance
- Business / financial integrity
- Industrial espionage
- Forensics and investigations
- Privacy

Strategic Security

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

Profi-developers also take care of critical security problems, such as:

- Intelligence
- Terrorism and cybercrime
- Strategies and tactics
- Nation-state interests
- Politics

App Security: Protect your Data from Cyber Attacks

When developing a mobile app, we take into account the data with which the application operates. The degree of value attached to data varies widely, demanding more sophisticated methods of secrecy to save from disclosure private user information, such as the password to enter the app or personal phone numbers and email addresses. This is especially important in light of the spread of mobile apps in all areas of business, including banking and finance. Below we've collected examples of a variety of cyber attacks which can be divided into several categories, allowing you to understand the key vulnerabilities of your software and how to safeguard them.

The Main Types of Attacks on Software

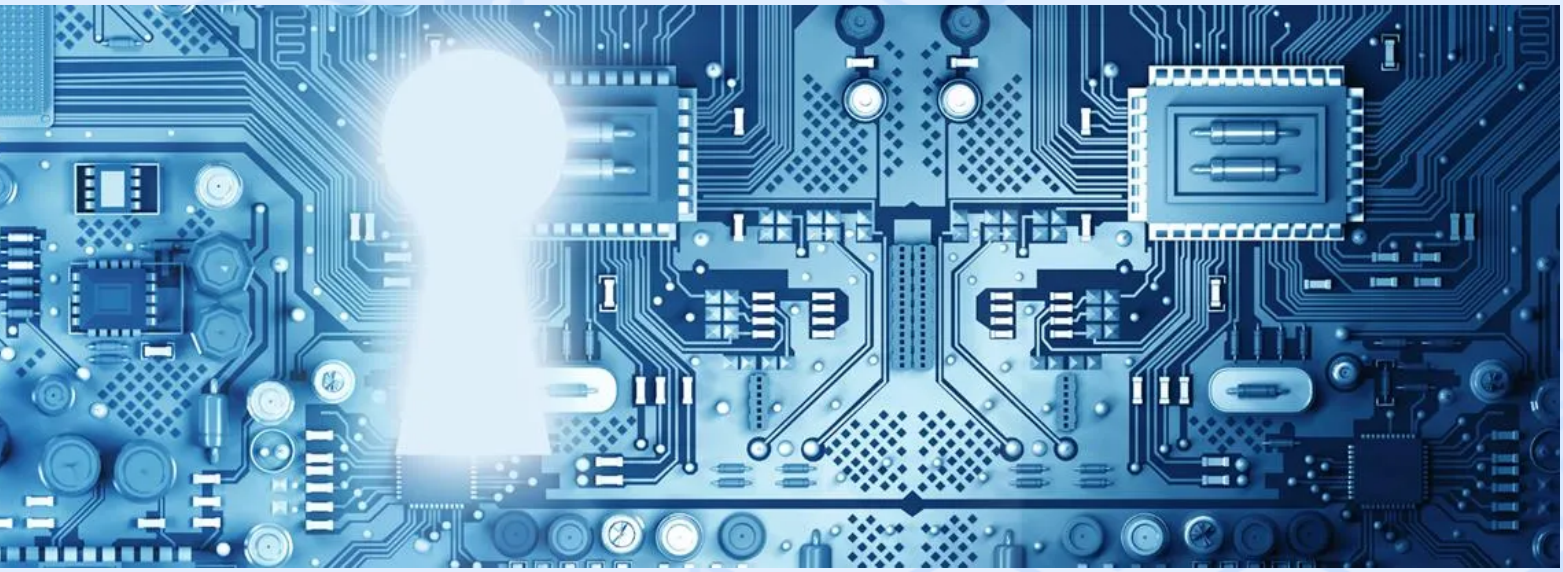
+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

First of all, there are mobile software threats that are always up to date. Read more about them and use a checklist to make sure you have taken all measures to protect your corporate data.

In 2019 software security requires even greater attention thanks to such threats as:

- ***App file decompilation (.apk-files for Android and .ipa-files for Apple iOS) and parsing of locally stored data.*** Protection at this most important level lies entirely on the shoulders of the mobile developer.
- ***MITM-attacks (Interception of data transmitted over the network).*** Most mobile apps are client-server – therefore, they constantly transmit large amounts of data. And although modern web and mobile development is actively completing the transition to the HTTPS communication protocol, we don't rely on a single protection line in the form of a secure communication channel but instead take other measures to guarantee the security of your app.
- ***Device rutting and the attack on the app and algorithms used through external debugging tools.***

How to Develop Secure Mobile Apps



There are several common points for all mobile platforms that our developers at Magora follow during the software and app creation.

User Code Protection

- If an app is protected by a user password (fingerprint scan, PIN code, graphic password, etc.), when it goes into the background, an input window for this security code should be immediately

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

displayed, overlapping the entire screen. This eliminates any opportunity for an attacker to obtain private information in case of theft of the device while the app is still running and in sleep mode.
- Any user code should have a limited number of input attempts, after which, in case of failure, the program should automatically log out (or be completely blocked, depending on the particular application).
- Currently, when using digital codes, it is strongly recommended to apply a code-length restriction of at least 6 digits (more is possible, fewer is not).

Operation of the Client-Server Application

- For client-server apps we recommend using a session mechanism with a limited session lifetime. This will prevent the application from “idling” in an unprotected mode if the user simply forgets to close it and leaves the device freely available. One of the implementation examples of such a mechanism is to obtain the absolute value of the time from the server after passing through the user authorisation procedure (the time and date should show when the session will become inactive). The time and date of the end of the session should not be generated on the device, as this reduces the flexibility and security of the software.
- The client-server application should not make changes to the critical user data in local mode. Any action that requires changes should be synchronised with the server. The only exception to this rule is the user login code, which is set personally by the user and stored in secure local storage.

Working with Dates

- When working with dates important for the operation of the app, such as the time of the session, we never rely on the relative time. That is, the data transmitted from the server should not contain the date in the form of "plus N minutes / hours / days from the current moment". Due to the presence of potentially lengthy delays in data transmission over the network from the mobile app to the server and back, such a synchronisation method will result in too many errors. In addition, an attacker (or simply an unscrupulous user) can simply change the local belt on the device, thus violating the logic of the restrictive mechanisms. It is always necessary to transmit only the absolute time value.
- Absolute values should be transmitted using universal methods of exchanging such information, without reference to the time zone of a specific user device. Most often, the best option is the software behaviour under which the data is displayed to the user in its local time zone but stored and transmitted in a format that is not tied to the time zone. Suitable formats for dates and times are either the universal UNIX timestamp stored in a 64-bit integer signed type variable (UNIX timestamp is the number of seconds since 1st January, 1970), or, in special cases, a string in the full ISO-8601 format with zero time zone. The UNIX time stamp is generally preferred, as it allows us to avoid potential problems and errors concerning the conversion of strings to dates and back on different mobile platforms.

5 Cybersecurity Hints for 2019

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

In custom development we manage to minimise software security risks. Here are our top 5 tips to build your app to be protected:

- **We never blindly trust open source libraries that offer some kind of protection for critical user data.** Exceptions include time-tested libraries and frameworks used to speed up development in large enterprise projects.
- **We don’t use closed-source cryptographic libraries (even paid ones).** Such solutions will not enable you to check how effective this library is, nor how "honest" its protection is (i.e. whether it has a backdoor mechanism to send the "protected" data to any third party).
- **In release builds, logging of data to the system console and unprotected files should be disabled**. We build specific logs for developers, but usually in encrypted form, in order to avoid third-party access to proprietary information that logs may contain.
- **We carry out selection and coordination of the protection level, as well as the list of critical user data in the app, at the earliest design stages.** Mobile sector vulnerabilities can be quite easily excluded from the software, and most often this does not introduce any special additional

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

costs if started at the early stages of development. The post-factum introduction of protective measures into an already running application may well be associated with significant time, effort and cost.

- **We create app design so that the private user information is not displayed in large, bright, well-readable fonts,** without the explicit need for it and a separate user request, in order to exclude the possibility of reading this data from a distance on the device's screen.

And we always recommend regular updates, as malware often attacks outdated software.

Want to know more about software security and malware threats? Read:

1. How a virus can physically destroy a smartphone
2. What iOS security feature has been hacked
3. What SSL/TLS are and why they are not so secure

At Magora we are always ready to answer your questions, implement validation of third party code or provide you with a software or app security audit. Get in touch with our team to create your secured bespoke software.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk