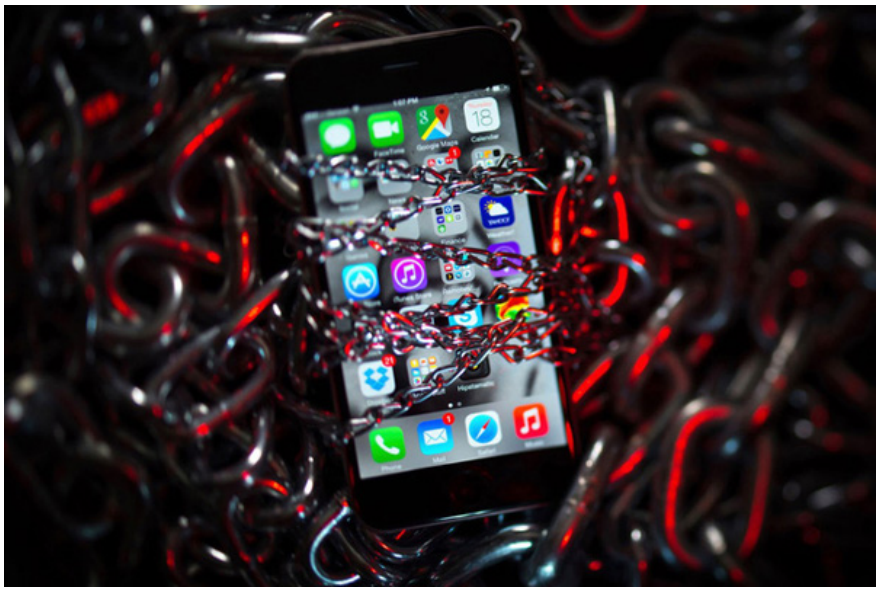
High security but iPhone can still be hacked when accessing malicious websites

Project Zero, a security research group at Google, recently published information that iPhone users are at risk of hacking when accessing a malicious website.

Project Zero, a security research group at Google, recently published information that iPhone users are at risk of being "hacked" when accessing certain malicious websites. According to the announcement, hackers can steal photos, messages and track the location of iPhone users in real time, even accessing the library of passwords stored on the device.

Project Zero said it found that some malicious websites 'servers could take advantage of some previously unpublished software vulnerabilities to silently hack victims' iPhones when they accessed them. If successful, they could secretly implant the tracking code lines into the device.



It is worth noting that websites containing such malware have existed for at least 2 years and attracted thousands of visits from iPhone users every week. Such an attack is called a "haphazard attack" by Google.

Since February 2019, security researchers have found a string of vulnerabilities, including a total of 12 separate security flaws that could affect iOS 10 through iOS 12. Seven of them are related to The browser is built into iPhone and Safari. The remaining five vulnerabilities allow hackers to silently install malicious applications to illegally track iPhone users without their knowledge.

Apple has quickly fixed the above security flaws in iOS 12.1.4 update only 6 days after Google discovered it.

1. iOS 12.4 was cracked after only a few weeks of launch due to the mistake of Apple and an anonymous developer
2. iPhone can be hacked with just a message without requiring user interaction

You finished reading the article "**High security but iPhone can still be hacked when accessing malicious websites**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
