Kaspersky uncovers fraudulent schemes for iPhone pre-order

Following Apple's recent presentation of the company's updates, and the iPhone 12 launch in particular, Kaspersky experts have uncovered dozens of suspicious resources around the world, which allegedly offered to pre-order the new smartphone. In reality, however, there may be many more such resources and schemes.

Photo by Torsten Dettlaff© from Pexels

The websites typically include a ‘call to action’ for the user to leave a prepayment or some personal information. If the victim falls for the scheme, all the data and money go to the scammers. Interestingly, on most of the resources, users were not just offered to place a pre-order, but were also motivated to participate in a win-win lottery promoting that they could win a new iPhone. For this purpose it was necessary for the user to answer some questions, and following that, the user was redirected to the next poll (and so on).

As a result, the victim was redirected to a page where it was necessary to pay a small sum for goods or services of the sponsors of the lottery. After that, the user could allegedly get a new iPhone for free, or the procedure with a redirect could go on forever. In this case, the attackers can probably get certain bonuses for traffic, while collecting a large amount of personal data.

In addition, the experts found another scheme in a popular messenger. After the presentation of the new device, the researchers have detected a blast of messages about a popular sale, which can be used to get the new version of the smartphone for free.

According to fraudsters, you only need to forward such message to 20 contacts or 5 groups. Then you need to click on a link to a phishing website supposedly in order to select the colour of the phone the user has won. To do this, the user is required to enter their data. In this case, the purposes of the attackers may be different: to subscribe to a person for a fee, to access their personal and payment data, to force under various pretexts to transfer money. The danger is that such mobile content is very viral - users often send each other messages with such "actions".

“We'd like to remind users that messages about pre-orders should be checked in reliable sources. At the same time, do not follow the links from suspicious letters or messages in messengers and social networks, as well as participate in suspicious lotteries. It is recommended to install a reliable security solution with actual databases of phishing and spam resources, such as Kaspersky Total Security,” said Tatyana Sidorina, security researcher at Kaspersky.