

ПРЕСС-РЕЛИЗ

Мошенники начали клонировать приложения банков, попавших под санкции

Из-за санкций мобильные приложения некоторых крупных банков исчезли из официальных магазинов приложений. Этим уже воспользовались мошенники. Они разрабатывают фейковые приложения, которые выглядят как настоящие мобильные банки, но на самом деле помогают аферистам получить доступ к персональным данным и деньгам человека.

Преступники распространяют свои приложения самыми разными способами. Иногда они размещают их в официальных магазинах, которые не всегда успевают вовремя отследить фальшивки. Но чаще продвигают их в альтернативных магазинах приложений и на разных сайтах. Ссылки для скачивания распространяют через соцсети, мессенджеры или по электронной почте. На сайтах объявлений уже встречаются предложения купить смартфоны с приложениями пострадавших из-за санкций банков, которые тоже могут оказаться мошенническими.

Если человек загрузит поддельное приложение и введет свои данные, аферисты получат доступ к его настоящему онлайн- или мобильному банку. Это приложение также может оказаться вирусом, с помощью которого преступники взломают и другие мобильные банки пользователя. В результате мошенники могут украсть все деньги со счетов, а также взять кредиты на имя ничего не подозревающего клиента. Человек не только потеряет сбережения, но и останется в долгах.

В таких ситуациях банки не возвращают украденные деньги и не аннулируют кредитные договоры. Ведь клиент сам установил поддельное приложение и открыл мошенникам доступ к своему личному кабинету.

Что делать, если банковское приложение вашего банка пропало из официального магазина:

- Когда официальная программа уже установлена, не надо ничего удалять – просто продолжайте ей пользоваться. Основные функции приложения будут работать. Ограничения действуют только на международные переводы, так как банк попал под санкции.

- Если у вас нет приложения или оно перестало работать из-за технического сбоя, используйте вместо него онлайн-банк. В браузере введите официальный сайт банка и зайдите в свой личный кабинет. Главное – внимательно проверяйте адрес банка, чтобы не угодить на поддельную страницу. Некоторые банки предлагают скачать приложение напрямую со своего официального сайта.

- Никогда не скачивайте программы с неизвестных сайтов, из неофициальных магазинов приложений или переходя по ссылкам, которые вам прислали незнакомцы.

- Если вы купили смартфон или планшет с рук, не пользуйтесь уже установленными приложениями – они могут оказаться поддельными.

Больше советов, как уберечься от киберпреступников и актуальные новости, вы найдете на сайте **fincult.info**

Источник: fincult.info

