«Посмотри фото и скачай вирус»

Константин, Истра

Фантазия у мошенников по ходу совсем иссякла. Вчера пришло сообщение от бывшего однокурсника в телеге: «Привет! Это ты на фотке?». А с ним файл с названием «Фото». Вот только расширение у него apk — как у мобильного приложения. И весит почти 10 Мб.

Это мы уже проходили: лет десять назад в соцсетях гуляли рассылки «Посмотрел фото с тусы, ты там так отжигаешь» и все в таком духе. Но если скачать эти типа фотки, то загрузишь себе на комп вирус.

Понятное дело, сейчас я ничего открывать не стал. Парню этому позвонил, предупредил про спам от него. Он объяснил, как его взломали: с ним связались от имени службы поддержки пользователей телеграма. Якобы от него поступила заявка на удаление аккаунта, а чтобы ее отменить, нужно было назвать код из сообщения. Ну он сказал, и вот теперь все его знакомые получили какие-то явно опасные файлы. Надеюсь, никто на эти старые грабли не наступит.

Совет эксперта по противодействию мошенничеству:

Аферисты не только выдумывают новые схемы, иногда они просто видоизменяют хорошо работавшие старые. В прошлом мошенники рассылали интригующие «фото с вечеринки» с расширением exe, zip или rar, которые оказывались вредоносной программой для компьютера или ноутбука.

Теперь преступники снова решили сыграть на любопытстве людей. Но сейчас общение перешло в мессенджеры на мобильных устройствах, так что мошенники адаптировали схему и отправляют файлы типа apk. Это программы установки приложений для гаджетов на базе Android.

Если скачать и открыть такой файл, то на смартфон или планшет загрузится вирус, который даст мошенникам полный доступ к устройству. В том числе к банковским приложениям.

У настоящих изображений название файла чаще всего заканчивается на jpg, gif, tiff или png, но никогда — на apk. Так что не стоит открывать непонятные файлы с таким расширением.

Гораздо выше вероятность, что человек заинтересуется и откроет опасный файл, если сообщение пришло от знакомого. Поэтому мошенники разными способами уводят чужие аккаунты. К примеру, выдают себя за представителей техподдержки мессенджера и предлагают обновить программу, пройти повторную верификацию или отменить удаление профиля.

Чтобы обезопасить от взлома свой аккаунт в телеграм, других мессенджерах и соцсетях, нужно соблюдать правила кибергигиены:

- не использовать простые и одинаковые пароли;
- настроить двухфакторную идентификацию (например, когда для входа нужно ввести и пароль, и код из СМС);
- не передавать никому пароль и проверочный код для входа в аккаунт.