«Посмотри фото и скачай вирус»

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. Больше о том, как защитить устройство от вирусов, вы узнаете из текстов «Мифы и правда о безопасности мобильных приложений» и «Как защитить свои гаджеты от мошенников».

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. Под этими предлогами они убеждают пользователя ввести данные аккаунта на фишинговой странице или выведывают код для входа в профиль.

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.