Поддельные домовые чаты и фишинговые ссылки на онлайн-уроки о новых схемах обмана

В России мошенники используют новые схемы для хищения персональных данных и реквизитов от электронных почт. Зачастую, злоумышленники перенимают опыт из соседних государств, из-за чего велика вероятность того, что и в Беларуси появятся подобные случаи обмана. Сейчас мы расскажем каким способом интернет-мошенники хотят завладеть вашими личными данными.

Аферисты подделывают чаты многоквартирных домов и подъездов и переманивают туда владельцев квартир и жильцов под видом настоящего чата. Затем, от имени старших по дому и представителей управляющей компании размещают объявления и уведомления, в которых просят жертв предоставить и м персональные данные.

Во втором случае, мошенники под видом учащихся образовательных заведений записываются на онлайн-занятия к репетиторам. После того как преподаватель отправляет ссылку на занятие, аферисты под различными предлогами, например, якобы имея проблемы с подключением к

Интернету, присылают свою, уже фишинговую ссылку. Жертва переходит по ссылке на сайт-подделку, где, ничего не подозревая, вводит данные д л я входа в приложение д л я дистанционного проведения занятия по видеосвязи.

Зачастую н а таких поддельных сайтах просят авторизоваться, например, через Google-аккаунт. Жертва вводит реквизиты для входа - фактически отдавая их мошенникам, которые потом с помощью этих данных получают доступ ко всем остальным ресурсам, зарегистрированным под указанной почтой.

Сотрудники милиции рекомендуют гражданам быть бдительными и соблюдать меры безопасного общения в интернете.

Будьте бдительны, чтобы не установить мобильное приложение с «сюрпризом»

В соседних государствах фиксируется рост рассылок вредоносных файлов под различными предлогами. Наиболее актуальный пример - это «кадры с места ДТП». Такие сообщения сегодня распространяются преимущественно в мессенджере Telegram, в том числе через домовые, родительские и другие крупные чаты.

Схема работает следующим образом: в общий чат отправляют эмоциональное сообщение о якобы произошедшей аварии с участием знакомых людей и прикрепляют ссылку на группу с громким названием (например, «ДТП.Происшествия.18+»). В группе размещено несколько новостей и файл с записью происшествия, который по факту является вредоносной программой для Android.

Напоминаем владельцам Android, как распознать вредоносные APK-файлы и как защититься от них.

В операционной системе Android любое приложение будет иметь формат .apk (Android Package Kit). APK-файл — это архив, внутри которого находятся все компоненты приложения.

Мошенники могут использовать разные APK-файлы для своих целей. Так, фишинговые APK-файлы маскируются под легальные приложения, которые после установки крадут пароли и платежные данные. Вирусные файлы получают доступ к SMS и банковским приложениям, подписывают жертву на платные услуги. Шпионские файлы скрыто записывают звонки, отслеживают местоположение и копируют переписки. APK-файлы также могут работать как бэкдоры, то есть позволять хакерам удаленно управлять устройством.

Android использует несколько механизмов для защиты пользователей от вредоносных APK. В первую очередь это встроенная система безопасности Google Play Protect, которая анализирует файлы перед установкой. Она работает при загрузке приложения и проверяет его цифровую подпись и поведенческий код. Однако часто мошенники присылают вредоносный APK жертвам в мессенджере и под разными предлогами убеждают установить файл.

Убедительно реуомендуем скачивать приложения только из проверенных источников (Google Play, Galaxy Store, Huawei AppGallery).

Сотрудники милиции рекомендуют гражданам быть бдительными и соблюдать меры безопасного общения в интернете.

Декларирование доходов»: как не попасть на уловку мошенников?

Хищение денежных средств по-прежнему остается одной из самых распространенных схем обмана доверчивых граждан. Под предлогом «защиты» сбережений злоумышленники предлагают их декларировать. Что же происходит в это время на самом деле?

Схема проста: мошенники звонят посредством мессенджеров и представляются госслужащими, сообщая, что на имя потенциальной жертвы прямо сейчас пытаются оформить несколько кредитов. Для «спасения» своих денежных средств и содействия правоохранителям граждан убеждают, что все сбережения необходимо срочно переписать и задекларировать, передав курьеру в указанном злоумышленниками месте или перевести на «безопасный» счет.

Доверчивые граждане поддаются панике и попадают на уловку мошенников. Так, 66-летняя жительница областного центра, поверив лжесотруднику КГБ передала курьеру ювелирные изделия из цветных металлов (золото и серебро) на общую сумму 45 000 рублей. А еще одна Могилевчанка, 68-летняя пенсионерка, поверив злоумышленникам по такой же схеме, лишилась около 50 000 рублей. Будьте бдительны и следуйте простым правилам:

- представители государственных органов (сотрудники милиции, КГБ, КГК и др.) не звонят в мессенджерах и не используют номера иностранных операторов;
- если вам поступил звонок с неизвестного номера, а собеседник представляется сотрудником правоохранительных органов/иных госструктур, уточните его должность (специальное звание, подразделение). Прервите разговор и обратитесь в ведомство/ официальный контакт центр организации, сотрудником которого представляется звонивший для проверки информации о его личности;
- не передавайте незнакомцем никаких денежных средств.

Как не стать жертвой туристических мошенников

С каждым годом мошенники в сфере туризма становятся все более изобретательными. Они придумывают новые схемы обмана граждан, многие из которых собирают деньги или берут кредиты на долгожданный отдых.

К сожалению, в Могилевской области все чаще фиксируются случаи, когда доверчивые люди, найдя относительно недорогой по стоимости туристический тур и поверив в выгодное предложение, лишились своих денег.

По словам начальника управления по противодействию киберпреступности УВД Романа Романенко, схема обмана проста. Мошенники в социальных сетях регистрируют аккаунт, зачастую созвучный с известным туроператором. На странице выкладывают весьма заманчивое предложение: «Отдых в Турции по самым низким ценам», «Горящие туры» и тому подобное. Отзывы о поездке, которые размещаются ниже, являются фальшивыми, а число подписчиков - накрученным.

При покупке туристических путевок необходимо опасаться компаний с «ударными скидками» и «выгодными ценами». Отсюда простое правило: при выборе туров не следует обольщаться слишком высокими скидками.

Кроме того, зачастую все общение между клиентом и «турфирмой» происходит в социальных сетях или в мессенджере. Прежде чем подписывать договор об оказании услуг или направлять предоплату, попросите у представителя турагентства номер телефона для связи, а также уточните адрес местонахождения самого офиса для того, чтобы его посетить и вживую пообщаться, уточнив все интересующие вас вопросы. Только после этого следует рассматривать вопрос о бронировании и приобретении тура. Запомните, если действует мошенник, то он никогда вживую с вами не станет встречаться, объясняя это различными причинами: занятость, слишком большой поток клиентов, акция на тур действует только сегодня и так далее.

На минувшей неделе Следственным Комитетом возбуждено уголовное дело по ч. 1 ст. 209 Уголовного кодекса Республики Беларусь по заявлению 60-летней бобруйчанки о том, что неизвестный в социальной сети «Instagram» на сайте под предлогом оплаты тура в Турцию завладел 3350 рублями,

переведенными на карт-счет неустановленного банка. Также в Турцию не сможет полететь 34-летний могилевчанин: в аккаунтах социальной сети «Instagram» и мессенджера «Telegram» под предлогом оформления тура он перевел мошеннику почти 2700 рублей.

Чтобы не стать жертвой злоумышленников, управление по противодействию киберпреступности криминальной милиции УВД рекомендует: никогда не перечисляйте деньги незнакомым людям в интернете и с большой настороженностью относитесь к гражданам (организациям), предлагающим туристический тур ниже рыночной стоимости.

Вишинг под прикрытием: как не поддаваться панике и сохранить сбережения

Будьте скептичны к неожиданным звонкам

Если вы получаете звонок от незнакомого номера, особенно если звонящий представляется сотрудником банка или другой организации, будьте настороже. Настоящие организации не запрашивают личные данные по телефону.

Не сообщайте личные данные

Никогда не разглашайте по телефону свои личные данные, включая номер паспорта, банковские реквизиты, PIN-коды или коды подтверждения из SMS. Это - база.

Проверяйте информацию

Если вам звонят якобы из МТС, Белтелеком, Энергосбыта или другой организации, не продолжайте разговор. Перезвоните в организацию самостоятельно, используя официальный номер телефона, указанный на их сайте или в документах.

Не поддавайтесь давлению

Мошенники часто создают ощущение срочности или угрозы, чтобы заставить вас действовать быстро. Оставайтесь спокойными и не принимайте решения в спешке.

Обновляйте программное обеспечение

Убедитесь, что ваше устройство и все приложения на нем обновлены, чтобы защитить себя от известных уязвимостей.

Сообщайте о мошенниках

Если вы стали жертвой, сообщите об этом в правоохранительные органы. Это поможет предотвратить мошенничество в будущем.

Обучайте родных и близких

Расскажите о способах мошенничества своим друзьям и семье, особенно пожилым людям, которые могут быть более уязвимы.