БЕЗОПАСНЫЙ ИНТЕРНЕТ

КАК ЗАЩИТИТЬ СВОИ СБЕРЕЖЕНИЯ В ВИРТУАЛЬНОМ МИРЕ

МОШЕННИКИ В КИБЕРПРОСТРАНСТВЕ

Все чаще мошенники для получения доступа к конфиденциальной информации не взламывают устройства, а выманивают нужную информацию, используя Ваши эмоции. Злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта и, проигрывая различные опасные ситуации, психологически воздействует на собеседника, чтобы тот самостоятельно сообщил все интересующие мошенника данные.

КАК НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан

2. У банков нет совместных контактных центров и служб безопасности, переключение между ними невозможно

3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка - это повод уточнить ее достоверность и перезвонить в Банк

4. Работники Банка никогда не просят озвучить смс-код, логин или пароль для входа в систему дистанционного банковского обслуживания

5. Никому и никогда не сообщайте данные своей карточки и всегда держите ее в поле зрения при совершении платежей

6. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания(интернет-банкинг), а также для подтверждения платежей

7. Используйте только официальный сайт Банка для входа в систему Интернет-банкинга или официальное мобильное приложение

8. Обязательно подключите 3D-secure и смс-оповещение

9. В случае выявления действий по карточке, которые вами не совершались, необходимо оперативно обратится в Банк или самостоятельно заблокировать карточку в системе дистанционного банковского обслуживания

САМЫЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСТВА СЕЙЧАС

Звонок из банка

Фишинг

Потенциальный покупатель

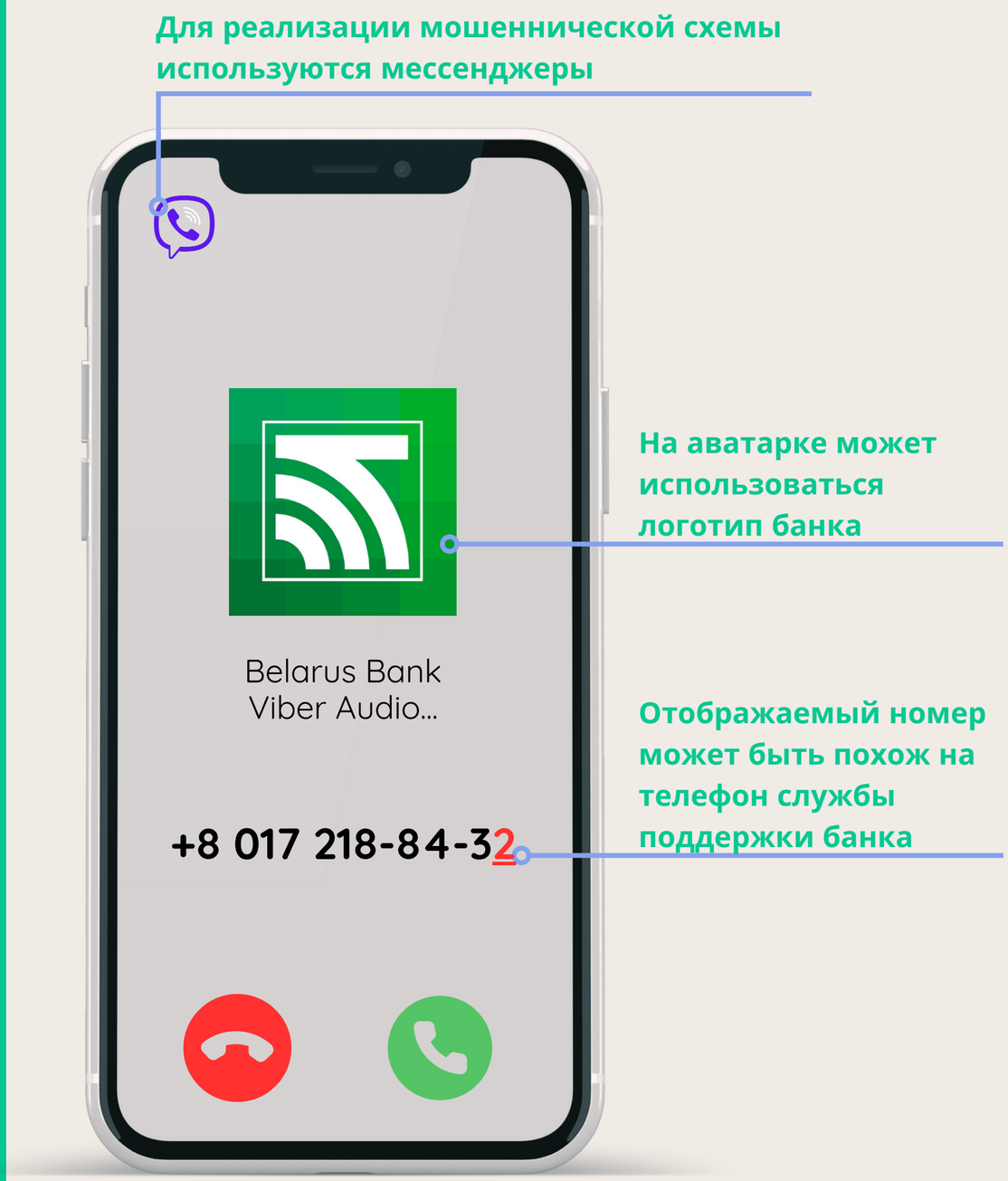
Сообщения в социальных сетях

Розыгрыши/ раздачи/ опросы

«ЗВОНОК ИЗ БАНКА»

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя». Он просит у вас конфиденциальные данные.



НИКОМУ НЕ СООБЩАЙТЕ СВОИ ЛИЧНЫЕ ДАННЫЕ, ДАННЫЕ КАРТ, ЗАЩИТНЫЕ КОДЫ, КОДЫ ИЗ SMS! ЕСЛИ С КАРТОЙ, ДЕЙСТВИТЕЛЬНО, ПРОИСХОДЯТ МОШЕННИЧЕСКИЕ ОПЕРАЦИИ, БАНК САМ МОЖЕТ ЕЕ ЗАБЛОКИРОВАТЬ!

ПОТЕНЦИАЛЬНЫЙ ПОКУПАТЕЛЬ

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания. Для проверки поступления перевода мошенник направляет вам ссылку или QR-код на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ. ДЛЯ ИНТЕРНЕТ-БАНКИНГА ИСПОЛЬЗУЙТЕ ТОЛЬКО ОФИЦИАЛЬНЫЙ САЙТ БАНКА ИЛИ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ. ВНИМАТЕЛЬНО ИЗУЧИТЕ САЙТ, НА КОТОРОМ ВВОДИТЕ ЛИЧНЫЕ ДАННЫЕ. ЗАПОМНИТЕ! ДЛЯ ПОЛУЧЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ НЕТ НЕОБХОДИМОСТИ ВВОДИТЬ СРОК ДЕЙСТВИЯ КАРТЫ И CVV-КОД.

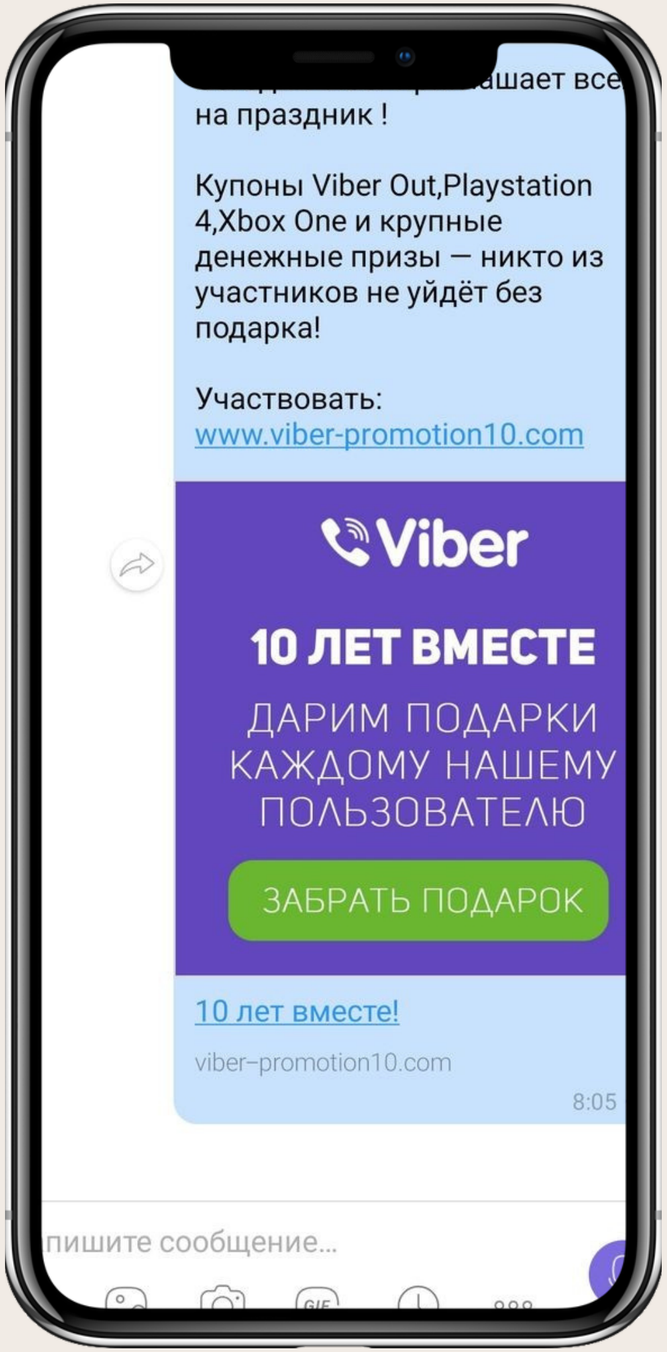
«СООБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ»

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям. Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

ПРИ ПОЛУЧЕНИИ СОМНИТЕЛЬНОГО СООБЩЕНИЯ ИЛИ МАЛЕЙШЕЙ НЕУВЕРЕННОСТИ В ТОМ, ЧТО ВЫ ДЕЙСТВИТЕЛЬНО ОБЩАЕТЕСЬ С ВЛАДЕЛЬЦЕМ СТРАНИЧКИ, ПОЗВОНИТЕ ЕМУ

РОЗЫГРЫШИ/РАЗДАЧИ/ ОПРОСЫ ОТ БАНКА ИЛИ ИНЫХ ОРГАНИЗАЦИЙ

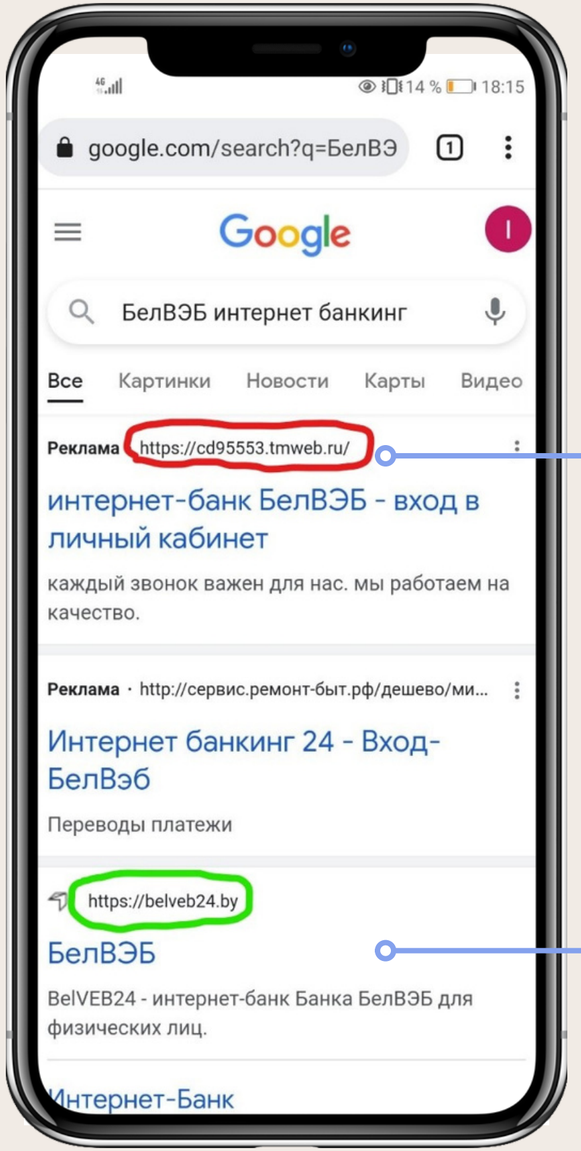
Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе/розыгрыше/раздаче призов от имени Банка. Организатор обещает денежное вознаграждение. Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего – ввести данные Вашей банковской карты. Данный вид мошенничества очень разнообразен и ограничивается только воображением мошенников.



ПОСЕТИТЕ ОФИЦИАЛЬНУЮ СТРАНИЦУ ОРГАНИЗАЦИИ ИЛИ ПОЗВОНИТЕ В КОНТАКТ-ЦЕНТР ДЛЯ ПРОВЕРКИ НАЛИЧИЯ АКЦИИ, РОЗЫГРЫША ИЛИ ОПРОСА

ФИШИНГ

Если Вы используете «Интернет-банкинг», Вам необходимо удостовериться в подлинности веб-ссылки, предназначенной для авторизации на интернет-сайте банка. Так как кибермошенники временно размещают в сети Интернет веб-ссылки, которые ведут на поддельные (фишинговые) веб-сайты, внешне не отличающиеся от оригинальных. В случае перехода на поддельный веб-сайт, то киберпреступники получат доступ к Вашему интернет-банкингу, а находящиеся на банковском счету денежные средства будут похищены. Также Вам не следует переходить по ссылкам, которые Вы получили от неизвестных людей в социальных сетях или мессенджерах.



Пример «фишинговой» ссылки на интернет-банкинг

Подлинная ссылка на веб-сайт интернет-банкинга «Банк БелВЭБ»

ИСПОЛЬЗУЙТЕ СПЕЦИАЛЬНЫЕ ПРИЛОЖЕНИЯ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ «МОБИЛЬНЫЙ БАНКИНГ», КОТОРЫЕ ДОСТУПНЫ ДЛЯ СКАЧИВАНИЯ В GOOGLE PLAY MARKET (ДЛЯ ANDROID) ИЛИ APP STORE (ДЛЯ IOS)

КТО ТАКИЕ ДРОПЫ

Дропы помогают преступникам «отмывать» нелегально полученные деньги. Дроп или «денежный мул» – этот тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу следствия. Дроп не всегда осознает, что вовлечет в преступную схему. Мошенники часто маскируют свои действия под «легальный бизнес».

КАК ОТЛИЧИТЬ ПРЕДЛОЖЕНИЕ СТАТЬ ДРОПОМ

*

Объявления о вербовке дропом могут быть замаскированы под предложения о работе от реальных компаний

01.

В описании работы указано, что необходимо переводить деньги

02.

Не описаны конкретные профессиональные требования к соискателю работы

03.

Отсутствуют требования относительно образования и уже имеющегося опыта работы соискателя

04.

Работа предполагает только онлайн-взаимодействие с работодателем

05.

Предложение о работе чрезвычайно выгодное

СТ. 222 УК РБ. ИЗГОТОВЛЕНИЕ ЛИБО СБЫТ ПОДДЕЛЬНЫХ ПЛАТЕЖНЫХ СРЕДСТВ. СТ. 212 УК РБ. ХИЩЕНИЕ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Ответственность за изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, предусмотрена ст. 222 УК Республики Беларусь.