ВТБ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПОВСЕДНЕВНОЙ ЖИЗНИ

ПРАВИЛА ЗАЩИТЫ ЛИЧНОГО УСТРОЙСТВА

Каждый день в своей жизни мы используем компьютеры, ноутбуки, планшеты, телефоны и другие устройства. Поэтому их потеря, кража или взлом могут иметь серьезные последствия.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Используйте только лицензионное ПО и ОС из официальных, надежных источников

ПОЛНАЯ ЗАЩИТА

Поставьте автоматическую блокировку экрана и защитите свое устройство паролем

АНТИВИРУС

Используйте проверенный антивирус. Настройте его на автоматическое обновление

БЕЗОПАСНОСТЬ УСТРОЙСТВ

Не оставляйте свое устройство без присмотра в публичных местах

РЕЗЕРВНОЕ КОПИРОВАНИЕ

В случае, если какая-то информация повредится, ее можно восстановить из резервной копии

КОНФИДЕНЦИАЛЬНОСТЬ

Следите за тем, чтобы никто не увидел конфиденциальную информацию с экрана вашего устройства

ПОДДЕЛЬНЫЕ ПРИЛОЖЕНИЯ

Создаются злоумышленниками, которые имитируют официальные приложения магазинов и банков. Они могут быть загружены с сомнительных источников или даже с официальных магазинов, например, Google Play, App Store, RuStore и др.

ОФИЦИАЛЬНЫЕ МАГАЗИНЫ

Загружайте приложения только из официальных источников, у которых есть проверка безопасности

ЛИЧНАЯ ИНФОРМАЦИЯ

Никогда не вводите личную информацию, если не уверены в безопасности приложения

ОТЗЫВЫ ПОЛЬЗОВАТЕЛЕЙ

Отрицательные отзывы признак того, что приложение поддельное

ИСПОЛЬЗУЙТЕ АНТИВИРУС

загружайте приложения только на устройства, которым вы доверяете и оно имеет антивирусное программное обеспечение

СВОЕВРЕМЕННО ОБНОВЛЕНИЕ

Обновления ПО часто содержат исправления уязвимостей, которые могут быть использованы злоумышленниками

ПРИЛОЖЕНИЯ БАНКА

Загружайте приложения Банка только по ссылке с официального сайта

Ответственность за безопасность устройства клиента лежит на самом клиенте. Банк не вмешивается в настройку клиентских устройств.

ФИШИНГ

Это атака, которую злоумышленники используют для получения доступа к вашей личной информации, такой как пароли, номера кредитных карт и другие конфиденциальные данные.

КАК РАСПОЗНАТЬ ФИШИНГОВОЕ СООБЩЕНИЕ:

- ✓ Общие или неофициальные приветствия
- ✓ Запрос личной информации
- ✓ Некорректная грамматика
- ✓ Неожиданные сообщения
- ✓ Срочность
- ✓ Предложение, от которого трудно отказаться
- ✓ Подозрительный домен

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА:

- ✓ Будьте в курсе новых методов фишинга
- ✓ Не отправляйте свои учетные данные
- ✓ Не нажимайте на подозрительные кнопки и ссылки
- ✓ Регулярно проверяйте учетные записи
- ✓ Используйте надежное решение для защиты от фишинга

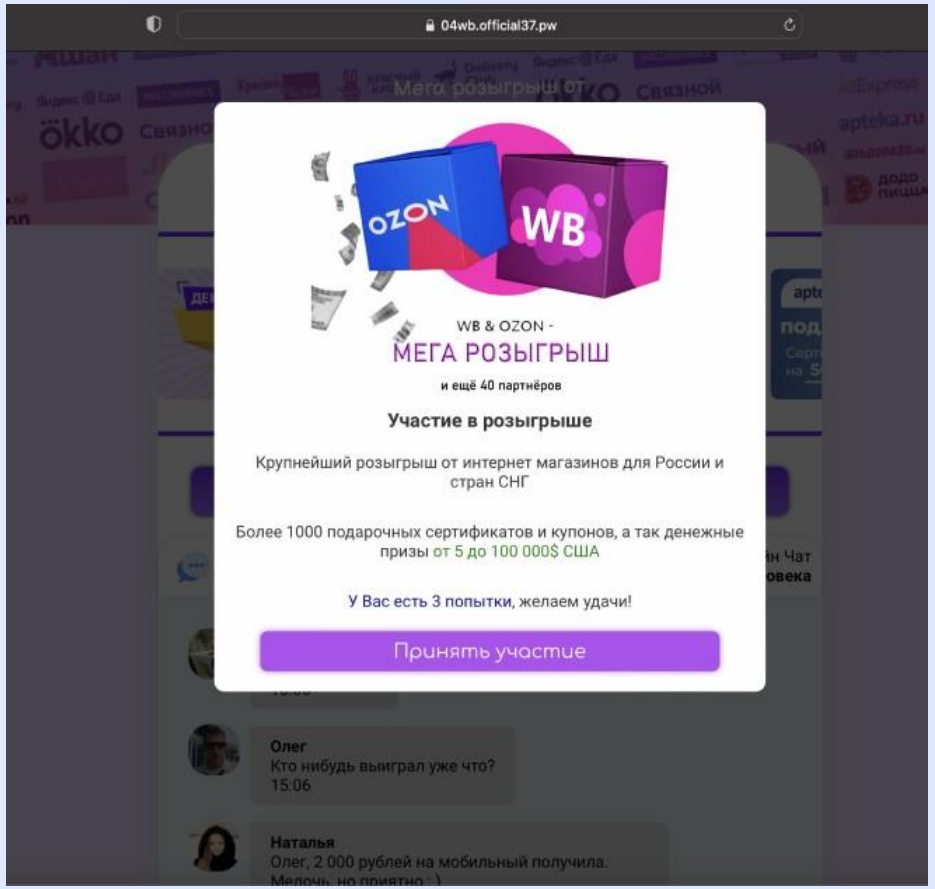
КАК ОПРЕДЕЛИТЬ ФИШИНГОВЫЙ САЙТ

Озон Москва интернет магазин каталог товаров...
ozkatalog.ru › moskva.html •••
Озон Москва. Интернет магазин **Озон Москва** — ознакомьтесь с представленным на официальном сайте каталогом товаров, а также действующими ценами и проводимыми акциями, чтобы получить максимальную... Читать ещё

Госуслуги Личный Кабинет - вход по номеру телефона...
gosuslugi-new.ru •••
...ограниченным количеством **государственных услуг**, подтверждение личности для которых не ... **Госуслуги** — войти в личный кабинет по номеру телефона или почте. Читать ещё

Это подключение не защищено

Этот веб-сайт может имитировать «123.123.123.123» с целью кражи Вашей личной и корпоративной информации. Закройте эту страницу.



DEEPFAKE (дипфейки)

фотографии и видеоролики, где лицо и/или тело одного человека изменены с помощью цифровых технологий так, чтобы он был похож на другого. При этом сохраняется внешность, мимика и освещение. Дипфейки представляют собой серьезную угрозу, так как подобного рода контент является информационной атакой.

ПОДМЕНА ЛИЦА

Лицо одного человека «накладывается» на лицо другого в видео.

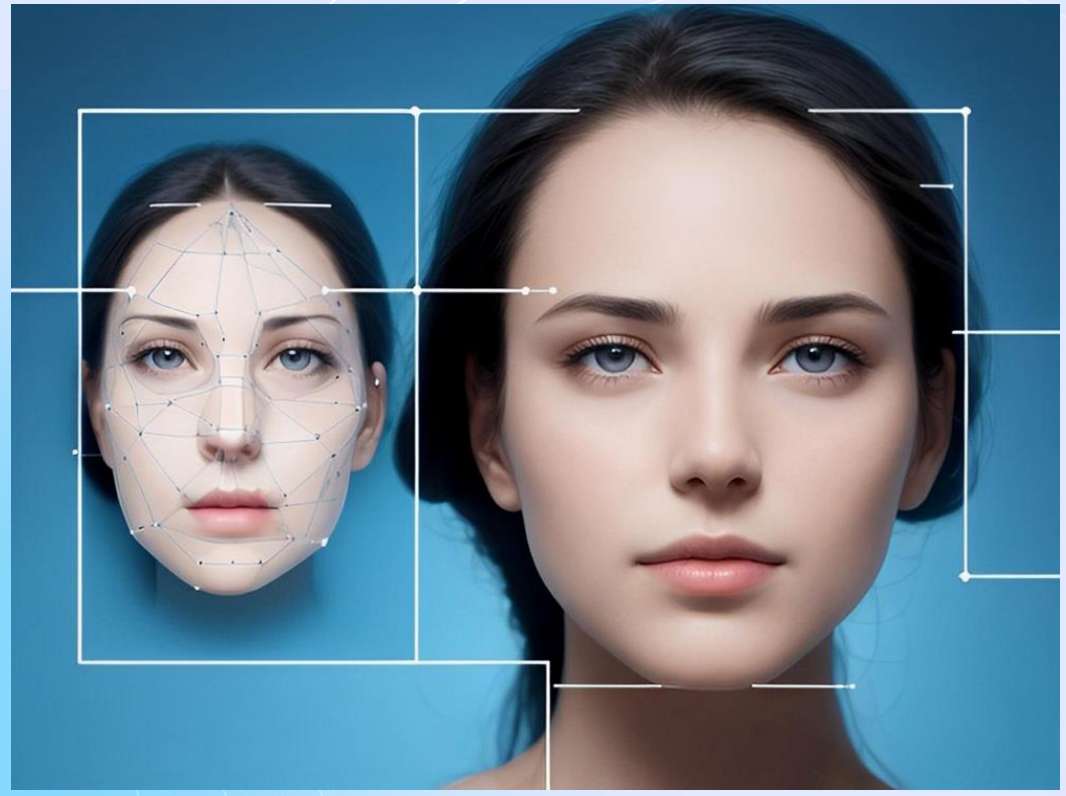
ПОДДЕЛЬНАЯ РЕЧЬ

Синтез речи на основе голоса реального человека.

ПОЛНОСТЬЮ СГЕНЕРИРОВАННОЕ ВИДЕО

С подменным лицом и с синтезированной речью.

ГЛАВНЫЕ ПРИЗНАКИ ПОДДЕЛКИ:



НЕЕСТЕСТВЕННОСТЬ

01 Слишком гладкое лицо и/или волосы, необычные тени на скулах, бессвязная мимика, движение губ не совсем соответствует словам, которые произносит персонаж ролика.

КОНТЕКСТ

02 Если на видео делают провокационные заявления или с агрессией обсуждают актуальные в обществе темы, то отнеситесь к ролику критически.

РЕЧЬ

03 Пользователя должно насторожить отсутствие пауз, необычное колебание записи вверх-вниз, полное отсутствие фонового шума и общий эффект роботизированного голоса.

Голосовой дипфейк выдает неестественная монотонность речи. Именно эта особенность может помочь распознать звонок или сообщение от мошенников.

КАК ЗАЩИТИТЬ СВОЙ КОНТЕНТ ОТ РИСКА СОЗДАНИЯ ДИПФЕЙКА

Технология создания дипфейков уже не исчезнет, её нельзя запретить или технически ограничить. Поэтому лучшая защита — соблюдение правил безопасности.

1. Минимизируйте загрузку своих фото и видео в соцсети и сторонние сервисы (или хотя бы ограничьте доступ к ним).

2. Проинформируйте коллег и членов семьи о том, как устроены дипфейки и с какими потенциальными рисками они связаны.

3. Если возникли сомнения, что перед вами дипфейк – используйте второй канал связи для проверки информации.

4. Чтобы подтвердить личность собеседника, спросите его о каком-либо факте, который известен только ему и вам.

5. Соблюдайте базовые правила кибербезопасности: надёжное хранение паролей, защиту данных, защиту от вредоносного ПО, резервное копирование и другие.

ПАРОЛИ

Использование надежного пароля может значительно снизить риск утечки конфиденциальных данных и предотвратить несанкционированный доступ к вашим учетным записям и личным данным.

ДЛИНА ПАРОЛЯ

- 0000
- 000000000000

ИСПОЛЬЗОВАНИЕ РАЗНЫХ СИМВОЛОВ

- 01234
- $0tRudn1K_3#

НЕ ИСПОЛЬЗУЙТЕ ЛИЧНУЮ ИНФОРМАЦИЮ

- 10041980
- IVAN1980

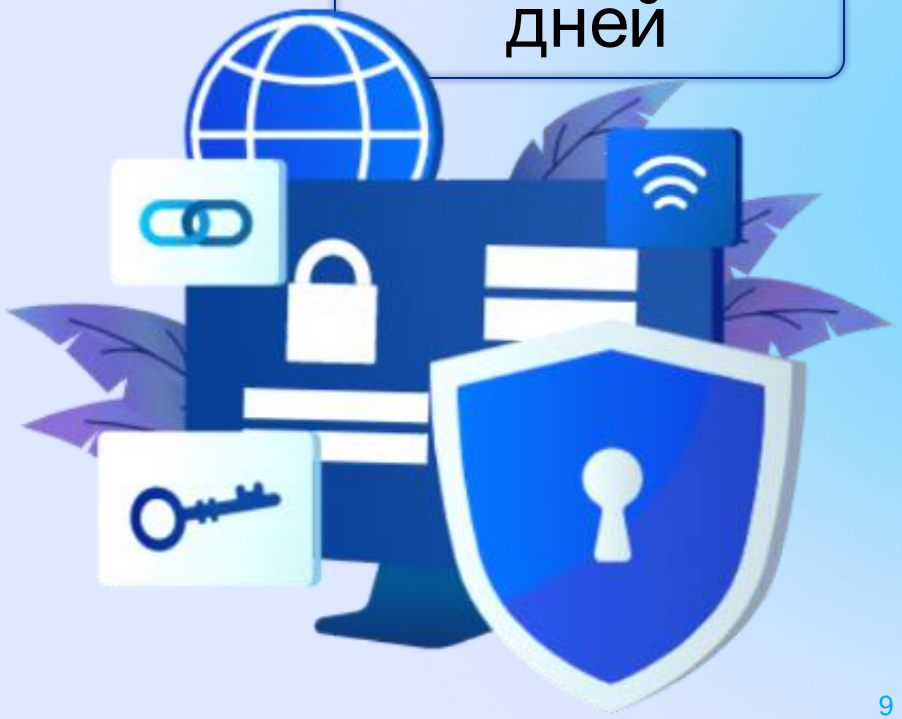
ИЗБЕГАЙТЕ ОЧЕВИДНЫХ КОМБИНАЦИЙ

- QWERTY
- PASSWORD

меняйте пароль каждые

90

дней



КАК ОБЕЗОПАСИТЬ СЕБЯ В СОЦИАЛЬНЫХ СЕТЯХ

Чем больше злоумышленник знает о вас (имя, день рождения, место проживания), тем выше вероятность того, что он сможет подготовить персонализированную атаку на вас или на ваши близких.

01 Отрегулируйте настройки конфиденциальности

сделайте личный аккаунт приватным, удалите неиспользуемые аккаунты, уберите домашний адрес и скройте информацию о своих контактах

02 Будьте аккуратны с публикуемой информацией

Ни в каком виде не разглашайте конфиденциальные данные и не выкладывайте фотографии важных документов

03 Настройте двухфакторную аутентификацию

Двойная проверка сделает взлом вашей страницы крайне сложным

04 Не используйте для регистрации рабочую почту

Лучше завести себе отдельный почтовый аккаунт для регистрации на разных ресурсах

05 Если вы встретили мошенника

обязательно сообщите в службу поддержки платформы. Страницу проанализируют и, в случае подтверждения, заблокируют

06 Будьте внимательны к письмам и ссылкам

Если вы когда-то отправляли конфиденциальную информацию, найдите и удалите эти сообщения.
Если ссылка вам неизвестна – лучше не переходить по ней

07 С осторожностью добавляйте «в друзья»

незнакомых людей. В настройках приватности запретите незнакомым людям оставлять комментарии. И скройте свои публикации от них, чтобы избежать спама и оскорблений

08 С осторожностью вводите данные при регистрации

Не указывайте данные, которые не нужны для получения некоторых услуг сервиса (номера удостоверения личности и т.п.)

WI-FI

Данные, передаваемые по общедоступной WI-FI-сети, можно легко перехватить. Многие пользователи мобильных устройств и планшетов подвергаются риску раскрытия частной информации, цифровых идентификационных данных и доступа к деньгам.

КАК ЗАЩИТИТЬСЯ ПРИ ПОДКЛЮЧЕНИИ К WI-FI

СВОЕВРЕМЕННО ОБНОВЛЯЙТЕ ПО

Это поможет защитить от уязвимостей и заражения устройства

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ

для своих учетных записей и никогда не используйте один и тот же пароль на разных аккаунтах

НЕ ОТКРЫВАЙТЕ ССЫЛКИ

и файлы, которые вы получаете от незнакомых и ненадежных источников

ЗАЩИЩЕННЫЕ WI-FI СЕТИ

Используйте защищенные Wi-Fi-сети, домашние или офисные сети, которые требуют ввода пароля

БУДЬТЕ БДИТЕЛЬНЫ

к конфиденциальной информации, которую вводите во время подключения к общедоступной сети

ОТКЛЮЧИТЕ АВТОПОДКЛЮЧЕНИЕ

к общедоступным Wi-Fi-сетям. Это поможет избежать подключения к поддельным сетям, созданным злоумышленниками.

АНТИВИРУСНАЯ ПРОГРАММА

Установите антивирус и регулярно обновляйте его. Это поможет защитить ваше устройство от вредоносных программ

VPN

Виртуальная частная сеть, обеспечивающая соединение «поверх» обычного Интернета. На данные момент многие пользователи предпочитают использовать бесплатные сервисы VPN. Однако стоит помнить, что при использовании таких сервисов существуют определенные риски.

РИСКИ ПРИ ИСПОЛЬЗОВАНИИ VPN

01 НЕТ ГАРАНТИЙ БЕЗОПАСНОСТИ

При подключении к бесплатным VPN-сервисам нет гарантии сохранения конфиденциальных данных (логины, пароли и т.д.)

02 МОЖЕТ СКОМПРОМЕТИРОВАТЬ ДАННЫЕ ПОЛЬЗОВАТЕЛЯ

а именно: продавать информацию о трафике для различных целей; собирать и многократно перепродавать сведения о действиях пользователя в сети

03 МОЖЕТ СОДЕРЖАТЬ ВИРУС

который может навредить устройству

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

ПРИЗНАКИ ЗВОНКОВ МОШЕННИКОВ:

- ✓ Создание ситуации с нехваткой времени, когда решения надо принимать очень быстро
- ✓ Весь разговор, с самого начала, на вас откровенно давят и убеждают, что всё происходит в ваших интересах и прямо сейчас буквально спасают ваши деньги
- ✓ Неправильная речь и шумы на фоне. Попытка (часто очень неплохая) имитировать колл-центр
- ✓ Технические ошибки
- ✓ Звонок в неудобное время
- ✓ Переключение с роботизированного помощника на сотрудников поддержки

КЕМ ПРЕДСТАВЛЯЮТСЯ И ЧТО ПРЕДЛАГАЮТ:

Звонок из Генпрокуратуры
Примите участие в расследовании
«Помогите поймать нечестного сотрудника…»

Звонок сотрудника Банка или Голосовой помощник (робот)
«Продиктуйте код для отмены мошеннической операции…»

Звонок из Службы безопасности Банка
«Карта заблокирована, перезвоните, пожалуйста по номеру…»
«Третье лицо обратилось в Банк с доверенностью от Вашего имени…»

Звонок из ЦБ, МВД, правоохранительных органов
«С Вашего счета хотят перевести деньги в другом городе…»
«Сообщаем об утечке Ваших данных..»
«На вас оформили кредит…»

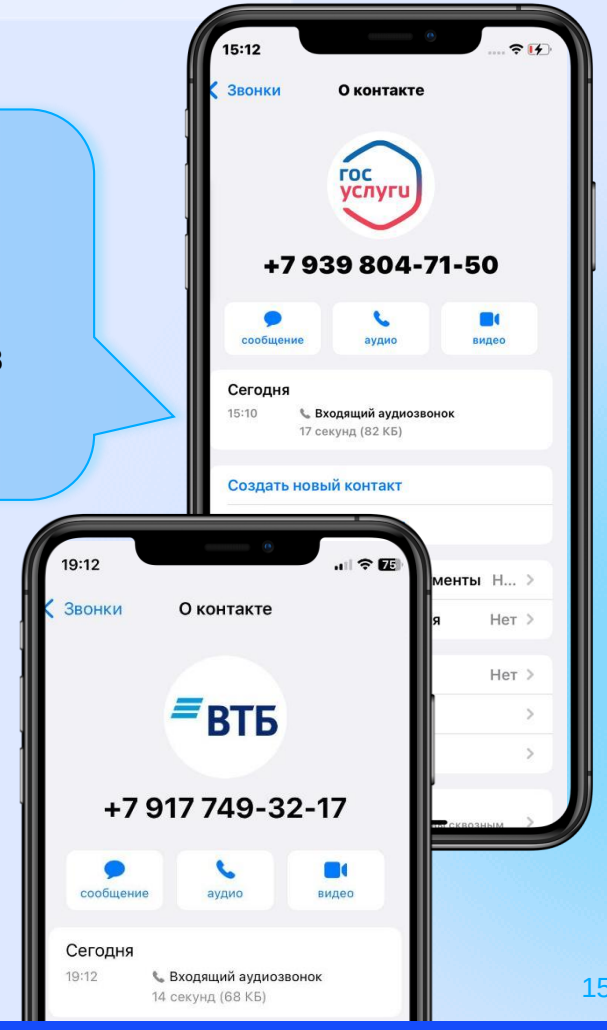
ПРАВИЛА УЧАСТИЯ В ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЯХ

КАК ДЕЛАЮТ МОШЕННИКИ:	КАК ПРОИСХОДИТ НА САМОМ ДЕЛЕ:
Звонят и сообщают о возбужденном уголовном деле, перечисляя статьи УК РФ	Настоящие сотрудники никогда не угрожают статьями, заведением уголовных дел, не проводят следственные и оперативные мероприятия по телефону
Присылают поддельные документы через мессенджеры	Сотрудник ПХО или судья вызовут вас в отделение полиции или направят повестку в суд. НО! никогда не будут обсуждать детали вопроса по телефону или направлять документы в мессенджерах
Переключают в рамках телефонного разговора между ведомствами и банками	Сотрудники ПХО или Банков не имеют возможности переключать в рамках одного телефонного разговора между ведомствами или банками

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО: Перевод на «безопасный счёт»

Звонок клиенту, представляясь сотрудниками «Службы безопасности» и сообщение о попытке совершения операции по Вашей карте:

Ваши средства находятся в опасности. Для исключения возможности финансовых потерь необходимо перевести сбережения на безопасную ячейку *якобы открытую на ваше имя. Это можете сделать вы сами или предоставить свои данные (номер карты, код из СМС) «сотруднику службы безопасности» для совершения перевода



*Данной «ячейкой» может являться счет физического лица, счет юридического лица, индивидуального предпринимателя, карты ВТБ и других банков

Часто пострадавшие закрывают все свои вклады, используют кредитные средства (карты, кредиты). Также клиент может провести операцию снятия наличных в АТМ и взнос на «безопасный счет»

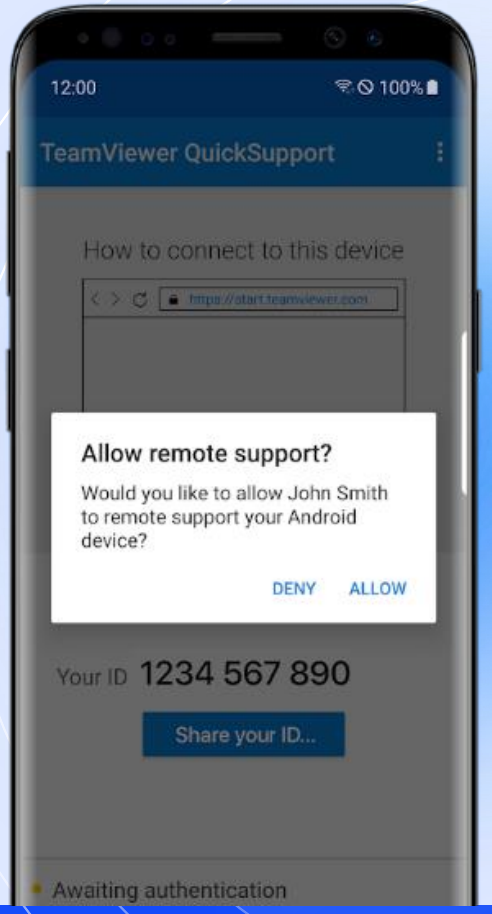
Использование программ удаленного управления

Звонок от сотрудника «Службы безопасности» и сообщение о попытке совершения операции по Вашей карте.

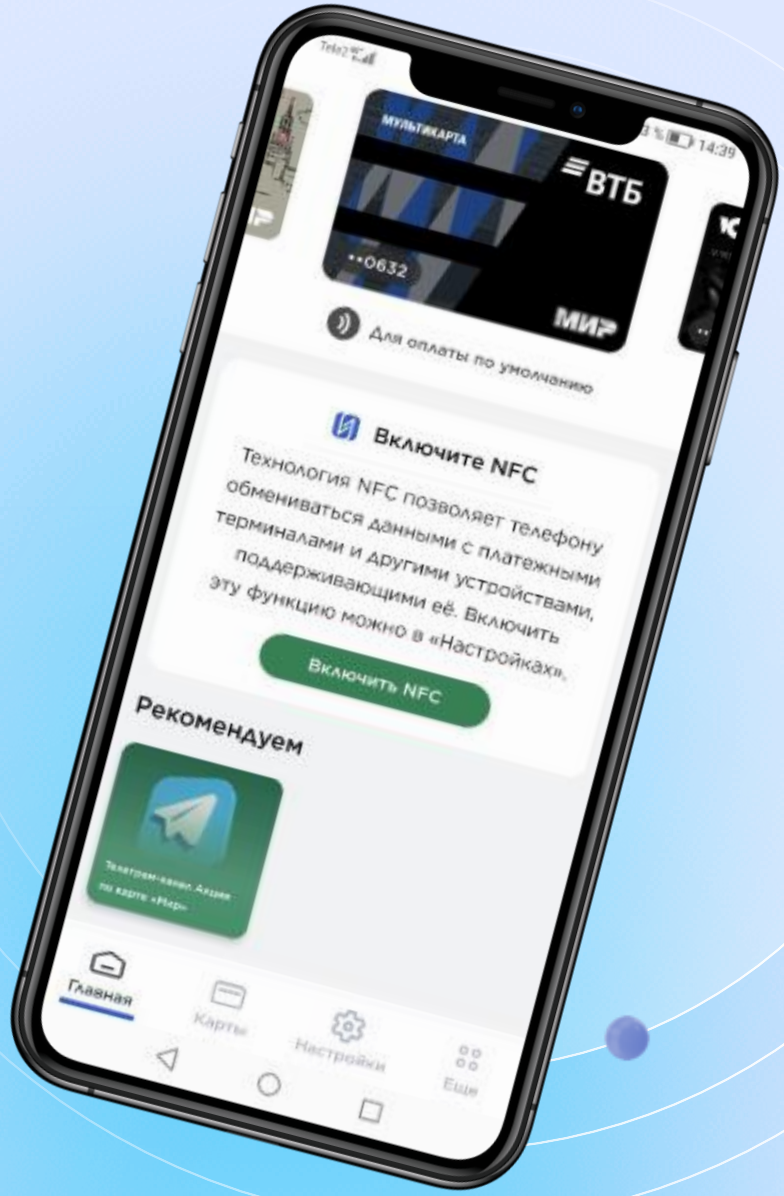
01 Клиента убеждают установить на мобильное устройство **приложение удаленного управления** (наиболее популярные: Quick Support, AnyDesk или AweSun) и разрешить подключение к устройству «сотруднику банка». Чаще всего предлогом для установки бывает удаление вирусов с устройства клиента, помощь в спасении средств клиента

02 В случае если устройство позволяет проводить операции удаленно, злоумышленники просят зайти в мобильное приложение и проверить сохранность средств, а затем перевернуть устройство и подождать, пока «сотрудники банка» удалят вирусы

03 В это время злоумышленники проводят списания через мобильное приложение клиента. Если мобильное приложение не позволяет проводить удаленное управление через программу, а только транслировать экран, злоумышленники убеждают клиента перевести средства на «безопасный счет»



Токенизация карты



01 Звонок клиенту от сотрудника «Службы безопасности» и сообщение о попытке совершения операции по его карте

02 Для спасения денежных средств клиента убеждают «выпустить новую карту». На самом деле клиент токенизирует (привязывает) у себя на устройстве карту мошенников

03 Для успешной токенизации клиенту сообщают одноразовый пароль(он приходит мошенникам, так как токенизируется их карта)

04 Далее клиента убеждают снять все деньги со счетов и внести их на новую карту через банкомат используя токен

БАНК ЗАБОТИТСЯ О БЕЗОПАСНОСТИ КЛИЕНТА

Если Клиент соблюдает правила финансовой безопасности, то мошенники не получат доступ к его счетам.

- При обнаружении подозрительной активности или компрометации данных клиента, Банк остановит операции или заблокирует карту/доступ к личному кабинету
- В ситуации, когда у Вас есть опасения о мошенничестве, обратитесь в Банк самостоятельно по безопасным каналам взаимодействия

БЕЗОПАСНЫЕ КАНАЛЫ ВЗАИМОДЕЙСТВИЯ С БАНКОМ

ЗАПОМНИТЕ: сотрудники банка никогда самостоятельно не инициируют общение через мессенджеры или социальные сети с клиентом

Если Вам поступают звонки, СМС-сообщения, сообщения в социальных сетях и мессенджерах от имени **«БАНКОВСКИХ РАБОТНИКОВ»** с информацией, касающейся финансовых операций:

01 Прекратите контактировать и ни в коем случае не перезванивайте на указанные в сообщениях номера

02 Не сообщайте звонящим поступающие на телефон СМС-коды подтверждения, данные банковских карт

03 Сообщите номер телефона мошенника в чат ВТБ Онлайн

ОФИЦИАЛЬНЫЕ НОМЕРА ТЕЛЕФОНОВ БАНКА ВТБ

- 1000
- 8 800 100 24 24
- +7 495 777 24 24

ОФИЦИАЛЬНЫЕ МЕССЕНДЖЕРЫ И СОЦИАЛЬНЫЕ СЕТИ БАНКА ВТБ

- Telegram: https://t.me/vtb_main_bot
- Сообщество «Вконтакте» https://vk.com/vtb

ОТВЕТСТВЕННОСТЬ И РИСКИ

НЕ РАЗГЛАШАЙТЕ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

Клиент при заключении ДКО (договор комплексного обслуживания) поставлен в известность о рисках компрометации и несет ответственность за безопасное и конфиденциальное хранение персональной информации

ВЫ ОТВЕТСТВЕННЫ ЗА СВОЙ КРЕДИТ

Клиент берет на себя личные обязательства перед Банком по возврату заемных денежных средств, полученных в результате оформления кредитных продуктов

НЕ СТАНОВИТЕСЬ ДРОПОМ*

Статья 158 Кража
Статья 159 Мошенничество
Статья 159.3 Мошенничество с использованием электронных средств платежа
Статья 187 Неправомерный оборот средств платежей

НЕ ФАЛЬСИФИЦИРУЙТЕ ЗАРПЛАТНУЮ ВЕДОМОСТЬ

Статья 327 Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков
Статья 174 Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем

*ДРОП – соучастник преступления, который задействован в выводе средств, полученных противозаконным способом

СПАСИБО
ЗА ВНИМАНИЕ!

Рекомендуем ознакомиться с Памяткой по безопасности на официальном сайте