**Наиболее распространенный способ выманивания персональных данных – введение в заблуждение в ходе разговора в мессенджере.**

    Совершая звонок в мессенджере, злоумышленники представляются работниками банков, сообщают что совершается в настоящий момент **осуществляются подозрительные операции по банковской платежной карте или по вкладу**. «Для установления личности» **предлагают назвать свои данные, в том числе данные карты и личный номер, а также коды из смс-сообщений**. В большинстве случаев злоумышленники обращаются по имени, могут также назвать последние 4 цифры банковской карты.
 *В Новополоцке местная жительница в ходе телефонной беседы с якобы сотрудником банка передала ему секретные сведения о реквизитах карты, своем идентификационном номере паспорта и коды из смс-сообщений от банка для подтверждения операций. В итоге женщина лишилась более 30 тысяч д*олларов, переведенных с нескольких ее счетов.
    Злоумышленники настаивают на проведении отмены операций. Для этого**предлагают установить**указанную ими известную **программу удаленного доступа** к устройству. Затем, чтобы проверить баланс счета, просят **войти в свой интернет-банкинг**. В свою очередь, установленная программа предоставляет злоумышленникам возможность видеть все происходящее на телефоне или компьютере, в том числе введенный пароль для входа в банкинг.
  *После телефонного общения с якобы сотрудником банка женщина потеряла более 20 тысяч долларов. Мужчина, в ходе разговора в мессенджере представился сотрудником банка и указал, что прямо сейчас с ее карт-счета осуществляется попытка списания денежных средств и для отмены несанкционированной операции необходимо установить на мобильное устройство или компьютер дополнительное программное обеспечение, а также передать коды из смс-сообщений от банка. Установленная женщиной программа предоставила мошеннику удаленный доступ к  компьютеру, где с помощью кодов из смс он вошел в интернет-банкинг и перевел все деньги на свой счет.*
    **Злоумышленники также представляются сотрудниками правоохранительных органов**. Под предлогом совместного разоблачения недобросовестного сотрудника банка, который используя ваши данные, оформил заявку на кредит от Вашего имени. Убеждают взять еще несколько кредитов и перевести их на «специально созданный защищенный счет», а после окончания «спецоперации» вернуть все деньги. При этом суть этой «спецоперации» необходимо держать в тайне.
  *Такое преступление случилось в начале 2021 года. Молодая девушка из Витебска, мама двоих детей, после разговора с сотрудницей банка оформила на себя кредиты на потребительские нужды в трех банках города почти на 16 тысяч рублей, а полученные средства перевела мошенникам.
    В августе и сентябре в Орше пожилой мужчина и рабочий завода в трёх банках взяли кредит на сумму более чем на 17 и 15 тысяч рублей каждый и, доверяя собеседникам из Viber, исполнили задания – перевели деньги на указанный киберпреступниками счет. Аналогичное преступление случилось в Витебске, рабочая крупного предприятия наличными взяла два кредита в банках на сумму более 9 тысяч рублей и через терминал перевела их на указанные ей злоумышленниками счета. И это только некоторые примеры.*
  **Новым способом** **мошенники получают реквизиты банковской карты через детей** держателей карт, в ходе общения в соцсетях под видом сверстников.
  *11-летняя девочка в ходе «дружеской» двухнедельной переписки в социальной сети с виртуальной подружкой, по ее просьбе передала собеседнице фотографии платежной карты матери, тем самым сообщив персональные данные. Заполучив данные карты, злоумышленники перевели с нее все имеющиеся средства. В ходе общения с ребенком, можно попросить передать и другие данные, такие как фотографии паспорта или смс-коды, что может повлечь открытие онлайн-кредита.*
    Получив доступ к аккаунту пользователя в соцсети (методом подбора пароля или вредоносного программного обеспечения), **злоумышленник осуществляет рассылку сообщений интернет-друзьям** и ждет отклика, **убеждает под разными предлогами передать денежные средства или конфиденциальную информацию, например фото банковской карты**.
  *Взломав аккаунт студентки витебского ВУЗа, от ее имени отправили сообщение с просьбой оказать материальную помощь на указанную банковскую карту в связи со скоропостижной смертью ее матери. Или от имени сестры, прислали сообщение с просьбой оплатить кредит, так как в этом месяце много потратила, а деньги вернет после зарплаты.*
    Или например другое сообщение: «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом отдашь мне. В долгу не останусь!»
    Злоумышленники также пользуются методом фишинга, который заключается в том, чтобы подделать страницу платежной системы и получить данные банковской карты владельца. Фишинговый сайт – это страница сайта созданная как точная копия настоящей. Чаще всего подделывают платежные системы и почтовые сервисы (Белпочта, Европочта, СДЭК). Поддельные страницы присылают в мессенджерах продавцам товаров с сайтов объявлений якобы для получения предоплаты за товар, на который оформлена доставка. В таком случае фишинговые страницы содержат сведения о продаваемом товаре и абсолютно повторяют фирменный стиль и сервисы сайта, в том числе и  онлайн-консультанта. Злоумышленники убеждают продавца товара ввести данные банковской карты, включая имя владельца, полный номер, срок действия и трехзначный код с обратной стороны карты. Данные, которые заполучает создатель страницы, дают ему возможность перевести все деньги с карты владельца. Отличием фишингового сайта является то, что ссылка на него направляется лично в мессенджере, а интернет-адрес в названии похож на настоящий, но имеет незаметное отличие в одной букве или цифре.

    *Примеры фишинговых страниц: belpochta.by, bellpost.by, belpocht.by, belpost.be, europocha.be, kufar.cc, bel-bank.online.by.*

**ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ КИБЕРПРЕСТУПНИКОВ**

* Никому ни под каким предлогом не передавать номер банковской карты, срок действия, трехзначный секретный код на обороте, логины и пароли доступа к банкингу, смс-коды от банка.
* Подключить услугу «3D Secure» и установить лимиты на суммы онлайн-операций (нужно подключить в настройках банкинга или в банке).
* Не устанавливать программы и не переводить деньги по указанию, полученному по телефону даже от работников банка или милиции.
* При поступлении звонка в мессенджере от работника банка, закончить разговор и перезвонить в банк самостоятельно.
* При онлайн-оплате, в том числе услуг такси, проверять адрес сайта и использовать отдельную карту (виртуальную), хранить на ней небольшие суммы.

*Актуальная информация о совершаемых киберпреступлениях доступна в Телеграм-канале «Цифровая грамотность»:*

[***https://t.me/cifgram***](https://t.me/cifgram)

*Листовки по кибербезопасности вложены в письмо.*

*Управление по противодействию киберпреступности
УВД Витебского облисполкома*