Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Преступность в виртуальном пространстве – явление относительно новое, но часть преступлений, совершаемых в сфере высоких технологий,– это знакомые кражи, мошенничества, вымогательство.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей.Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации с использованием сети Интернет.

Правила, которые помогут Вам не стать жертвой киберпреступлений:

– храните номер карточки и ПИН–коды в тайне;

– не используйте один пароль для всех интернет-ресурсов;

– к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;

– регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;

– поставьте лимит на сумму списаний или перевода в личном кабинете банка;

– не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;

– не переводите денежные средства на счета незнакомых лиц;

– не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;

– будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей и всегда проверяйте вложения на наличие вирусов, если это возможно;

– не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;

– не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;

– насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством,преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;

– не размещайте в открытом доступе и не передавайте информацию личного характера.

Рассмотрим самые распространенные схемы мошенничества:

1. **«Звонок из Банка»**

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

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

У вас просят конфиденциальные данные

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

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить

- «*Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! 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!

2. **«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.

Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

QR-код

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

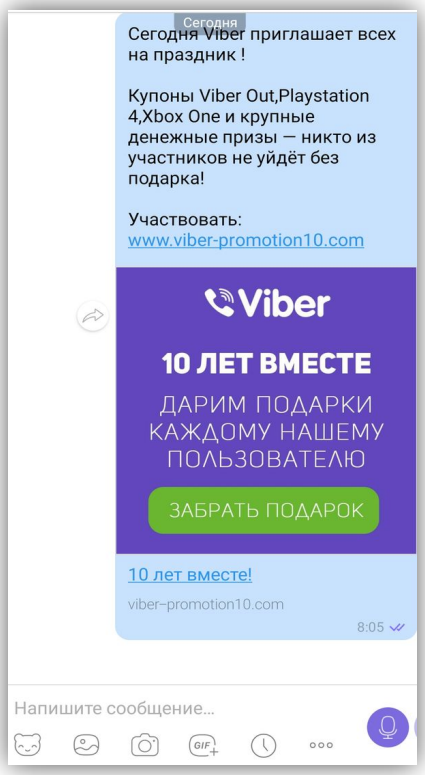
3. **«Сообщения в социальных сетях»**

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.

Важно! При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

4. «Розыгрыши/раздачи/опросы от Банка или иных организаций»



Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса 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 кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

Как защитить свои сбережения в виртуальном мире

На протяжении текущего года в Республике Беларусь вновь наблюдается рост количества преступлений в сфере информационных технологий. Подавляющее большинство из них составляют хищения денежных средств путем завладения реквизитами банковских платежных карт – ст. 212 (хищение имущества путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь.

Понимание того, что такое киберпреступление, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

В этой статье подробно расскажем о том, что такое киберпреступность, от каких угроз и как нужно защищаться, чтобы обеспечить свою безопасности в сети интернет.

Что такое киберпреступление

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

Типы киберпреступлений

Вот несколько примеров различных типов киберпреступлений:

- Мошенничество с электронной почтой и интернет-мошенничество;
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);
- Кража финансовых данных или данных банковских карт;
- Кража и продажа корпоративных данных;
- Кибершантаж (требование денег для предотвращения кибератаки);
- Атаки программ-вымогателей (тип кибершантажа);
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев);
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций).

Большинство киберпреступлений относится к одной из двух категорий:

- Криминальная деятельность, целью которой являются сами компьютеры;
- Криминальная деятельность, в которой компьютеры используются для совершения других преступлений.

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Примеры киберпреступлений

Рассмотрим резонансные примеры различных типов кибератак:

1. Атаки с использованием вредоносного ПО

Атака с использованием вредоносного ПО – это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей.К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

Известным мировым примером атаки с использованием вредоносного ПО является атака вымогателя WannaCry, случившаяся в мае 2017 года.Ransomware– это тип вредоносного ПО, который используется для получения денег в обмен на разблокирование устройства/файлов жертвы. WannaCry - это тип программ-вымогателей, которые используют уязвимость компьютеров Windows.Жертвами WannaCry стали 230 000 компьютеров в 150 странах мира. Владельцы заблокированных файлов отправили сообщение с согласием заплатить выкуп в криптовалюте BitCoin за восстановление доступа к своим данным.Финансовые потери в результате деятельности WannaCry оцениваются в 4 миллиарда долларов.

2. Фишинг

Фишинговая кампания – это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают.Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также

могут просить получателя в ответном письме предоставить конфиденциальную информацию.

Известный пример фишинг-мошенничества произошел на Чемпионате мира по футболу в 2018году. По информации Inc, фишинговые электронные письма рассылались футбольным фанатам.

В этих письмах злоумышленники привлекали болельщиков фальшивыми бесплатными поездками в Москву на Чемпионат мира.У людей, которые проходили по ссылке в сообщениях, были украдены личные данные.

Другой тип фишинговой кампании известен как целевой фишинг. Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают.В отличие от массовых неперсонифицированных фишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

3. Распределённые атаки типа «отказ в обслуживании»

Распределенные атаки типа «отказ в обслуживании» (DDoS) - это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (InternetofThings – Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

Известным примером DDoS-атаки является атака на веб-сайт Национальной лотереи Великобритании в 2017 году. Результатом стало отключение веб-сайта и мобильного приложения лотереи, что не позволило гражданам Великобритании играть.

Как не стать жертвой киберпреступления

Теперь, понимая, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные?

Следующие советы помогут обезопасить себя и сохранить Ваши деньги:

1. **Регулярно обновляйте ПО и операционную систему**

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

2. **Установите антивирусное ПО и регулярно его обновляйте**

Использование антивируса или комплексного решения для обеспечения интернет-безопасности,– это правильный способ защитить вашу систему от атак.Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

3. **Используйте сложные пароли**

Используйте сложные пароли, которые трудно подобрать, и, по возможности, нигде их не записывайте, особенно в цифровом виде. Можно воспользоваться услугой надежного менеджера паролей,

который облегчит вам задачу, предложив сгенерированный им сложный пароль.

4. **Не открывайте вложения в электронных спам-сообщениях**

Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

5. **Не нажимайте на ссылки в электронных спам-сообщениях и на сайтах, которые Вам не знакомы**

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, – это вредоносные ссылки в спамовых электронных письмах или других сообщениях, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

6. **Не предоставляйте личную информацию, не убедившись в безопасности канала передачи**

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

7. **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос**

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

8. **Внимательно проверяйте адреса веб-сайтов, которые вы посещаете**

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Убедитесь, что они выглядят легитимно. Не переходите по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.Если ваш продукт для обеспечения безопасности в сети интернет включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

9. **Внимательно просматривайте свои банковские выписки**

Наши советы должны помочь вам не стать жертвой киберпреступников. Но если все же это случилось, важно понять, когда и как это произошло.Просматривайте внимательно свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

Теперь вы понимаете, какую угрозу представляют киберпреступники, и знаете, как от нее защититься.

Мошенники в киберпространстве и как им противостоять!

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя Ваши эмоции.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;

2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;

3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.

Помните! Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.

Обращаем Ваше внимание, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.

Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в Банк по номеру, указанному на Вашей банковской карте.

Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!

Вот несколько простых советов, соблюдение которых, позволит 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 (задайте другу вопрос, ответ на который знаете только вы оба);

2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по указанному на банковской карте или официальном сайте номерам;

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, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему дистанционного банковского обслуживания (Интернет-банкинг, М-банкинг и другие). В такой ситуации немедленно прервите разговор и свяжитесь с Банком;

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

6. Обязательно подключите 3D-secure и смс-оповещение;

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

8. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания, а также для подтверждения платежей;

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.

Рассмотрим самые распространенные схемы мошенничества сейчас:

5. **«Звонок из Банка»**

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

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

У вас просят конфиденциальные данные

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

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить

- «*Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! 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!

6. **«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.

Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

QR-код

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

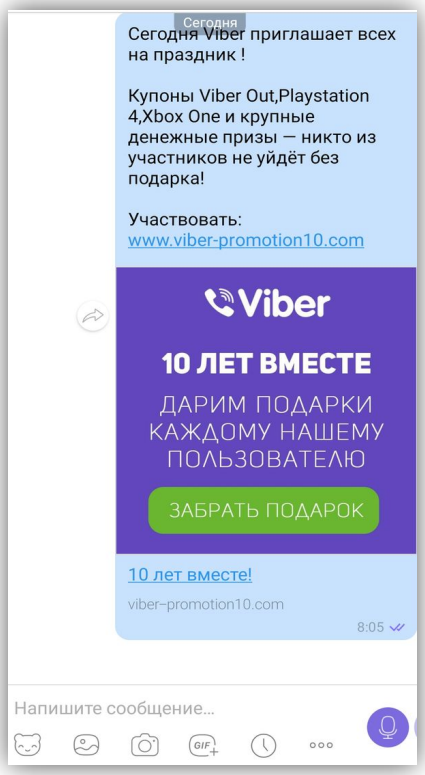
7. **«Сообщения в социальных сетях»**

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.

Важно! При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

8. «Розыгрыши/раздачи/опросы от Банка или иных организаций»



Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса 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 кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.