Мошенничество: наиболее распространенные схемы и практические рекомендации по противодействию

WWW.BELAPB.BY

ЧАСТЬ I. ПРОСТО О ПРОСТОМ.

Базовые понятия и «бытовые» случаи мошенничества

Банковская платежная карточка. Базовые знания

Банковская платежная карточка — пластиковый носитель, позволяющий проводить операции оплаты товаров и услуг онлайн и офлайн, а также операции снятия наличных денежных средств со счета.

Для списания и зачисления средств необязательно держать карточку в руках - достаточно ее платежных данных.

Не все данные, указанные на пластиковом носителе, являются платежными.

К реквизитам, не отраженным на пластиковом носителе, относится номер счета банковской карточки и **ПИН-код**. ПИН-код необходим для подтверждения операций по карточке при расчетах пластиковым носителем.

Банковская платежная карточка. Базовые знания

К реквизитам, необходимым для **СПИСАНИЯ** средств в онлайн режиме, относят:

- **номер карточки**, нанесенный на лицевой стороне;
- **срок действия карточки**, указанный на лицевой стороне ниже номера;
- **фамилия и имя держателя карточки**;
- CVV2/CVC2 (Visa/Mastercard), КПП2 (БЕЛКАРТ) - код, состоящий из трех цифр, называемый еще проверочным числом или кодом безопасности, указан на обороте рядом с магнитной полосой.

Ряд операций требует подтверждения паролем, направляемым клиенту по СМС (**3D-Secure - код**). Он генерируется для каждой операции отдельно, имеет ограниченный период действия, направляется только на номер телефона, указанный держателем карточки в анкете.

Для **ЗАЧИСЛЕНИЯ** перевода на счет вашей карточки в онлайн режиме используется:

- номер карточки;
- иногда – срок действия карточки.

ПИН-код

ПИН-код - (англ. PIN - Personal Identification Number) – персональный идентификационный номер, являющийся секретным кодом карточки.

Код присваивается карточке с целью идентификации держателя при проведении финансовых операций. Это электронный аналог подписи держателя.

Помните, что утраченный (забытый) ПИН-код восстановить невозможно, он известен только держателю карточки. ПИН-код можно сменить (например, через СДБО* или в подразделении банка) или необходимо перевыпустить карточку.

У держателя карточки, как правило, есть 3 (три) попытки правильного ввода кода. Когда количество попыток превышает максимально допустимый предел, карточка автоматически блокируется.

В случае блокировки по причине неверно набранного ПИН-кода, банкоматы могут изъять карточку.

*СДБО – системы дистанционного банковского обслуживания.

ЭТО ДОЛЖЕН ЗНАТЬ КАЖДЫЙ:

1. Код должен знать только держатель карточки. Его необходимо хранить в тайне и ни в коем случае не разглашать третьим лицам, в том числе родным и знакомым.

2. Никогда не пишите свой ПИН-код на карточке. Если вы случайно потеряете карточку или она будет украдена, таким образом вы предоставите ворам мгновенный доступ к вашему счету, чтобы снять ваши деньги.

3. Не храните письменную копию ПИН-кода в бумажнике или кошельке вместе с карточкой.

4. Скройте свой ПИН-код. Когда бы вы ни вводили свой ПИН-код, будь то в банкомате, в магазине или ресторане, всегда помните, что нужно использовать одну руку для ввода ПИН-кода, а другой рукой прикрывать клавиатуру, чтобы никто не мог видеть, какой ПИН-код вы вводите.

Что можно сделать, зная реквизиты карточки

Держатель карточки может получать и отправлять денежные переводы, оплачивать покупки, пополнять счет своего мобильного телефона и выполнять другие расчетные операции.

Мошенники, завладевшие **реквизитами** вашей **карточки**, могут совершить все те же действия.

Возможности хищения средств тем шире, чем больше данных известно мошенникам:

- Номер карточки и имя, фамилия держателя - исходящие платежные операции провести нельзя;
- Номер карточки, имя и фамилия держателя, срок действия - доступна оплата покупок в некоторых онлайн-магазинах, где не требуется ввод CVV2 /CVC2 / КПП2– кода и 3D-Secure - кода.
- Номер карточки, имя и фамилия держателя, срок действия, CVV2 / CVC2 / КПП2 – код — можно совершать покупки во многих онлайн-магазинах, «привязать» карточку к различным магазинам приложений.
- Номер карты, имя и фамилия держателя, срок действия, CVV2 / CVC2 / КПП2– код и 3D-Secure – код — эти данные позволяют оплатить любые покупки, сделать перевод, пополнить счет электронного кошелька и т.д.

Утеря, кража карточки

Как злоумышленник может похитить деньги с утерянной / украденной карточки?

- *Совершить покупку в объектах торговли (сервиса) посредством бесконтактной технологии оплаты* на сумму ниже определенного лимита (в таком случае не требуется проведение верификации держателя карточки, т.е. не нужно вводить ПИН-код).

- *Совершить операции в сети Интернет*.
  На карточке указаны данные (номер карточки, имя и фамилия держателя карточки, проверочный код), которых достаточно для оформления покупки или перевода денежных средств на Интернет-ресурсах.

- *Обналичить в банкомате*.
  Возможно только в случае, когда злоумышленнику известен ПИН-код от карточки.

Что делать, если ваша карточка была утеряна / украдена?

- Заблокировать карточку любым удобным способом (в мобильном приложении, по звонку в Банковский процессинговый центр, USSD-командой и т.д.);

- Проверить историю операций (выписку), в случае хищения денежных средств с карточки – рекомендуется обратиться в правоохранительные органы с соответствующим заявлением;

- Перевыпустить карточку.

РЕКОМЕНДУЕМ:

- Подключить СМС-информирование. Вы сразу узнаете о попытках оплаты, снятия денег и сможете оперативно заблокировать карточку.

- Установить лимиты расходования денежных средств посредством мобильного приложения. Эта услуга увеличивает уверенность в сохранности денежных средств на счете и обеспечивает дополнительный контроль над расходованием средств по карточке.

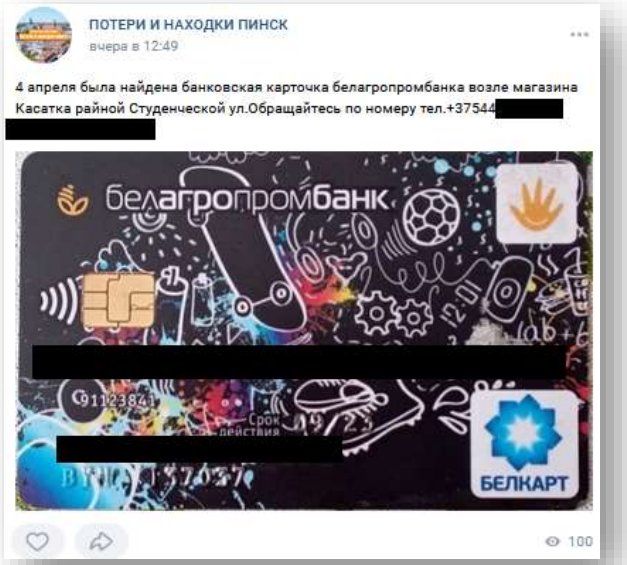
Сообщества «потеряшек»

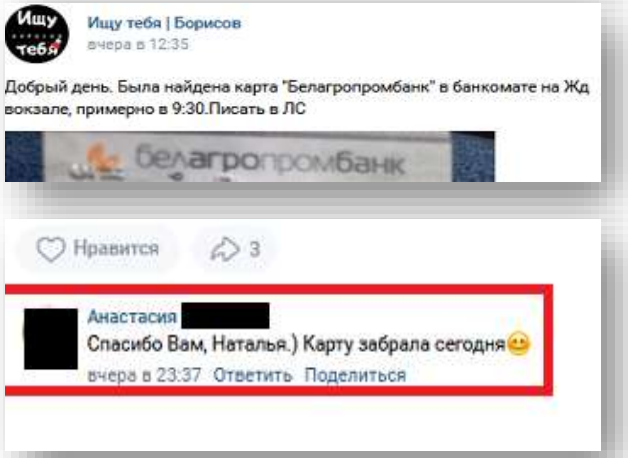
Что делать, если карточку нашли и вернули?

Появление третьих лиц в истории с пропажей карточки – это большой риск.

Даже если карточку вам вернули и списаний денег не было – реквизиты карточки (номер карточки, имя и фамилия держателя карточки, проверочный код) стали известны третьим лицам.

Поэтому такую карточку рекомендуется *перевыпустить*. По той же причине рекомендуется перевыпускать карточки, забытые в банкоматах, инфокиосках, на кассах в магазинах и т.д.





Что делать, если вы нашли чужую карточку?

НЕ РЕКОМЕНДУЕМ:

- **Пытаться воспользоваться чужой карточкой.**

В ином случае действия гражданина могут попадать под часть первую ст. 212 «Хищение имущества путем модификации компьютерной информации» Уголовного кодекса Республики Беларусь.

- **Искать держателя карточки.**

В банке-эмитенте карточки постороннему лицу информацию о держателе карточки не предоставят, т.к. данная информация является банковской тайной.

Допустим, вы нашли держателя карточки через соцсети. Однако, с большей долей вероятности, при личной встрече вместо «спасибо» вы получите обвинение в воровстве.

Так же нужно помнить, что фотографии карточек компрометируют и держателей карточек, и тех, кто размещает эти изображения в сети. После размещения фотографии может поступить звонок от мошенника, представляющегося «держателем карточки» или «сотрудником» службы безопасности банка, правоохранительных органов. Как правило, мошенник начинает шантажировать нашедшего и использовать различные уловки для завладения средствами как на самой карточке, так и средствами нашедшего ее.

РЕКОМЕНДУЕМ:

Если обнаружили чужую карточку в банкомате.

В такой ситуации лучше ничего не делать. Если карточка видна из картоприемника, значит владелец еще не далеко отошел от банкомата. Возможно, он услышит звуковой сигнал и вернется к устройству.

Если владельца карточки нет поблизости, нужно подождать пока банкомат втянет карточку в картоприемник. Когда владелец обнаружит пропажу, он сможет обратиться в свой банк. Карточку извлекут из банкомата и вернут держателю.

Если нашли карточку на улице, в магазине, в транспорте и т.д.

* Можно обратиться на «горячую линию» банка (как правило, номер телефона указан на оборотной стороне карточки) и сообщить, что обнаружили утерянную карточку. Оператор заблокирует ее.

* Можно вернуть карточку в ближайший офис банка-эмитента. Специалисты банка самостоятельно свяжутся с держателем карточки, а затем ее перевыпустят.

* Можно сообщить о находке в милицию. Сами правоохранители называют такой способ реагирования на находку в виде пластика «оптимальным».

«Захват» наличных

Мошенники устанавливают специальную планку с липкой лентой на отверстие для выдачи денег в банкомате. Так, во время операции по снятию средств **банкноты прилипают к мошеннической накладке изнутри**, и держатель карточки не может их получить. Очень часто человек, не получив деньги, решает, что в работе банкомата произошел сбой или закончились наличные, и отходит, открывая преступнику доступ к захваченным с помощью устройства денежным средствам.

Что делать, если вы попали в такую ситуацию?

1. Убедитесь, что на экране банкомата появилось сообщение о выдаче наличных. Если при этом деньги не были поданы из специального отверстия – *проверьте отверстие для снятия наличных, нет ли там подозрительных предметов*.

Большинство мошеннических устройств устанавливается быстро и на короткий срок, не является частью общей конструкции банкомата, потому всегда присутствует небольшой люфт (то есть, *дополнительную, мошенническую, «накладку» можно легко расшатать рукой*). Если вы обнаружили накладку-планку с деньгами в отверстии для выдачи наличных, *позвоните в банк* по номеру, указанному на банкомате.

2. *Не отходите от банкомата*. Позвоните в банк по телефону, указанному на банкомате, или по телефону, указанному на карточке.

Если вы отойдете от банкомата, к нему вскоре подойдет мошенник, который заберет деньги, застрявшие в отверстии для выдачи наличных.

Поскольку банкомат зафиксировал успешную операцию по снятию наличных с вашей карточки, то банк не несет финансовую ответственность за то, что эти деньги были украдены уже после снятия.

Электронная почта

На электронную почту мошенники присылают письма с обещанием подарков, денег и «беспроцентных» кредитов. В строке отправителя может быть как неизвестный вам человек (часто иностранец), так и известный сайт, платежная система, онлайн-сервис или банк.

Ничего страшного не произойдет, если вы просто откроете письмо, но не переходите по ссылкам и не скачиваете вложения из письма — так вы рискуете заразить компьютер (смартфон) вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карточки.

Как предотвратить?

- Включите спам-фильтр на почте, тогда часть подозрительных писем будет попадать в специальную папку.
- Всегда обращайте внимание на заголовок письма, его отправителя и содержание. Компании всегда рассылают почтовые рассылки с одних и тех же адресов и редко допускают ошибки в письмах — а вот мошенники часто пишут с большим количеством ошибок, нечитаемых системой символов и перевирают название компании в адресе.
- **Не переходите по ссылкам из таких писем и не скачивайте вложения из них.**

Мобильный телефон

Зловредные программы умеют маскироваться под приложения от известных компаний, банков, которые вы скачиваете на телефон.

Как предотвратить?

- Скачивайте приложения на телефон только из официального магазина (GooglePlay, AppStore, AppGallery и т.д.).
- Обращайте внимание, в первую очередь, на разработчика программы - в официальных банковских приложениях указан сам банк.
- Внимательно читайте описание и не скачивайте приложения сторонних разработчиков.

Карты детям не игрушки

Бывают случаи, когда поиски злоумышленников, ворующих деньги с банковских карточек, приводят родителей к их собственным детям.

Дети неумышленно помогают «облегчить» родительский кошелек, увлекшись онлайн-играми, скачанными из магазина приложений. На первый взгляд все безобидно: приложения бесплатные. Однако в процессе игры у участников появляется необходимость «докупить» те или иные элементы, для чего к своему аккаунту они привязывают банковскую карточку одного из родителей. Пока ребенок играет и пополняет онлайн-реквизит, мамы и папы недоумевают: почему со счета исчезают деньги?

Формально в действиях ребенка в таких случаях усматривается состав преступления, т.к. держатель банковской карточки (родитель) не санкционировал проведение денежной операции.

Как предотвратить:

- Не передавайте свою банковскую карточку и не сообщайте ее реквизиты третьим лицам, в т.ч. родственникам;
- Не «привязывайте» реквизиты своей *зарплатной* карточки к магазину приложений на телефоне. Совершайте онлайн-покупки с помощью отдельной карточки (например, виртуальной);
- Выпустите ребенку отдельную *детскую* карточку. Контролировать расходование денежных средств по ней очень просто: установите *лимиты*, регулярно просматривайте историю платежей (выписку) посредством системы дистанционного банковского обслуживания.

Сложный пароль – это важно

Хранение пароля в секрете очень важно, однако пароль также должен быть достаточно сложным, чтобы противостоять попыткам его подбора. Злоумышленник, который хочет похитить ваши данные, может воспользоваться программой автоматического подбора пароля, которая будет многократно пытаться зайти на сайт с вашим логином и различными паролями. Подбирать пароль можно, просто перебирая всевозможные комбинации символов, вводимых с клавиатуры. Существенно упростить задачу помогает словарь часто используемых паролей. Оказывается, многие люди недостаточно оригинальны и выбирают одни и те же пароли, даже не сговариваясь.

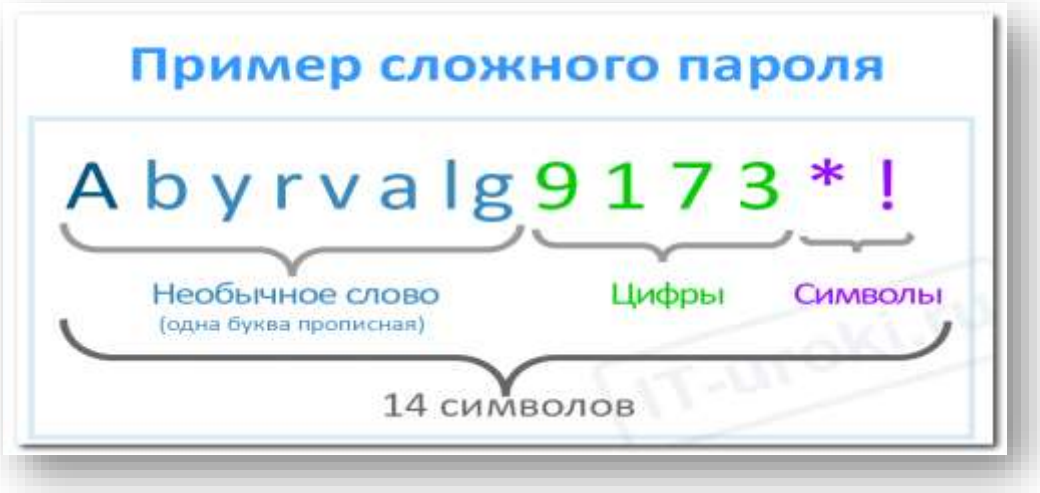
Словари для подбора паролей собирают чаще всего в результате кражи баз паролей с взломанных сайтов. Однако есть и другие способы, эксплуатирующие человеческое невежество и любопытство.

Некоторое время назад в Интернете появились сайты, предлагавшие проверить пароль на стойкость. Для этого достаточно было ввести свой пароль и увидеть результат оценки. Были и такие сайты, которые обещали поискать пароль в словаре для подбора паролей. Очевидно, всё это примеры социальной инженерии злоумышленников. **Никогда нельзя вводить свой пароль на сайте, отличном от того, для которого этот пароль предназначен!**

Как же создать стойкий пароль, который с гарантией не окажется в словаре злоумышленников?

Прежде всего, стойкость пароля заключается в его длине. Чем больше в пароле символов, тем дольше придется его подбирать и тем меньше шансов его подобрать по словарю. В настоящее время стойкими считаются пароли длиннее 14 символов.

Кроме того, настоятельно рекомендуется использовать в пароле не только буквы, но и цифры, а также знаки препинания и служебные символы вроде $, @ и %.



ЧАСТЬ II. ПРОСТО О СЛОЖНОМ

Социальная инженерия

Социальная инженерия

психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации

Наибольшее распространение в Республике Беларусь получили следующие виды социальной инженерии:

Фишинг – вид мошенничества, суть которого – завладение логинами и паролями от важных сайтов, аккаунтов, счетов в банке и другой конфиденциальной информацией путем перенаправления пользователя на мошеннический сайт, внешне очень похожий на настоящий. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести на поддельной странице свои логин, пароль и одноразовый код, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Вишинг – метод, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, правоохранительных органов и т.д.), под разными предлогами выманивают у держателя платежной карточки конфиденциальную информацию или стимулируют его к совершению каких-то действий со своим счетом или банковской платежной карточкой.

Взлом социальных сетей – взламывается страница пользователя и от его имени идут сообщения его друзьям, чаще всего с просьбой «скинь денег на карточку».

Схема «Помощь другу»

Суть: Мошенник «взламывает» профили отдельных пользователей социальных сетей (чаще «Вконтакте» и «Одноклассники») и направляет друзьям «взломанного» пользователя личные сообщения с просьбой помочь в получении денежного перевода, одолжить небольшую сумму в долг и т.д.

В ход идут самые разные легенды: мол, нет средств к существованию из-за блокировки карточки по вине обслуживающего банка; умер близкий человек и нет денег на похороны; необходимость срочного лечения и т.д.

Иногда мошенник «соблазняет» жертву обещая % или определенную сумму от перевода, для поступления которого необходимы реквизиты карточки (или Интернет-банкинга) жертвы.

Важно: после непосредственного «взлома» аккаунта мошенник изучает историю личных сообщений, чтобы скопировать стиль письма «взломанного» пользователя.

Что делать?

1. Связаться с человеком, от имени которого было направлено сообщение, альтернативным способом, например, по телефону.
2. Не сообщать (в т.ч. не отправлять фото) реквизиты карточки, значения СМС-кодов, логины и пароли от Интернет-банкинга. Не следует это делать и в случаях, когда пользователь не был «взломан».
3. Не переходить по подозрительным ссылкам.
4. В случае, если платежная или конфиденциальная информация была сообщена мошеннику – незамедлительно заблокировать карточку и/или сменить логин+пароль от Интернет-банкинга. Сообщить о случившемся в банк.
5. Направить в службу технической поддержки социальной сети жалобу на действия пользователя (жалоба должна быть обоснована, поэтому детально опишите ситуацию, предоставьте все имеющиеся доказательства, например, скрин-шоты переписки).
6. Обратитесь в правоохранительные органы.

привет не отвелкаю помощь нужна что за карта у тебя? 02:30

Здаров 02:30

Виза 02:30

я карту потерял можно я тебе деньги свои переведу ? а ты мне руки отдашь ? просто востанавливать долго а деньги нужны 02:31

Ну давай, когда увидится сможем? 02:31

просто щас нужно потому что кто то пытается деньги с нее снять давай я хотя бы просто переведу??ъ 02:32

просто щас нужно потому что кто то пытается деньги с нее снять давай я хотя бы просто переведу??ъ 02:32

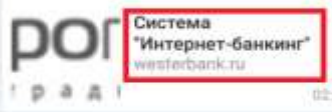
пожалуйста 02:33

Дим а там сверху написано что за банк 02:37

БЕЛАГРОПРОМБАНК 02:37

сейчас минуточку 02:37

я создал заявку зайди подтверди просто все



02:40

[redacted]... У меня что-то с интернет банкингом 02:44

подожди а у тебя карта не блокирована??? 02:44

у меня вообще ошибку выбило 02:44

Смс не приходит на номер 02:44

Не, норм всё

Короче [redacted] не могу зайти в банкинг свой 02:45

Спроси кого другого 02:45

блин ну ты не уходи еще я что то придумаю 02:46

ок? 02:46

Ну давай 02:47

подожди а у тебя сеансовые ключи есть? 02:48

[redacted] я сейчас не дома, а карточка с ключами там осталась 02:49

Короче я не могу зайти в банкинг...

а можешь тогда смс код сказать который приет 02:49

мб тех работы?? 02:50

скажи пожалуйста 02:50

мб так получится 02:50

Ооооо 02:50

Пришёл код 02:50

Только что 02:50

Ща погодь 02:50

жду 02:51

Ну вроде зашёл 02:52

жду 02:51

Ну вроде зашёл 02:52

Вот такую шнягу написало 02:52

а что ты ввел? 02:52

покажи 02:53

Ну код, который мне пришёл 02:53

Смс 02:53

На телефон 02:53

а что за код вообще 02:53

как он выглядит 02:53

Ну цифры 02:54

05281 02:54

Типо такого 02:54

Ну что? 02:55

грузит что то 02:57

скажи код 03:02

подтверждение перевода 03:02

Дим 03:03

??? 03:04

ауу 03:04

Димаа 03:06

Что за [redacted]? 03:10

Я только потом догнал что тут что-то неладное) 03:11

Ну как будем поступать? 03:13

03:19

От тебя не ожидал такого, ты видимо у [redacted] этого набрался 03:20

Схема «Звонок сотрудника»

Суть: неизвестный звонит в мессенджере (чаще в Viber), при этом в качестве фотографии контакта используется логотип банка или какого-либо гос. учреждения, имя контакта - идентично названию банка / гос. учреждения. **Мошенник представляется сотрудником банка (правоохранительных органов, Национального банка и т.д.) и сообщает, что на ваше имя кто-то пытается оформить кредит в банке или рассказывает легенду о преступниках, которые пытаются незаконно использовать вашу карточку, списать с нее деньги.**

Нередко мошенник, представившийся «сотрудником» правоохранительных органов (МВД, КГБ, прокуратуры и т.д.), настойчиво предлагает **стать участником «спецоперации»** по выявлению недобросовестного работника банка. Для большей убедительности «сотрудник» может прислать фотографию удостоверения (конечно, поддельного).

Далее мошенник может прислать **ссылку** на скачивание «специального» приложения (чаще это **приложения по удаленному управлению телефоном** – RustDesk, AnyDesk, TeamViewer, Ассистент, Webkey и др.). Такие приложения позволяют мошеннику управлять телефоном (входить в банковские приложения, просматривать СМС-сообщения), а главное – дают возможность украсть деньги.

Мошенник также может попросить «жертву»:

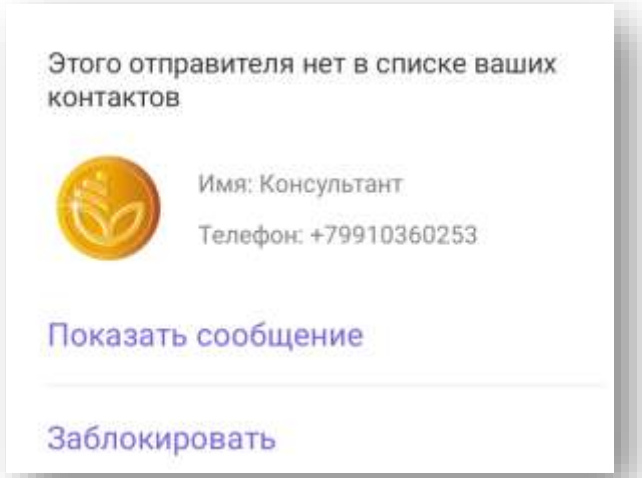
-продиктовать ему полный номер карточки, «сверить» паспортные данные, значения СМС-кодов, логин и пароль от Интернет-банкинга и т.д.

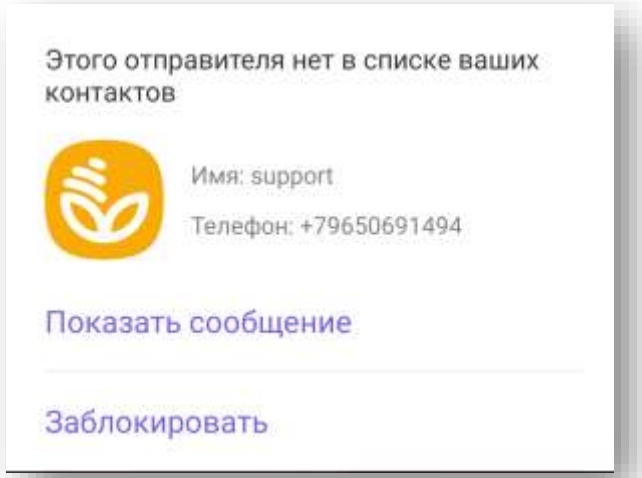
- совершить перевод денег на «безопасный» счет, оплатить некий налог, бронь, штраф и т.д. При этом мошенник диктует реквизиты для перевода.

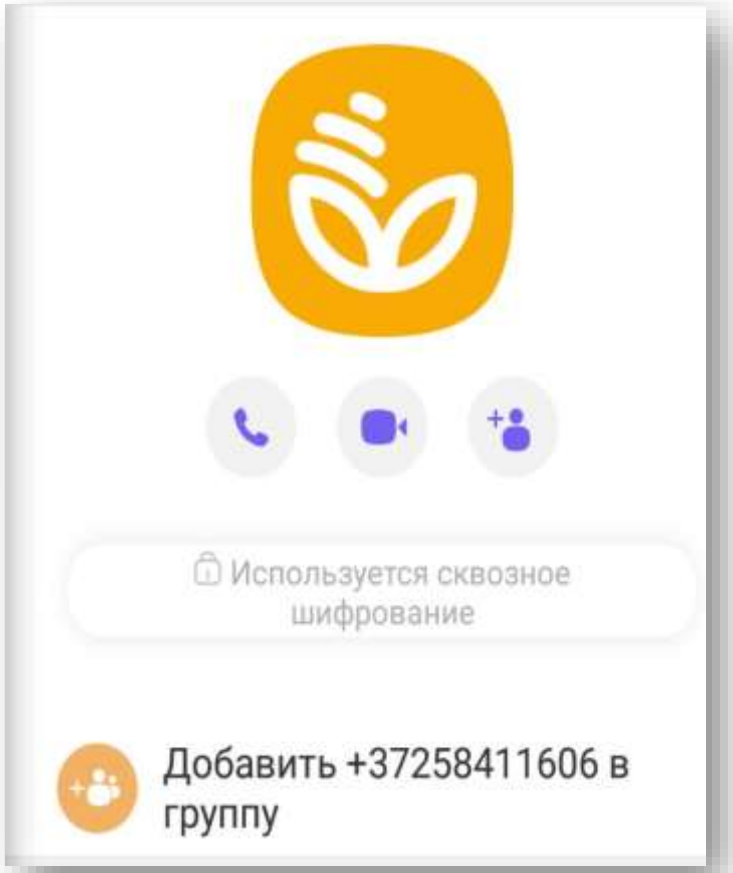
Возможные последствия в случае, если клиент сообщил мошеннику критические данные:

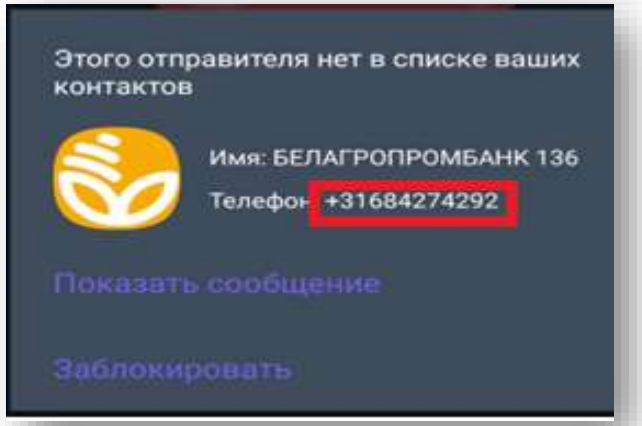
1. хищение денежных средств с карточек в Интернет-банкинге, Мобильном приложении банка;
2. открытие кредитной линии и последующее хищение денег в Интернет-банкинге, Мобильном приложении;
3. выпуск виртуальной карточки, которая, в дальнейшем, используется для перечисления денег, похищенных у других клиентов (промежуточное звено схемы обналичивания) и т.д.

Пример отображения контакта мошенника в мессенджере









«Защита от лишних звонков» в Viber

В Viber есть функция «Защита от лишних звонков», при активации которой пользователь не будет получать уведомлений о звонках с номеров, которых нет в списке его контактов.

Новая функция доступна в последней версии Viber для всех пользователей с белорусскими номерами мобильных телефонов.

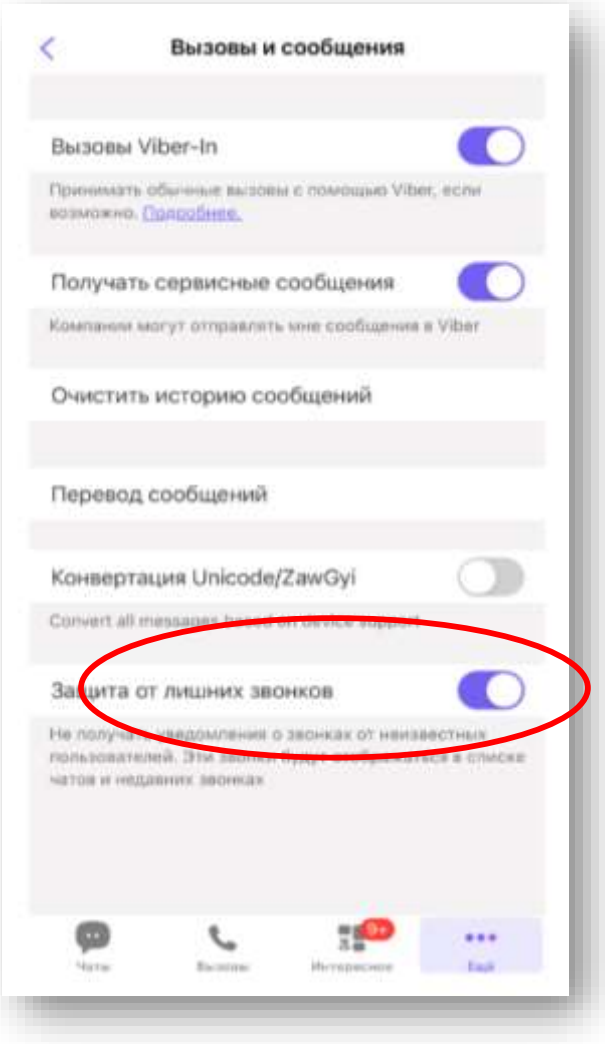
Чтобы активировать «Защиту от лишних звонков», надо:

открыть раздел «Еще»;

войти во вкладку «Настройки»;

выбрать «Вызовы и сообщения»;

включить тумблер напротив пункта «Защита от лишних звонков».



Приложение для «дополнительной безопасности»

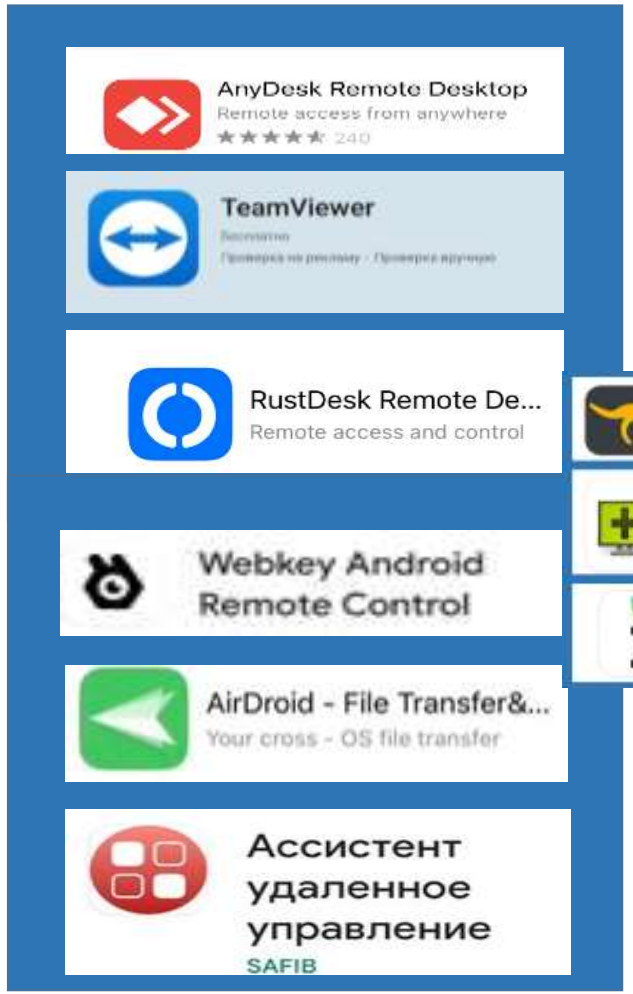
В ходе телефонного разговора мошенник может предложить жертве установить «банковское» приложение «для защиты телефона» либо обновления «старой небезопасной» версии.

Фактически же жертва устанавливает на телефон не банковское приложение, а приложение по УДАЛЁННОМУ УПРАВЛЕНИЮ её телефоном (например, RustDesk, AnyDesk, Ассистент, Webkey).

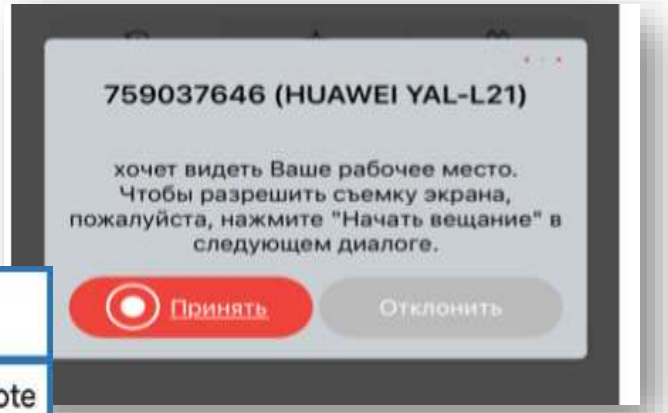
Получая доступ к телефону, мошенник может не только видеть экран устройства жертвы, читать содержание СМС, но и выполнять финансовые операции в мобильном приложении (списывать деньги с карточки жертвы).

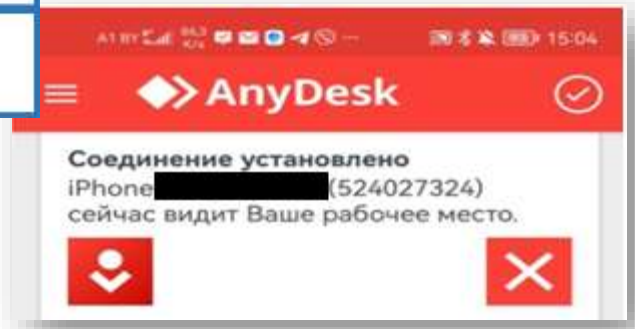
Как правило, приложения для удалённого управления предупреждают пользователя о рисках.

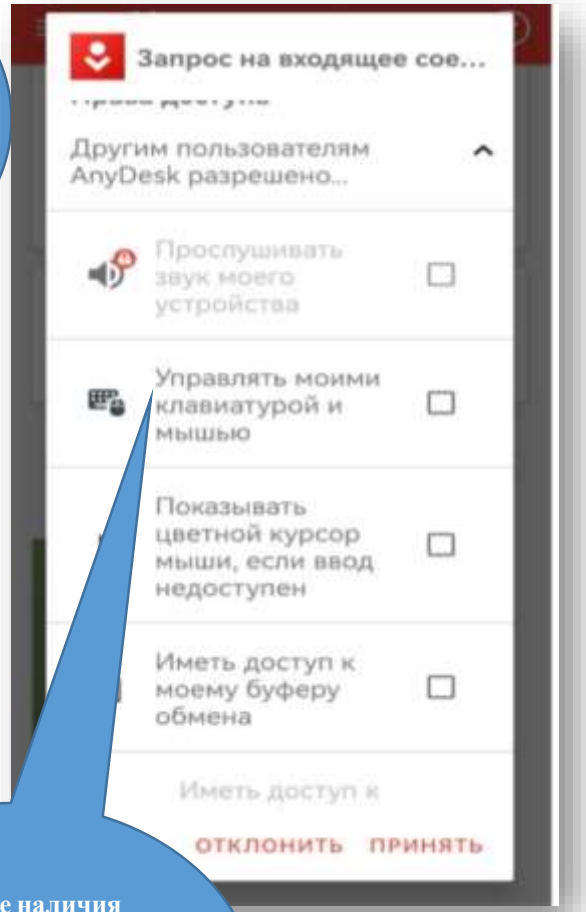
Приложения для удаленного доступа к устройству



Пароль для соединения с другим устройством (значение пароля просит сообщить мошенник для доступа к телефону жертвы)







В случае наличия отметки в данных функциях, мошенник сможет не только просматривать экран устройства жертвы, но и управлять им

Схема «Ложный босс»

Суть схемы: мошенники собирают сведения о работниках интересующей компании – сделать это достаточно легко посредством тематических чатов и каналов в мессенджерах, в соцсетях. Далее *злоумышленник регистрирует в мессенджере* (чаще в Telegram) *поддельный аккаунт на имя руководителя компании*: в аккаунте указывают ФИО руководителя, добавляют его фотографию - все это также получено из открытых источников сети Интернет. **Цель:** введение в заблуждение подчиненного персонала.

Мошенник с поддельного аккаунта «руководителя компании» осуществляет общение с работниками компании. Изначально переписка может вестись на бытовые темы, после чего «руководитель» указывает «своему» работнику на *необходимость общения с неким представителем правоохранительных органов (или какого-либо надзорного органа),* который в скором времени должен будет перезвонить (см. скрин).

Через некоторое время работнику поступает звонок от «представителя правоохранительных органов», который в ходе диалога **требует следовать его инструкциям**, например:

- скачать приложение по удаленному управлению телефоном;
- сфотографировать и переслать ему фото карточки;
- перевести деньги на «защищенный банковский счет» и т.д.

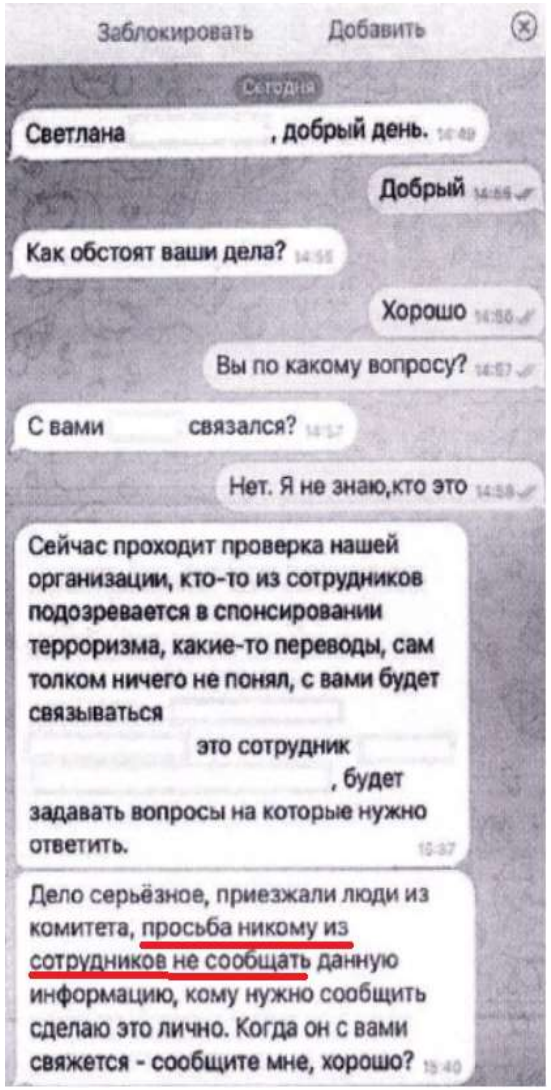


Схема «Спецоперация «Кредит». Квест

Суть квеста: мошенник, представляясь сотрудником Национального банка (МВД, КГБ или другого государственного органа), сообщает, что на имя гражданина (и без его ведома) некто оформил кредит в банке. Под подозрением все и особенно сотрудники банка! И, безусловно, без помощи клиента никак не обойтись.

Условия квеста предельно просты: необходимо *лично* обратиться в банк и оформить кредит на карточку (при этом не подавать вида, что проводится спецоперация по «вычислению» злоумышленника!). Подтверждением успешного прохождения являются реквизиты только что полученной в банке кредитной карточки.

К сожалению, финал квеста для незадачливого клиента обычно печален: мошенники – с деньгами, а клиент – с платежами по кредиту.

Схема «Оператор связи»

Описание схемы:

1. Мошенник **под видом сотрудника службы поддержки оператора связи А1** (МТС, Life, Белтелеком) связывается с клиентом по телефону либо в мессенджерах (Viber, Telegram, WhatsApp).
2. Лже-сотрудник **рассказывает легенду** о том, что нужно «продлить срок действия сим-карты или договора», о «жалобах других абонентов на спам-рассылку с вашего номера», про «сторонние сессии с нескольких телефонов в мобильном приложении» и т.п.
3. Лже-сотрудник, как правило, уточняет у клиента вид операционной системы его телефона: Android или iOS? Затем уточняет установлено ли на телефоне приложение «Мой А1» / «My A1» («Мой МТС», «Мой Белтелеком»)?
4. * Если такого приложения нет, то лже-сотрудник настойчиво требует установить программу на телефон.
   * Если приложение уже есть, заверяет, что надо его «обновить».
   Когда «жертва» соглашается, приходит ссылка для скачивания файла формата «*.apk»** (установочный файл).
   ВАЖНО! Ссылка на скачивание ведет не в официальный магазин приложений. Ссылка направляется личным сообщением в мессенджере.
5. Как только приложение загружается на телефон мошенник получает полный доступ ко всем данным хранящимся на телефоне, в т.ч.:
   к логинам и паролям к банковским приложениям;
   к контактам и **СМС-сообщениям**;
   доступ к управлению мессенджерами;
   доступ к камере, микрофону, **ко всем файлам в памяти телефона**.
6. Мошенники, получив сведения с телефона, используют их для получения денег, например, путем **хищения со счетов через системы дистанционного банковского обслуживания или шантажа.**

Что представляет собой файл, ссылку на который направляет мошенник?

Это вредоносный файл (содержит вирус), замаскированный под официальное приложение оператора связи.

Задачи вируса:

1. Получить полный доступ к памяти телефона «жертвы», собрать максимально возможное количество данных и передать их в «командный» пункт, т.е. на устройство мошенника.
2. Получить доступ к удаленному управлению устройством «жертвы».

Что делать?

1. **Отключить интернет** на мобильном телефоне.
   Передача собранных вирусом данных возможна только при включенном интернете.
2. **Осуществить на телефоне «сброс до заводских настроек».**
   Удаление только ярлыка скаченного приложения недостаточно, т.к. ярлык – это всего лишь обманка, которая рассчитана на то, что «жертва» удалит фальшивый ярлык приложения и успокоится, а на самом деле вирус скрытно будет продолжать передавать данные мошенникам и управлять телефоном.
3. **Сменить логины и пароли ко всем приложениям (особенно банковским), установленным на телефоне**, а также к аккаунтам, в которые когда-либо осуществлялся вход через браузер телефона. Выполнить только после п.2, не раньше.
4. В случае, если в период, когда на телефоне было установлено вредоносное приложение, на телефон **приходили СМС-сообщения с кодами** – незамедлительно обратиться в службы поддержки данных организаций. Например, если приходило сообщение от «msi-erip» – по телефону 141, если от «А1» – по номеру 7107 и т.д.

Почему люди «ведутся»?

Эффект «дымовой завесы».

Мошенник говорит много слов, которые выступают как «дымовая завеса». У обывателя, не привыкшего к бюрократическому языку и сложным конструкциям, сознание не в состоянии долго держать под пристальным вниманием такой разговор. Оно начинает «выключаться» и такое состояние отлично позволяет пропустить тот момент, когда мошенник как раз начинает выяснять нужную информацию или просить сделать что-то, что поможет ему получить деньги.

Использование терминов к месту и не к месту вызывает у человека уверенность, что он говорит с профессионалом и действительно сотрудником банка.

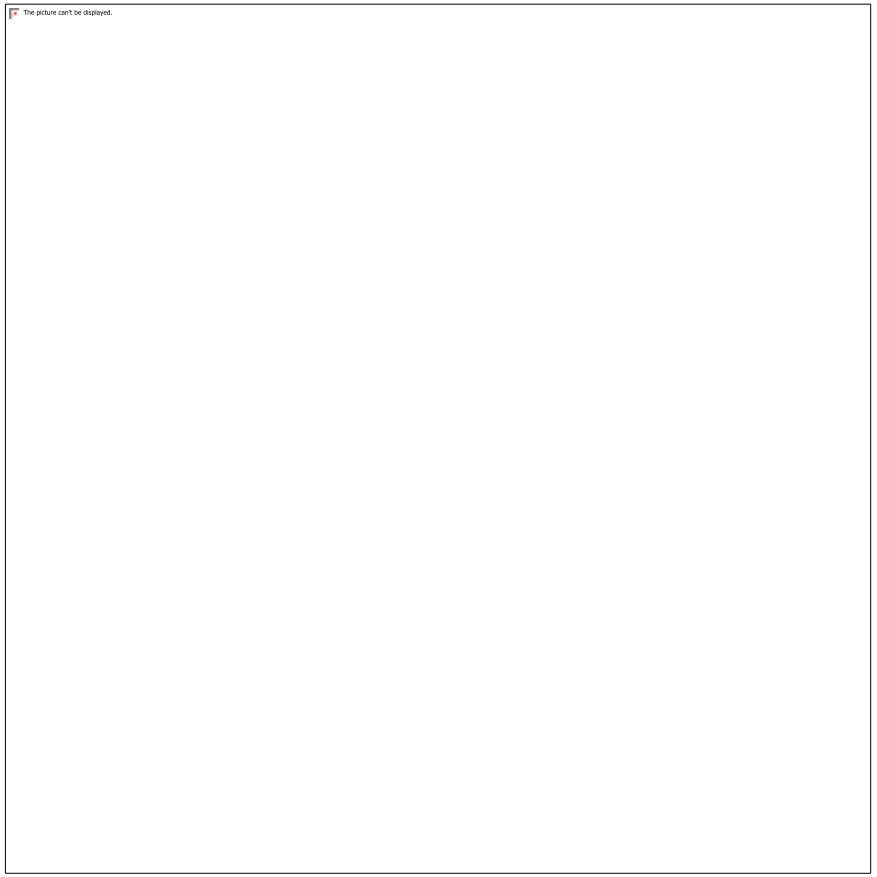
Чувство вины.

Если человек начинает сомневаться в честности звонящего, тот пытается «надавить» на него. Мошенник вызывает у клиента чувство вины: он может потерять деньги из-за своей нерасторопности.

«Из-за Вас и Вашего недоверия мы не несем ответственности за Ваши деньги, Вы их потеряете!» и т.д. Цель этих фраз – создать у человека тревогу и ощущение будто он мешает сотруднику и теряет прямо сейчас свои деньги, и заставить его передать необходимые мошеннику данные.

Чувство страха.

Мошенник пытается сыграть на страхе клиента потерять деньги навсегда. Использует фразы типа: «Вы даете голосовой отказ от предоставления информации». Мошенник пытается надавить на страх человека перед ответственностью за свои действия: подтвердив отказ, он уже не сможет вернуть все назад и сам будет разбираться со своей проблемой.



Как на 100% распознать телефонного мошенника?

12 признаков, которые должны вас насторожить:

1. Вам звонят на мобильный телефон из мессенджера (чаще, Viber).

Сотрудники Белагропромбанка НИКОГДА НЕ ЗВОНЯТ НА VIBER и не используют для связи с клиентом мессенджеры.

2. Звонок с иностранного номера.

Проверьте номер абонента. Международный код Беларуси: +375 - в остальных случаях звонки стоит игнорировать и не пытаться перезвонить подозрительному абоненту.

3. Звонок поступает в ночное или позднее время.

Мошенник рассчитывает застать собеседника врасплох: спросонья у человека недостаточно концентрации, чтобы распознать мошенника.

4. «Сотрудник» отказывается назвать свое ФИО и должность.

На самом деле «проверить» сотрудника очень просто: перезвоните по официальному номеру банка – тому, который указан на сайте, и уточните работает ли в банке такой сотрудник и в каком подразделении.

5. «Сотрудник», якобы для повышения степени защищенности мобильного приложения, Интернет-банкинга или восстановления доступа к счету, настоятельно рекомендует установить неизвестное (сомнительное) приложение.

Зачастую мошенник просит установить приложение для удаленного доступа (AnyDesk, RustDesk, Assistant, Webkey, Airdroid, ISL Remote Control) к мобильному телефону «жертвы».

6. Собеседник не может ответить на простые вопросы.

Например, собеседник не может назвать: ваше ФИО; полный номер карточки, с которой, якобы, осуществляется списание денежных средств. Не знает адрес центрального офиса банка, номер Контакт-центра и т.д.

Как на 100% распознать телефонного мошенника?

7. Неизвестный просит вас (под различными предлогами) продиктовать ему полный номер карточки, паспортные данные, значения смс-кодов, логин и пароль от Интернет-банкинга и т.д.
Рекомендуем спокойно прервать разговор с мошенником и обратиться в банк.

8. Собеседник под любым предлогом просит совершить перевод денег на какой-то «безопасный» счет, оплатить некий налог, бронь, штраф и т.д. При этом неизвестный диктует реквизиты для перевода. Переводить деньги по таким реквизитам нельзя, даже если легенда кажется убедительной.

9. Неизвестный представился «сотрудником» банка или правоохранительных органов и рассказывает легенду о том, что он сейчас ищет сотрудника банка, который обманывает клиентов, и для помощи в расследовании просит вас оформить кредит. **Это обман!**

10. Неизвестный, якобы, звонит от лица популярного онлайн-магазина и рассказывает легенду о том, что на ваше имя по ошибке оформлен заказ или кредит на покупку. Для отмены заказа / кредита необходимо продиктовать паспортные данные и значения смс-кодов. **Это обман!**

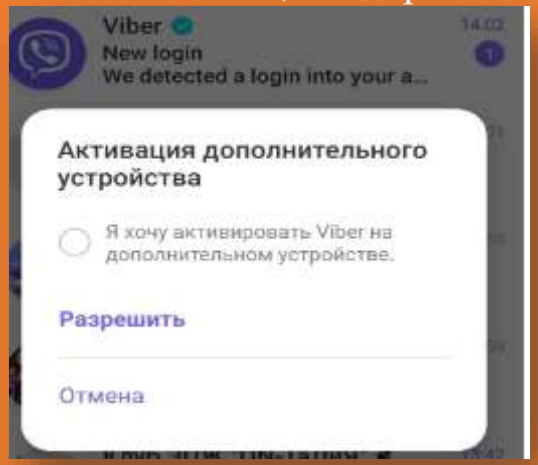
11. Собеседник рисует перед вами пугающие сценарии и морально давит на вас.
Требует немедленно принять решение о переводе денег или сообщить данные, иначе – заблокирует счет или карточку, начислит штраф за кредит и т.д. Запомните: несколько минут ничего не решат. Скажите, что вам нужно подумать и положите трубку. Затем перезвоните по официальному номеру банка, который указан на сайте, и спокойно разберитесь в ситуации.

12. Вы на 100% не уверены в том, откуда исходит звонок или кто именно вам звонит.
Скажите, что вы заняты или не можете разговаривать в данный момент. Попросите вам перезвонить позже – так у вас будет время на то, чтобы проверить номер телефона, с которого вам звонили. К тому же, мошенники далеко не всегда перезванивают повторно, предпочитая решать задачу за один звонок.

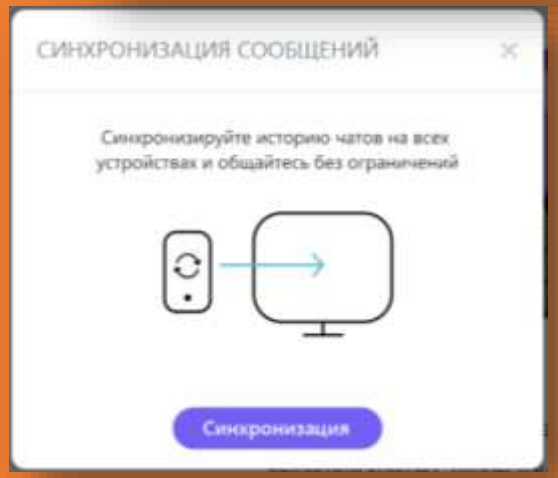
Кража аккаунта в мессенджере (на примере Viber)

В мессенджер от неизвестного абонента либо от знакомых, если они уже были «взломаны», поступает сообщение, содержащее ссылку.

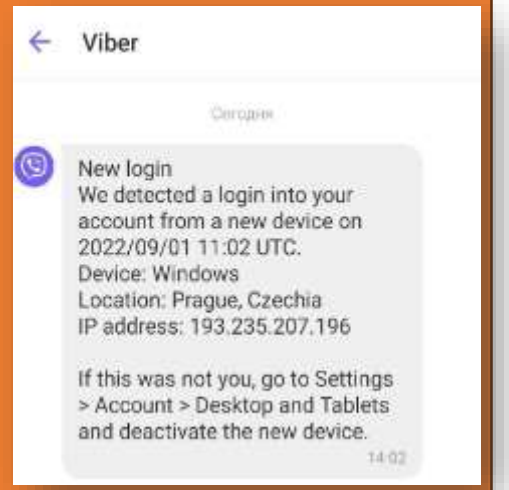
После клика по ссылке на экране телефона появляется сообщение-запрос о добавлении дополнительного устройства к вашему аккаунту.



Зачастую в спешке и по невнимательности пользователи дают разрешение на добавление нового устройства, тем самым предоставляя доступ мошеннику к своему аккаунту.



Viber направляет предупреждение о попытке добавить новое устройство к вашему аккаунту (как правило, оно содержит информацию о геолокации устройства и его ip-адресе).

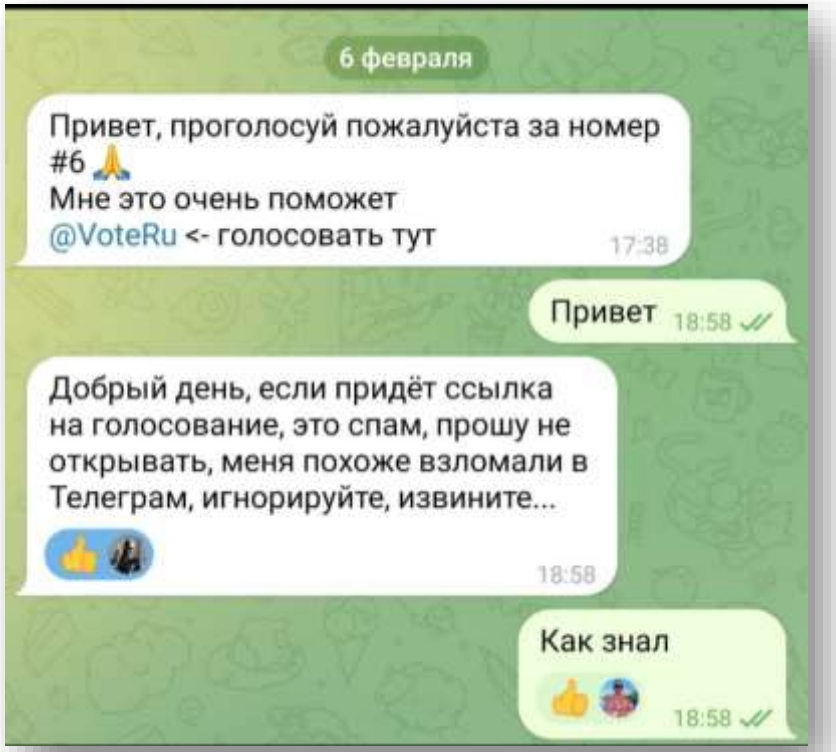


Получив доступ к вашему аккаунту в мессенджере, мошенники могут осуществлять звонки с вашего номера другим гражданам в преступных целях (обман, вымогательство, хищение денег).

Удалить доступ к аккаунту с других устройств:
Перейдите в меню «Настройки» - «Учетная запись»-«Компьютеры и планшеты», выберите устройство, которое нужно удалить, и нажмите «Деактивировать».

Кража аккаунта в мессенджере (на примере Telegram)

Пользователь получает сообщение от одного из своих контактов с просьбой о принятии участия в голосовании. Для голосования предоставляется ссылка, которая ведет на фишинговый ресурс.

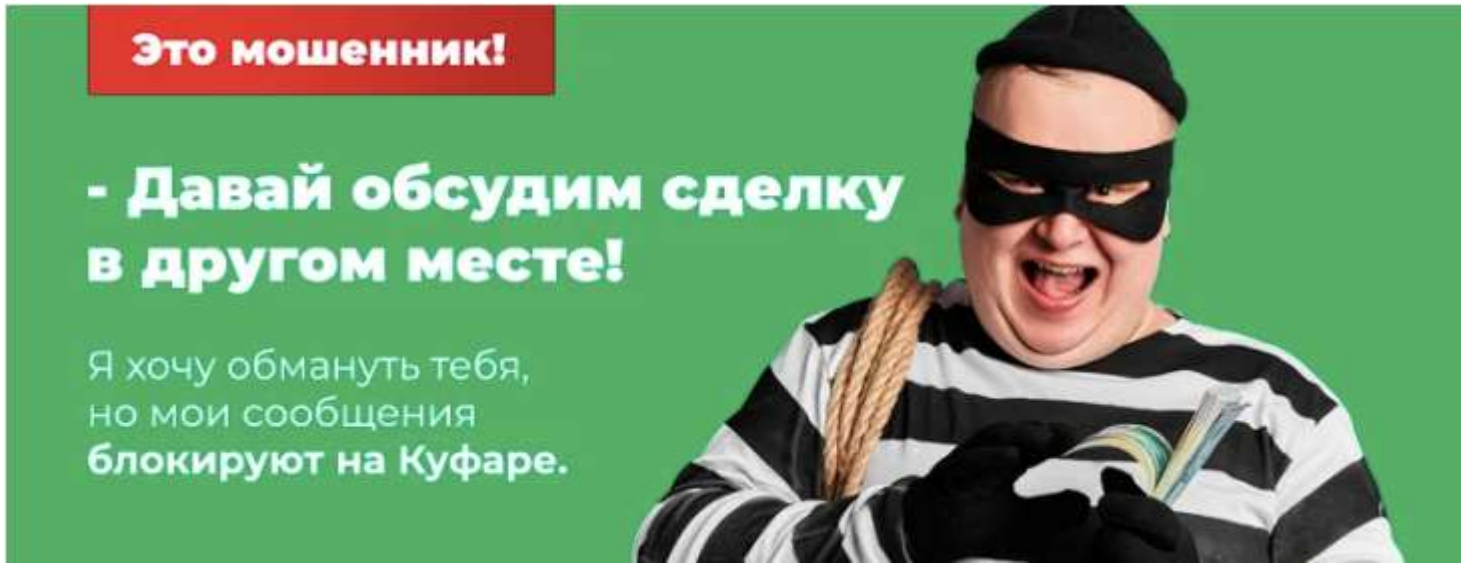


При попытке проголосовать ресурс запрашивает номер телефона и код, якобы для голосования.

Как только жертва вводит код в предложенное окошко, мошенник или бот получает ключ для захода в телеграм-аккаунт. Он получает доступ к контактам, группам, подпискам.

Как правило, со взломанного аккаунта происходит фишинговая рассылка контактам жертвы, аналогичная той, на которую она и попалась.

Схема «Куфар»



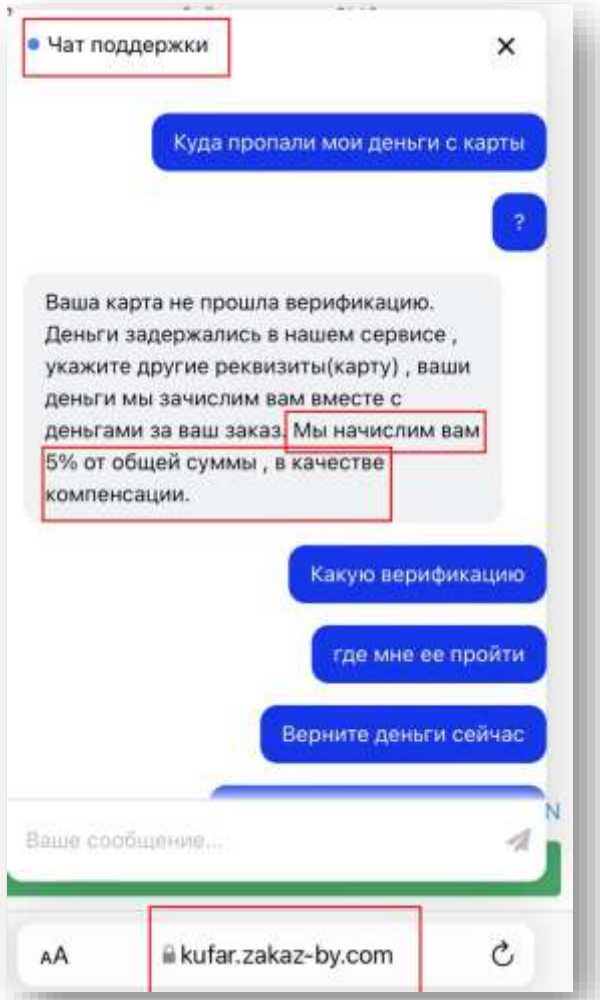
Для продавцов

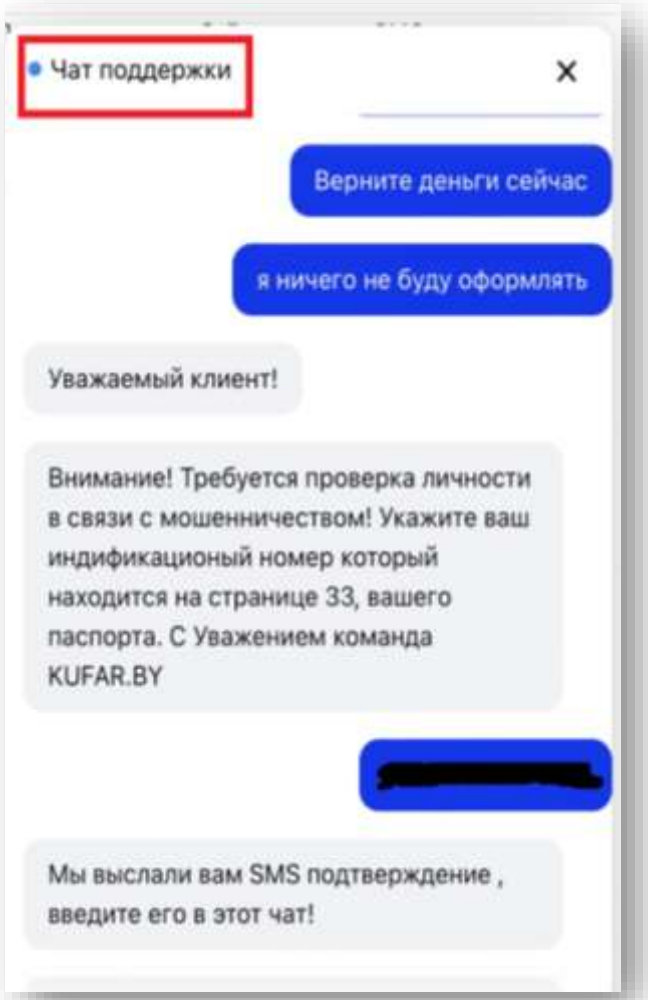
1. Мошенник находит продавца на площадке объявлений, копирует его контактные данные, но на площадке не пишет, - заблокируют. Ищет номер продавца *в мессенджерах*, представляется якобы покупателем с Куфара, говорит, что готов купить товар по предоплате.
2. Высылает продавцу *ссылку* на поддельную страницу предоплаты, где продавцу нужно ввести реквизиты своей карточки и SMS-код для того, чтобы получить деньги от покупателя.
3. Продавец денег не получает - как только он введет данные, деньги будут списаны с карточки.

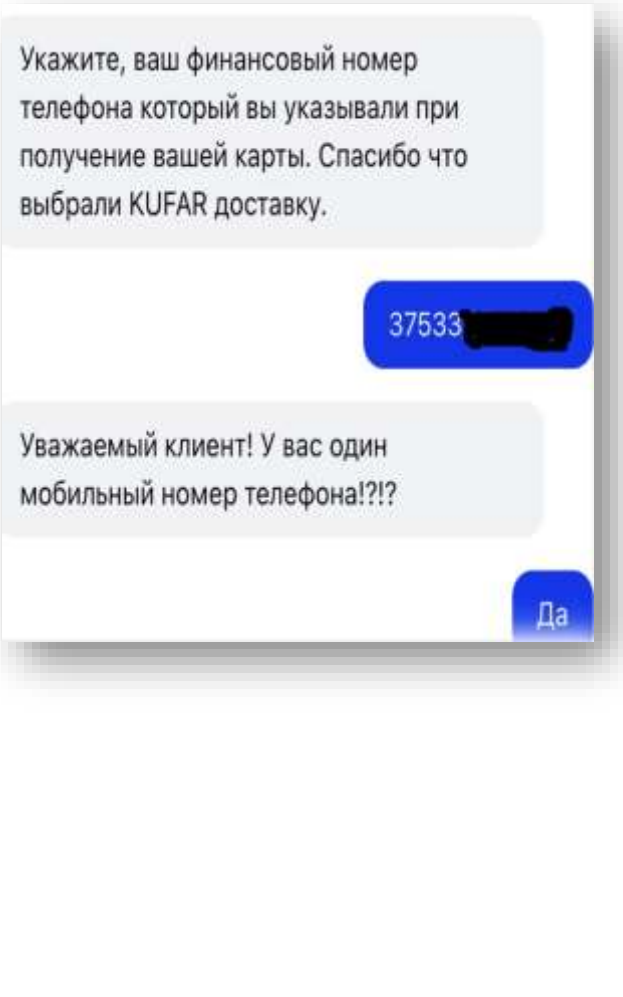
Для покупателей

1. Мошенник выставляет *товар с крайне выгодной ценой*.
2. Когда потенциальный покупатель пишет ему, под любым предлогом *предлагает перейти в мессенджер*. Говорит, что на Куфаре неудобно общаться, что в мессенджере можно созвониться и т.п.
3. Уговаривает покупателя на *предоплату* или доставку под любым предлогом: уехал из города, боится встречаться во время эпидемии коронавируса, нет времени.
4. Чтобы развеять сомнения покупателя, говорит о новой услуге холдирования (временной блокировке) средств, которая появилась на Куфаре: если доставки не будет, Куфар автоматически вернет средства на карточку.
5. Высылает покупателю *ссылку* на поддельную страницу, которая имитирует страницу Куфар Доставки, где нужно ввести данные карточки, чтобы совершить предоплату.
6. Как только пользователь вводит данные своей карточки, с него списываются деньги, посылка не приходит.

Пример переписки с компрометацией паспортных данных







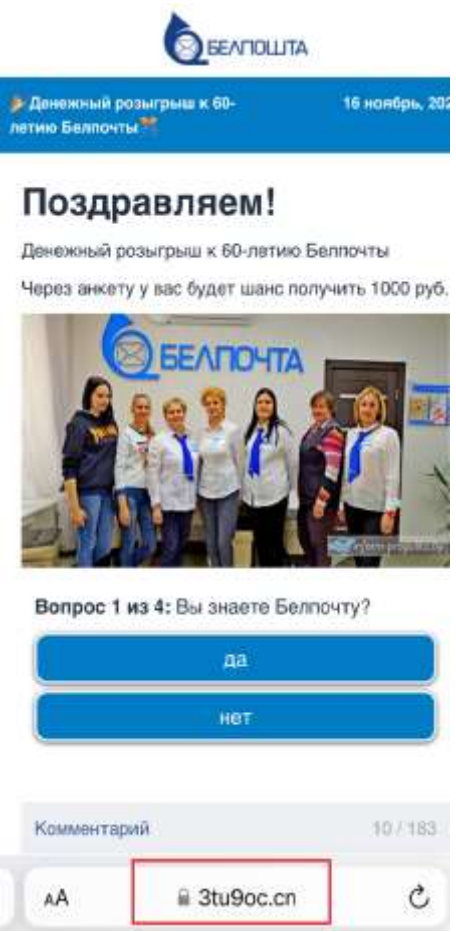
Как распознать мошенника?

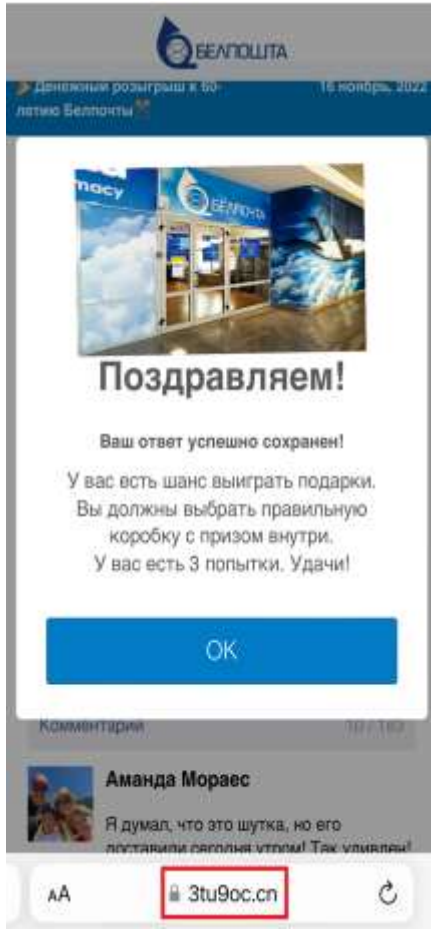
Вот 8 признаков, которые должны вас насторожить:

1. Крайне выгодная цена на товар. Не зря говорят: бесплатный сыр бывает только в мышеловке.
2. Продавец / покупатель под любым предлогом пытается перевести переписку в мессенджер (Viber, WhatsApp, Telegram).
3. Обратите внимание на номер телефона: иностранные номера – один из основных признаков того, что вы общаетесь с мошенником.
4. Предложите собеседнику созвониться: мошенник чаще избегает общения голосом.
5. Вам присылают какие-то ссылки. Тут все просто: либо фишинговый (поддельный) сайт, либо троян (вирус).
Если вы все-таки перешли по ссылке, то обратите внимание на позиции, которые предлагается заполнить для оформления перевода денег. Позиции «остаток на карточке», «код-подтверждение», «личный (идентификационный) номер паспорта» - верный признак того, что сайт поддельный.
6. Собеседник предлагает оформить оплату через некий сайт, при этом использует такие вызывающие доверие выражения как «надежная покупка», «безопасная покупка».
7. Собеседник под любым предлогом просит совершить перевод денег на какой-то «безопасный» счет, оплатить некий налог, бронь, штраф и т.д. При этом неизвестный диктует реквизиты для перевода. Переводить деньги по таким реквизитам нельзя, даже если легенда кажется убедительной.
8. Фейковая служба поддержки. Чаще всего поддельная служба поддержки «включается» в работу, когда, к сожалению, человек уже доверился мошеннику и перевел ему денежные средства. Служба поддержки предлагает вернуть списанные средства… через этот же поддельный сайт.

ВАЖНО! Используйте для расчетов в Интернете виртуальную карточку.
ПОМНИТЕ! Для перевода денежных средств на вашу карточку отправителю достаточно знать только полный номер карточки и иногда – срок ее действия. Больше ничего.

Схема «Розыгрыш». Сценарий №1





Через рекламу в соцсетях пользователю предлагают поучаствовать в опросе или конкурсе. Цель мошенника: заинтересовать потенциальную жертву щедрой суммой (при этом сумма выглядит реалистичной и некруглой – для большей правдоподобности).

На заключительном этапе респонденту **предлагается сделать репост** у себя в аккаунте или **разослать сообщение об акции** нескольким своим контактам. Такое условие мошенники, вероятно, используют для дальнейшего распространения спама.

Забрать выигрыш можно заплатив небольшую «комиссию». Победителя перенаправляют на фишинговый ресурс, где он должен ввести данные банковской карточки. В итоге жертва теряет деньги, уплаченные в счет «комиссии», и компрометирует реквизиты карточки.

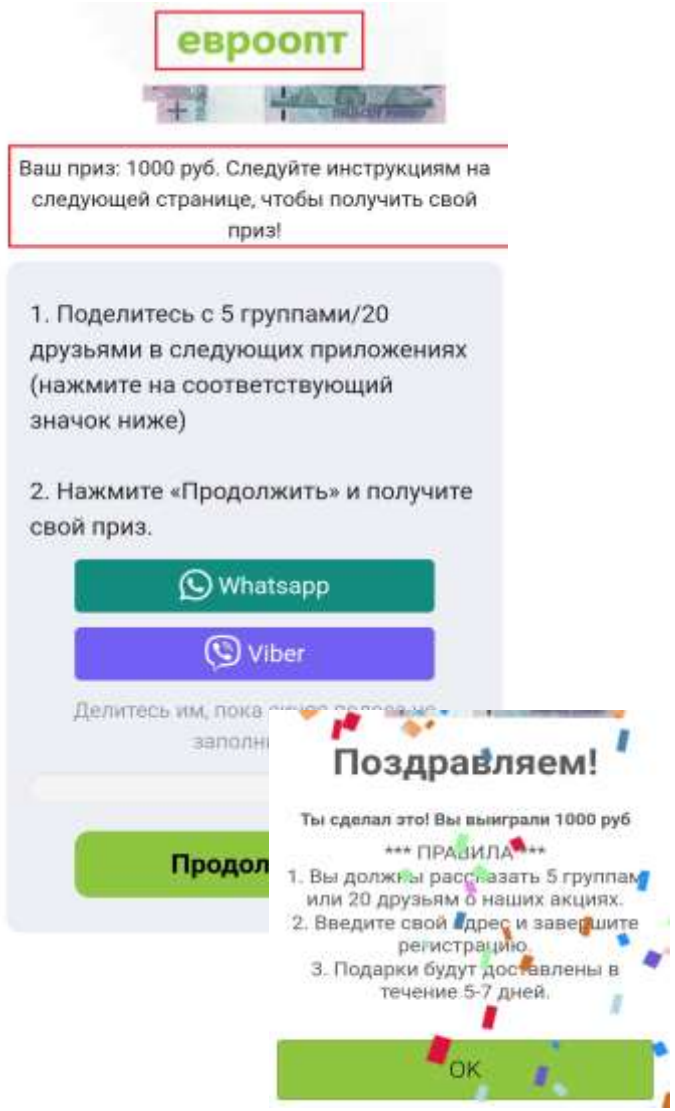


Схема «Розыгрыш». Сценарий №2

«Коробочки»

Виртуальное воспроизведение аферы «наперстки».

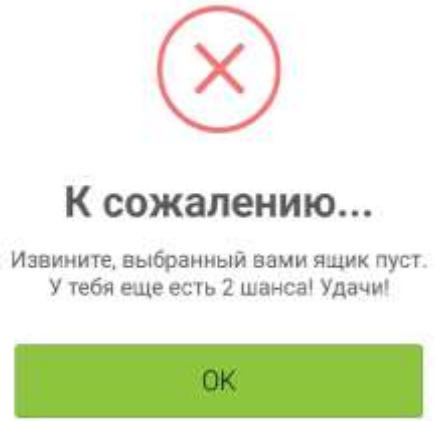
Пользователю дают три попытки, чтобы выбрать коробку с призом.

После нескольких неудачных попыток пользователь «натыкается» на приз. Далее - стандартная фраза о необходимости оплатить комиссию.

Важно!

На фейковых сайтах мошенники часто используют названия крупных компаний, банков.

Под рекламными постами (сообщениями) часто встречаются фотографии счастливчиков, выигравших призы, и их отзывы. На самом деле, фотографии собраны из Интернета, а отзывы подделаны.



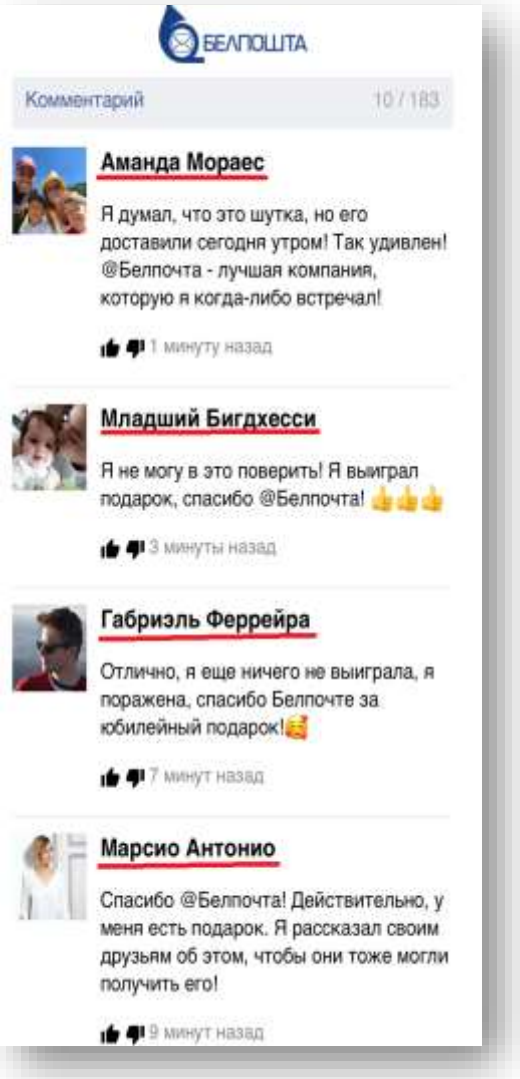
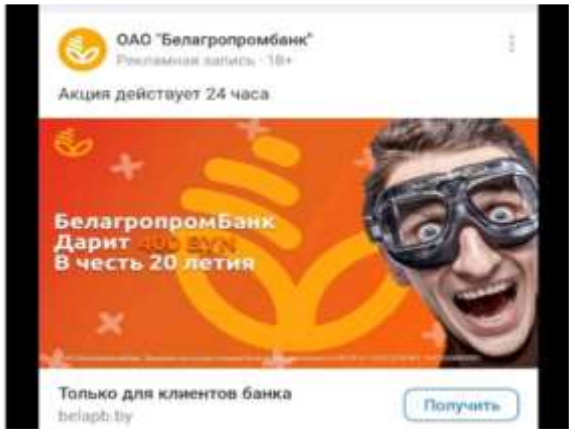
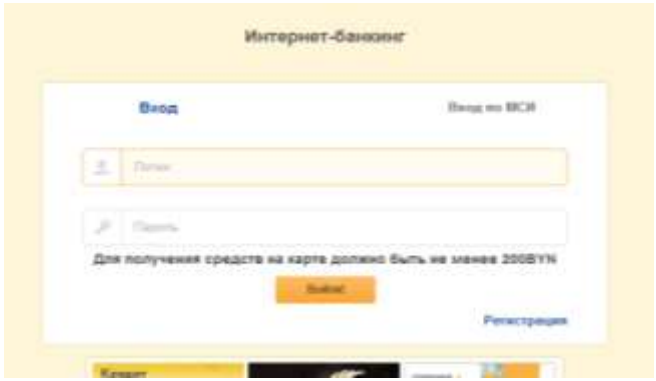


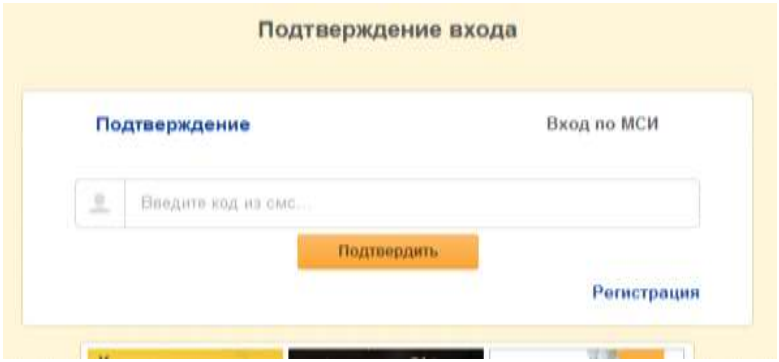
Схема «Деньги от банка»

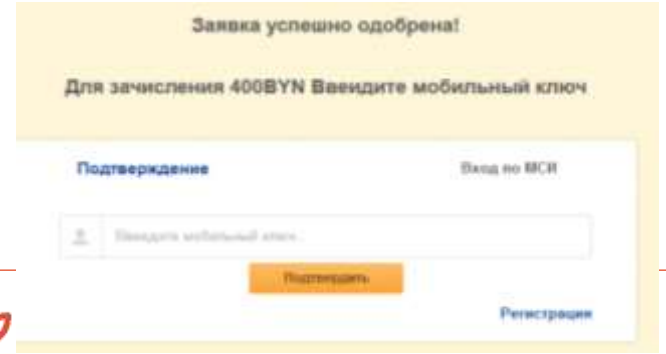


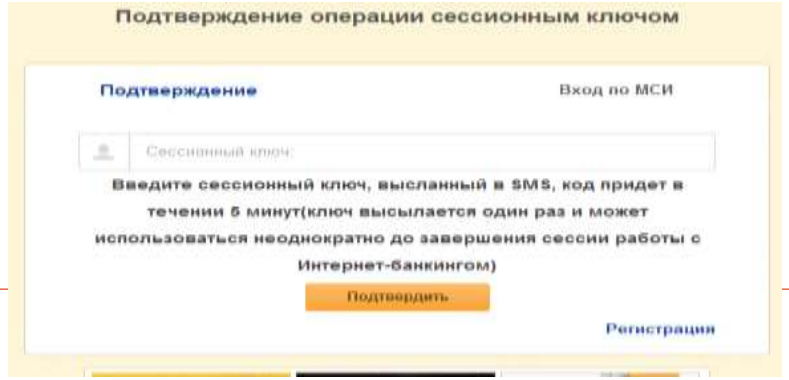
Суть: В социальных сетях нелегитимно распространяется реклама, якобы от имени Белагропромбанка, о проведении розыгрыша денежного приза.

Мошенническая реклама кликабельна и перенаправляла пользователя на фишинговый сайт, web-дизайн которого идентичен дизайну официального сайта системы «Интернет-банкинг».









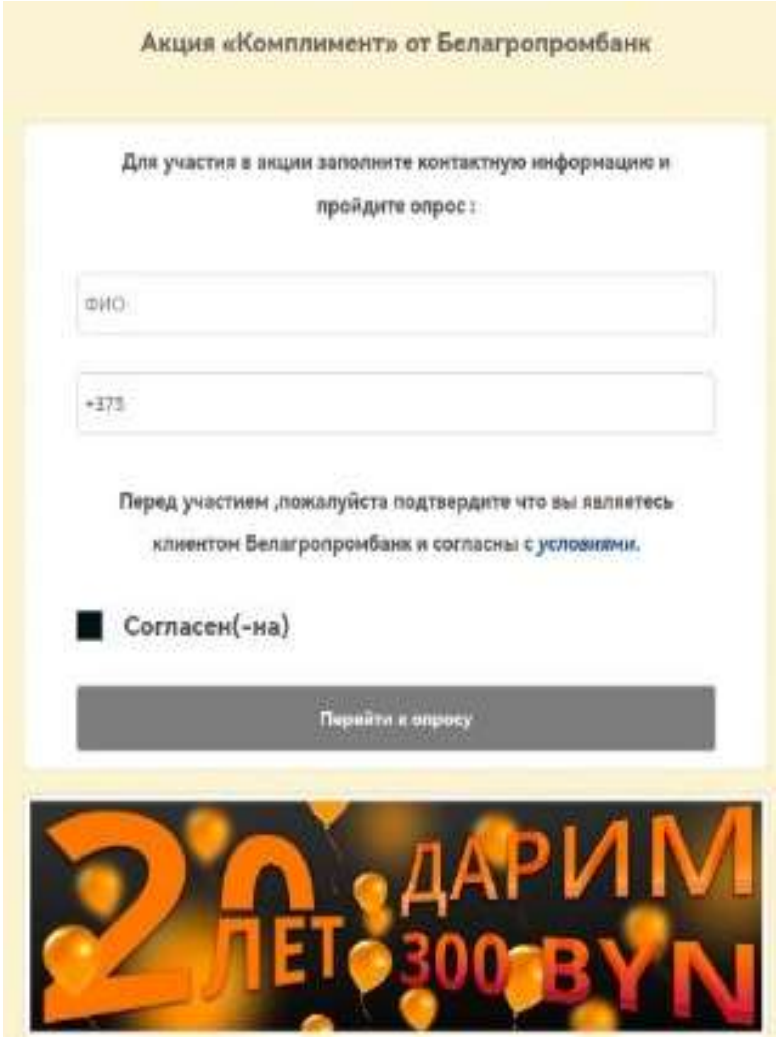


Схема «Ценные призы от банка»

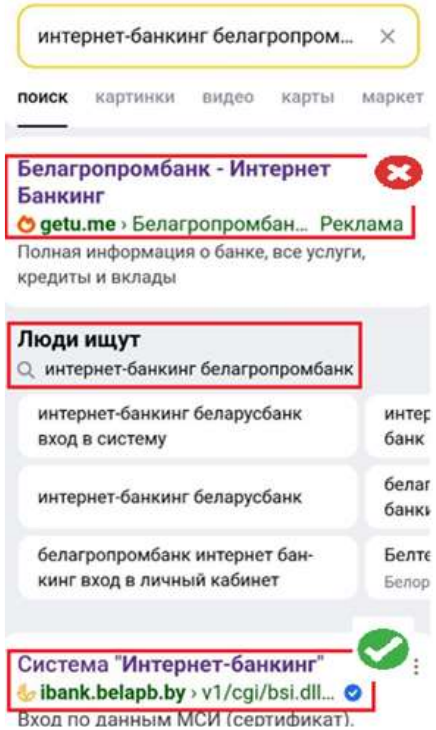
Суть: В Instagram и Facebook нелегитимно распространялась реклама, якобы от имени банка, о проведении розыгрыша ценных призов (мобильных телефонов, бытовой техники). Мошенническая реклама кликабельна и перенаправляет пользователя на фишинговый сайт, web-дизайн которого идентичен дизайну официального сайта системы «Интернет-банкинг» банка.

Схема «Фишинг. Поиск»

Суть: **Мошенники создают фишинговый сайт, внешне очень похожий на сайт системы «Интернет-банкинг» банка.**

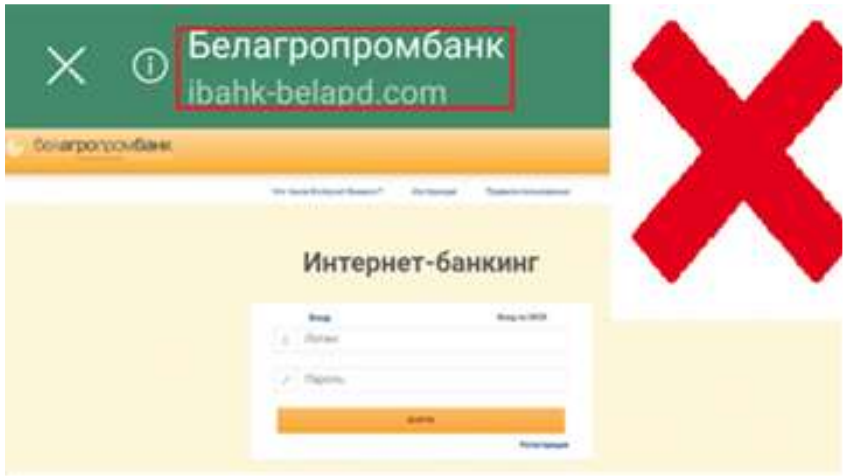
С целью «продвижения» поддельного сайта мошенники используют такие инструменты веб-маркетинга как **платная реклама**, в результате чего, **мошеннический сайт может оказаться в первых строках поисковой системы в браузере**.

Пример результата поискового запроса с фишинговым сайтом:



Пример фишингового сайта:

:



Признаки фишингового (поддельного) сайта системы «Интернет-банкинг»

1. **Неверное доменное имя, доменное имя с ошибками, домен верхнего уровня не «.BY»**.

Официальный адрес системы «Интернет-банкинг» банка - **www.ibank.belapb.by.**

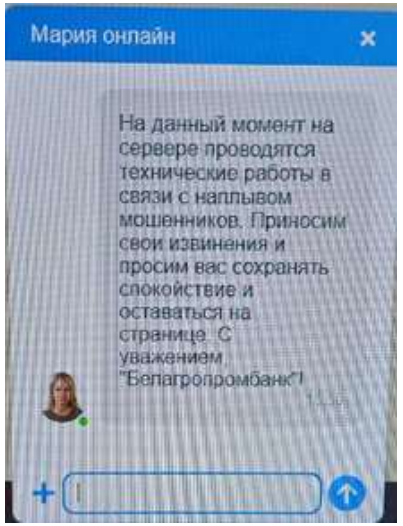
Пример адреса фишингового сайта: iba**h**k-belap**d.com**.

2. Фишинговый сайт часто после ввода на нем логина и пароля от учетной записи **«подвисает»** или **«тормозит»**, т.к. мошенникам нужно время для проверки корректности введенных потенциальной «жертвой» данных на официальном сайте «Интернет-банкинг» банка.

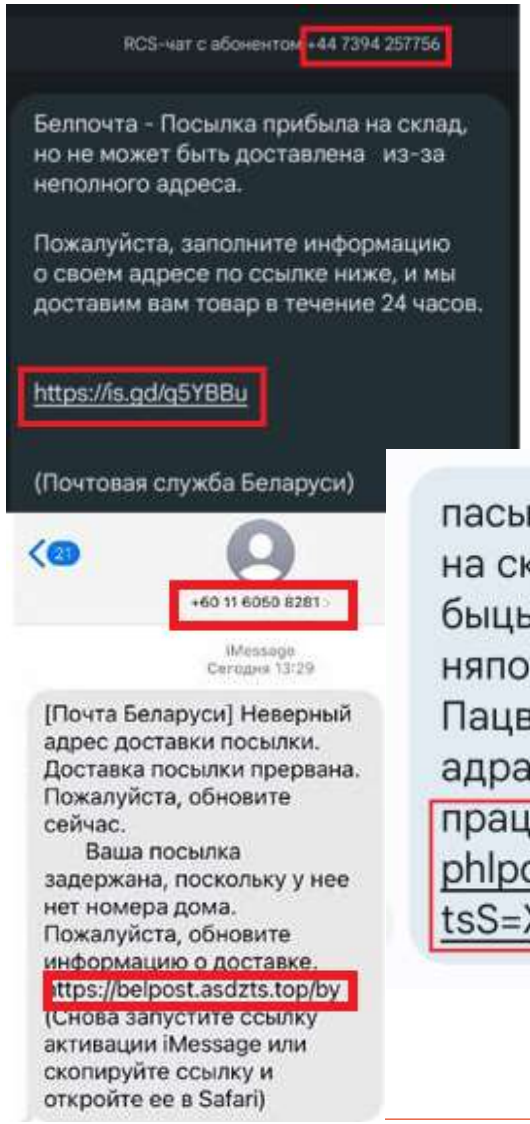
3. Под различными предлогами после ввода логина и **пароля сайт просит ввести значение СМС-кода или сеансового ключа**.

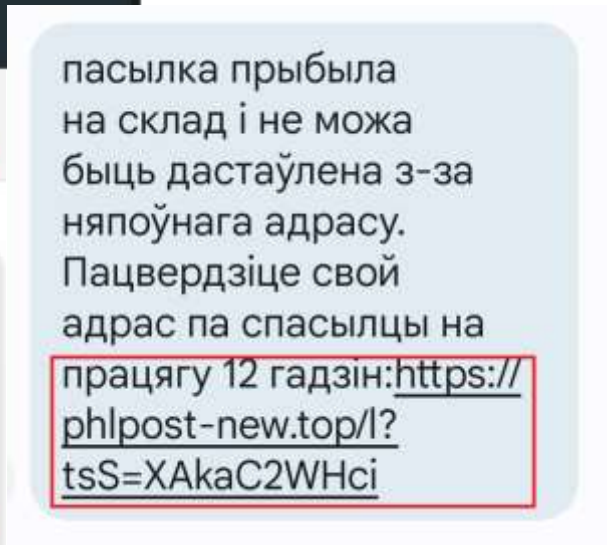
ВНИМАНИЕ! На фишинговом (поддельном) сайте может работать чат-бот с фейковой службой поддержки банка, оператор которой может попросить клиента предоставить паспортные данные, реквизиты карточки, ввести значение СМС-кода.

Пример фейковой службы поддержки:



Фишинг по мессенджеру





Мошенники от имени оператора почтовой связи направляют сообщение о необходимости уточнения адреса доставки почтового отправления, для внесения информации предлагается *пройти по ссылке*.

Ссылка перенаправляет пользователя на *поддельный сайт*, внешне похожий на сайт оператора почтовой связи. На сайте предлагается ввести уточненный адрес и оплатить услугу повторной отправки.

Что происходит на самом деле?

На поддельном (фишинговом) сайте происходит компрометация:

- реквизитов карточки;
- значения CMC-кода (3D-Secure-код);
- персональных данных.

Используются мошенниками для хищения денег с карточки

Используются мошенниками для продажи в даркнете (сегмент Интернета, скрытый от общего доступа, в связи с чем часто используется киберпреступниками для незаконной деятельности)

Квишинг. QR-код как носитель фишинга

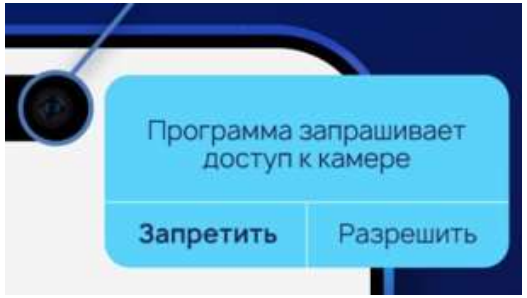
Квишинг – это форма фишинга, при которой мошенники используют QR-коды для обмана граждан и кражи как денег, так и персональных данных.

ВАЖНО. Прежде чем сканировать QR-код, подумайте, где вы его нашли: в соцсетях, в электронном письме, на неизвестном сайте или встретили на улице. *Доверять стоит только проверенным источникам, например, официальным сайтам компаний.*

QR-код – это просто другой вид отображения ссылки, поэтому обращайте внимание на ее внешний вид. Так, длинные и запутанные URL-адреса, вероятно, сигнализируют об потенциальной опасности. Например:

ВАЖНО. Если после перехода по QR-коду смартфон запрашивает доступ к камере, контактам или другой конфиденциальной информации, то *это признак мошенничества*.

Остерегайтесь QR-кодов, которые требуют дополнительного разрешения.



ВАЖНО. Если QR-код предназначен для скачивания сторонней программы, проверьте ее подлинность в официальном магазине приложений перед установкой на устройство. Поддельные утилиты могут представлять угрозу для безопасности данных.

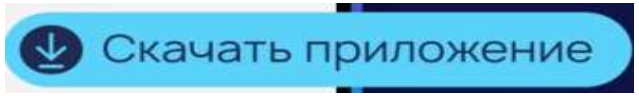
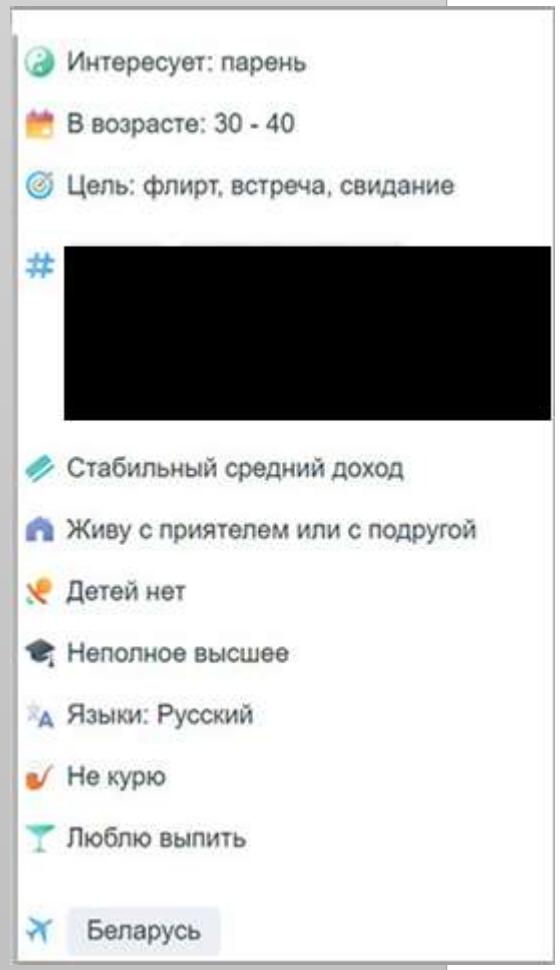


Схема «Свидание»

На форумах онлайн-знакомств мошенники, используя фотографии привлекательных девушек, знакомятся с мужчинами и обещают незабываемое свидание в кино либо театре.

Собеседница рекомендует купить билеты онлайн и сбрасывает ссылку на сайт заведения, куда предлагает пойти вечером.

Жертва проходит по ссылке и оказывается на фишинговом сайте, вводит реквизиты карточки, с которой, в последствии, списываются денежные средства.



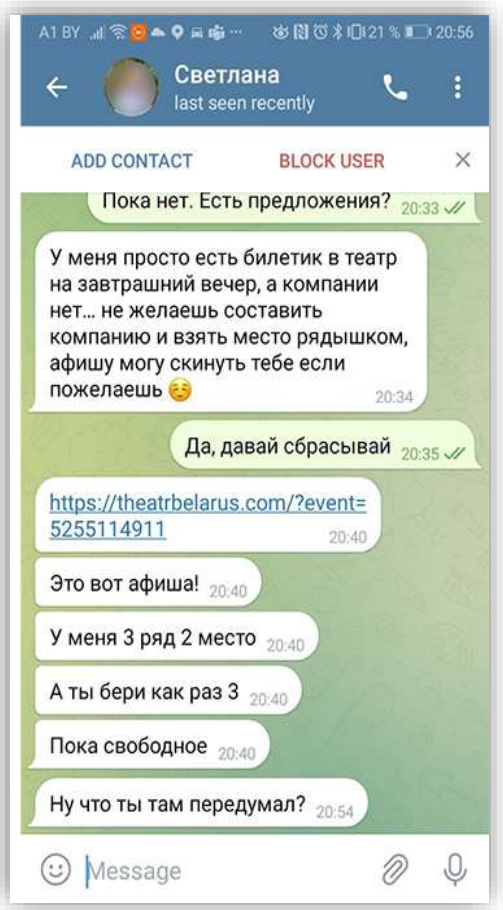
После списания денег может прийти сообщение, что заказать билеты в данный момент невозможно и для возврата списанных денег нужно ввести данные другой карточки.

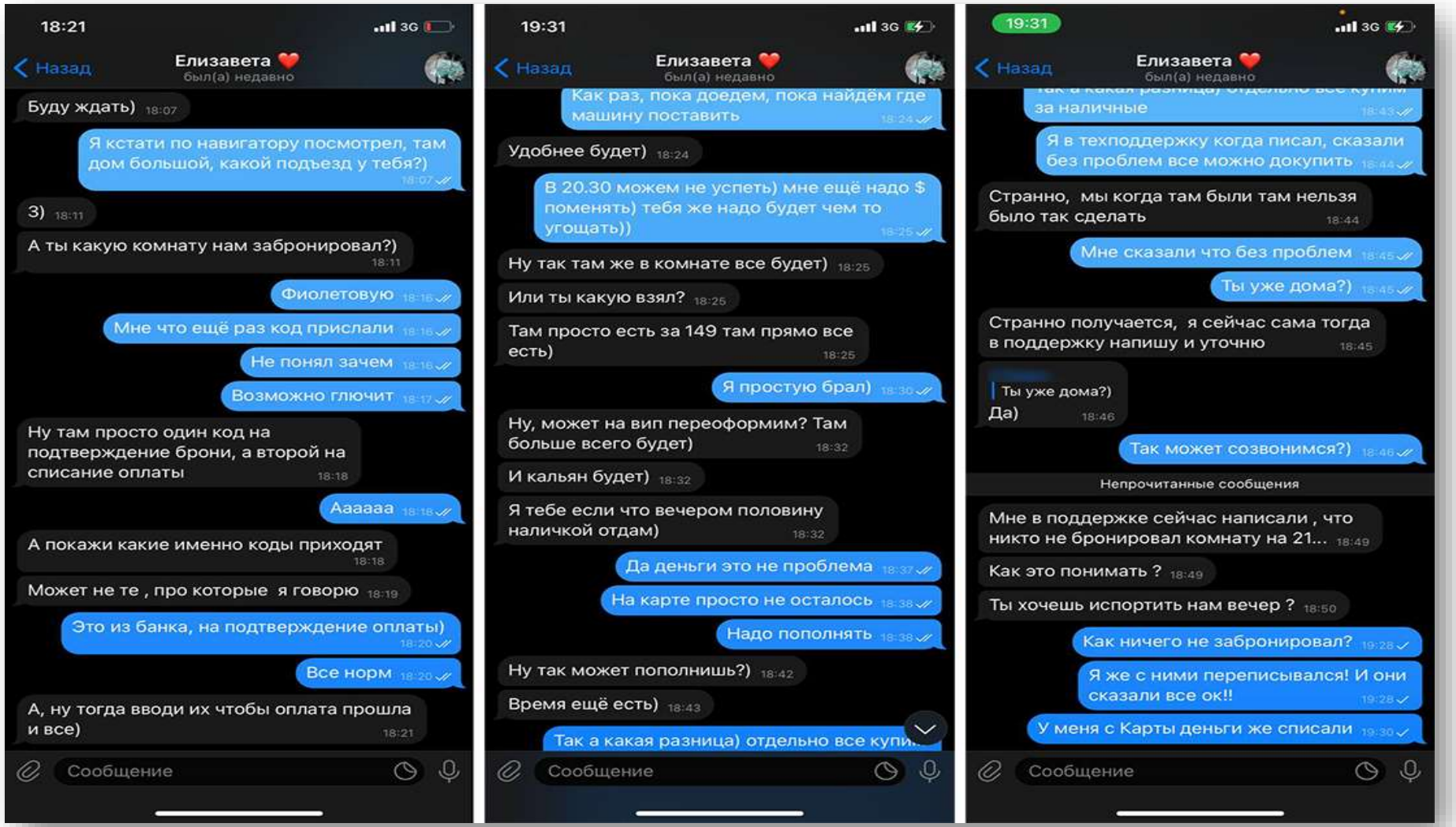
В итоге деньги списываются с обеих карточек.

Будьте осмотрительны при знакомствах в социальных сетях / мессенджерах.

НЕ ПРОХОДИТЕ по ссылкам, отправленным вам неизвестными.

Пример переписки в мессенджере (схема «Свидание»)

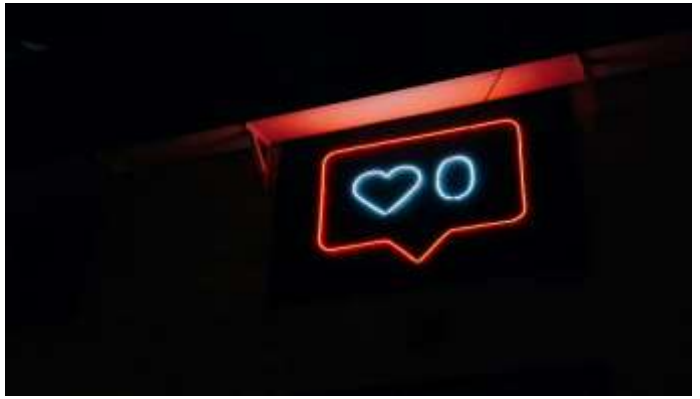




Торговля в соцсетях

Суть: в соцсети (чаще в Instagram) создаётся страница магазина, например, одежды или техники. Профиль наполняется фотографиями, украденными из настоящих онлайн-каталогов, а *товары предлагаются по цене в несколько раз ниже рынка или с огромными скидками.* Причём их действие ограничивается для дополнительной стимуляции пользователей на покупку.

Для правдоподобности накручиваются подписчики и публикуются фейковые отзывы. Далее всё по классике: *покупатель оплачивает товар и либо не получает его вовсе, либо ему приходит, как говорится, жалкое подобие вместо неповторимого оригинала.* Любые последующие попытки связаться с продавцом заканчиваются неуспешно.



Как понять настоящий аккаунт или нет?

1. Проверьте профиль на подлинность.

А) **Верификация.** Официальные страницы брендов отмечаются синими галочками.

Б) **Лента.** В настоящем профиле публикации выходят более или менее регулярно и последние посты «свежие».

В) **Имя.** Как и в случае с фишинговыми ссылками, фейки обычно слегка видоизменяют узнаваемый логин или название бренда.

2. Проверьте профиль на накрутки.

А) **Подписки и подписчики**. Насторожитесь, если подписок значительно больше, чем подписчиков. Выборочно пролистайте несколько подписчиков, чтобы проверить: «живые» это страницы или боты;

Б) **Лайки**. В «живых» аккаунтах количество лайков составляет примерно 10% от количества подписчиков. Если на нескольких последних постах лайков в разы больше, чем на предыдущих, то, скорее всего, они «накручены»;

В) **Комментарии**. При большом количестве подписчиков отсутствие комментариев выглядит странно. Если они есть, обратите внимание на содержание и на то, кто их оставляет. О накрутке скажет большое число односложных наподобие "Супер!" или "Отличное фото" от сомнительных пользователей.

Схема «Платные соцвыплаты»

Мошенники запускают рекламу в социальных сетях о, якобы, вступлении в силу закона о единовременной выплате денежных средств от государства.

Реклама кликабельна и перенаправляет граждан на поддельный сайт, на котором предлагается пройти опрос, внести свои персональные данные и данные карточки. Скомпрометированные данные используются мошенниками для хищения денежных средств.

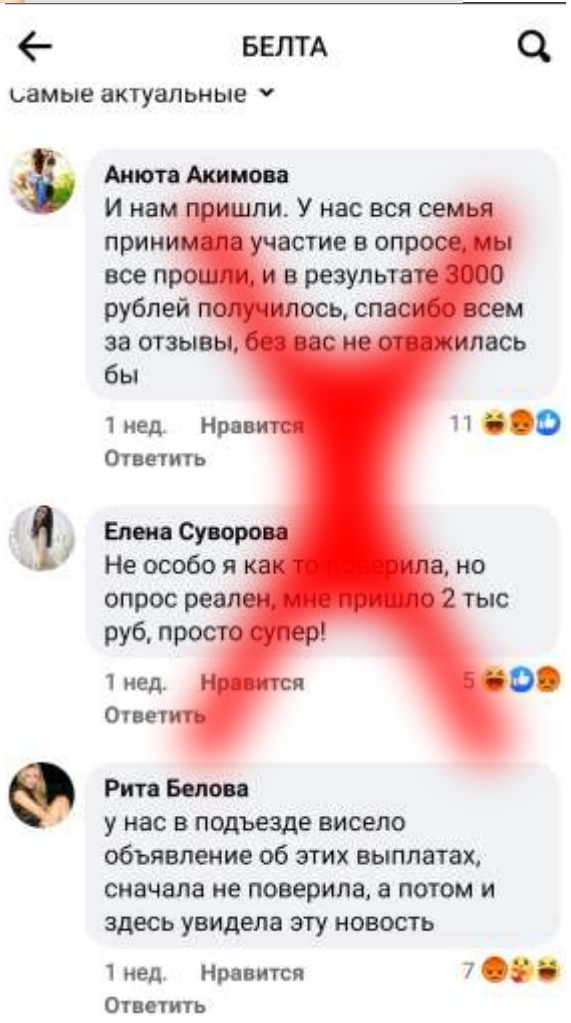
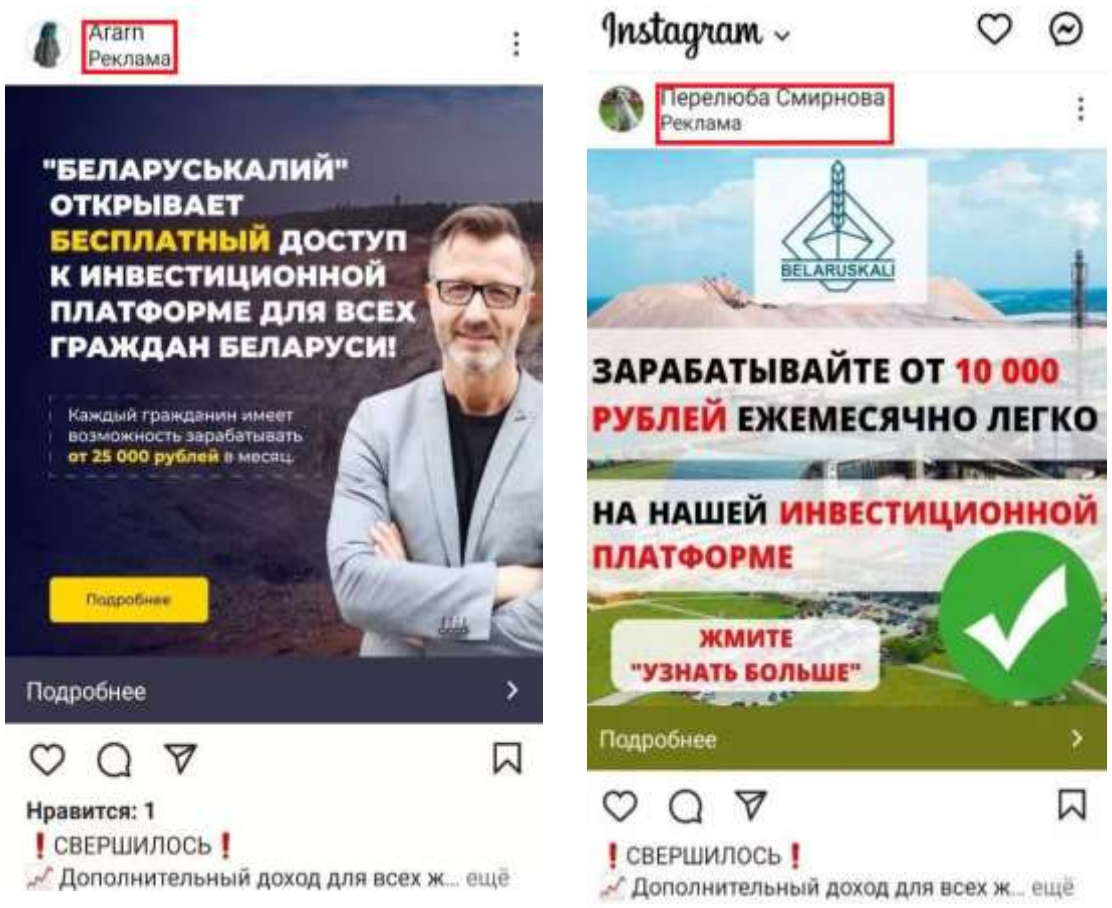


Схема: «Инвестиции»



Суть:

В последнее время в социальных сетях (чаще, Instagram) стали появляться сообщения рекламного характера о якобы «легком» заработке путем инвестирования денежных средств в акции известных компаний (Беларуськалий, Газпром и т.д.)

Мошенники, выдавая себя за инвестиционных брокеров, во время переписки (разговора) в мессенджере убеждают жертву перевести денежные средства в счет покупки акций. Сначала, как правило, речь идет о небольших суммах, например, 100$. Часто, одновременно с этим, мошенники просят жертву установить на свой смартфон *программы по удаленному управлению* (Anydesk, Rustdesk и пр.).

Лжеброкеры удаленно демонстрируют жертве как, якобы, «растут» ее доходы даже от такой незначительной суммы (например, 100$ виртуально прирастают в месяц на 30%, т.е. на фейковом счету жертвы уже не 100$, а 130$).

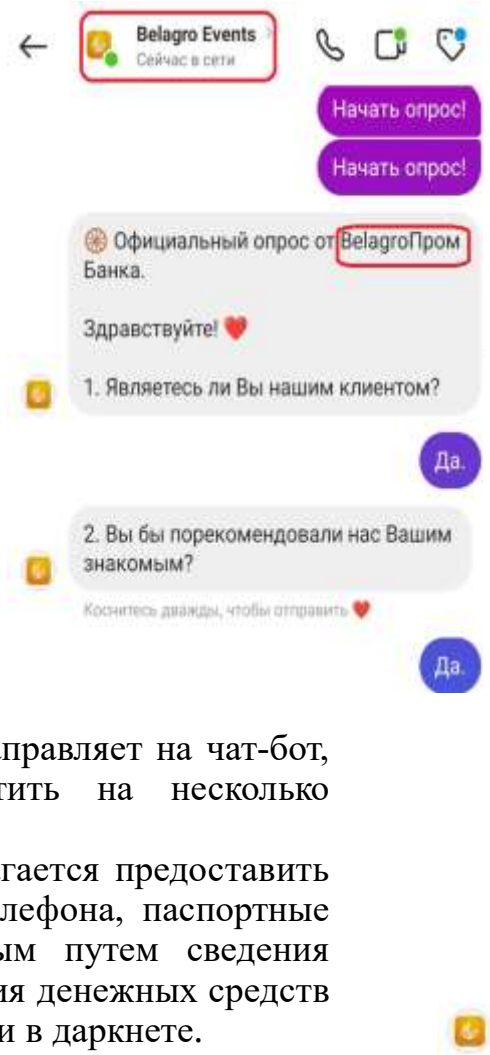
Далее жертва (будучи уверенной, что «схема рабочая») перечисляет мошенникам более значительные суммы. Лжеброкер уверяет: чем больше вложение, тем больше доход! Иногда мошенники наводят жертву на мысль о необходимости взять кредит.

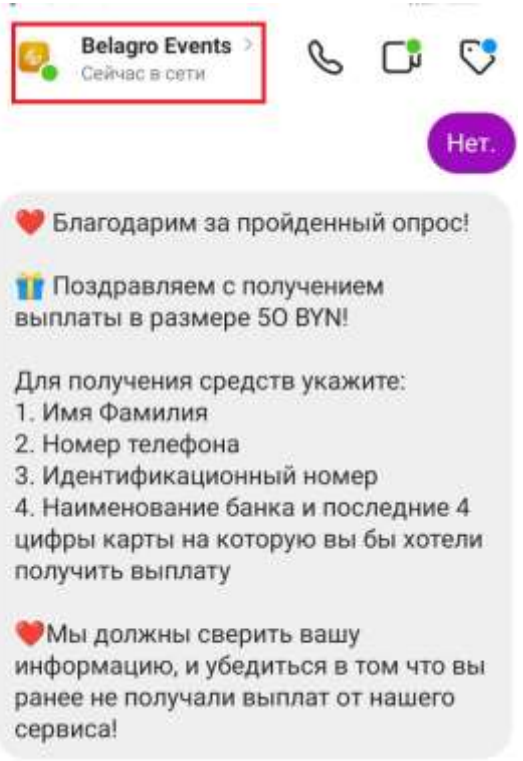
Как только мошенники начинают понимать, что жертва не может далее «вкладываться в акции» или жертва начала требовать перечислить дивиденды на ее счет, мошенники перестают выходить на связь. Незадачливый инвестор остается и без вложенных им денег в акции, без самих акций и без дивидендов.

Схема «Опрос»

Суть: в Instagram и Facebook нелегитимно распространялась реклама, якобы от имени банка, о проведении опроса. За прохождение опроса предполагается денежное вознаграждение респонденту.

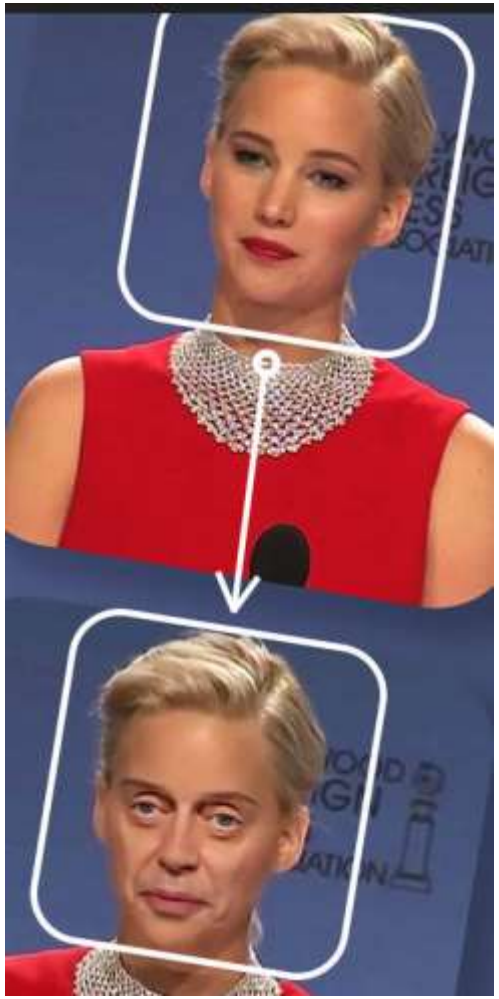
Вариант 1.
Кликабельная ссылка с рекламы перенаправляет на чат-бот в мессенджере (чаще в Telegram), где речь идет уже не о прохождении опроса, а о выгодах брокерских сделок на бирже и инвестировании в криптовалюты (см. схема «Инвестиции»)





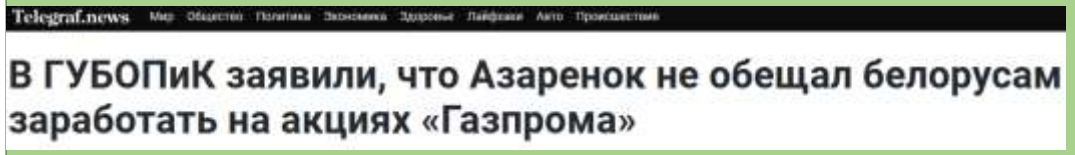
Вариант 2.
Кликабельная ссылка с рекламы перенаправляет на чат-бот, где респонденту предлагается ответить на несколько простых, даже примитивных, вопросов.
Затем для получения выигрыша предлагается предоставить персональные данные (ФИО, номер телефона, паспортные данные и т.д.). Полученные обманным путем сведения используются мошенниками для хищения денежных средств со счетов граждан, шантажа или продажи в даркнете.

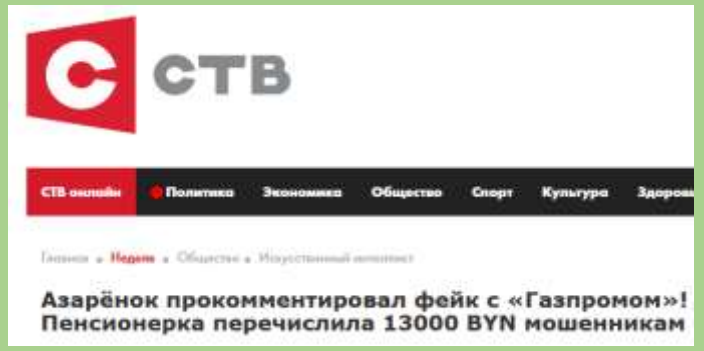
Что такое «дипфейк»?



Дипфейки – это фото, видео или аудиозапись, обработанные с помощью искусственного интеллекта. Данная технология позволяет оживить несуществующих людей, подделать любой голос, мимику, добавить в речь слова, которые человек никогда не произносил.

В Беларуси мошенники часто дипфейк-технологию используют в схеме «Инвестиции» (рекламные ролики лжеброкеров, распространяемые в соцсетях).





Как не попасться на фейк?

* Мошенники редко уделяют должное внимание качеству своего «продукта», будь то видео, фото или аудио. Поэтому странное моргание человека, либо его отсутствие, слова невпопад, легкое заикание или роботизированный тон должны вас насторожить.
* Проверяйте информацию у официального источника: предлагают инвестировать в Газпром? Зайдите на официальный сайт ПАО «Газпром» и направьте обращение на электронный адрес компании.

Внимание! Не используйте те, якобы, официальные контактные данные компании, которые представлены в подозрительной (фейковой) рекламе.

* Используйте критическое мышление. Гарантированный доход обещают только мошенники. Подобным «рекламам», даже без использования дипфейков, где просто используются изображения известных и уважаемых людей, не нужно доверять.

Схема «ДТП*»

Потенциальной жертве звонят с незнакомого номера, представляются сотрудником правоохранительных органов. «Сотрудник» уверенно и спокойно называет вымышленное Ф.И.О., должность, номер телефона, чем располагает к себе. Далее он сообщает о том, что родственник жертвы является виновником ДТП (нередко жертва сама случайно подсказывает имя того, о ком она волнуется).

Для подтверждения истории к разговору присоединяется псевдородственник и просит деньги, чтобы избежать уголовной ответственности и оказать материальную помощь пострадавшим в ДТП. Для убедительности псевдородственник разговаривает плачущим голосом, что создает трудность в опознании близкого человека.

После беседы, спустя некоторое время, приезжает курьер и забирает деньги.

Мошенники действуют с использованием психологических приемов:

не дают времени потерпевшим для возможности проанализировать ситуацию и позвонить своим родственникам, разговором вводят жертв в стрессовое состояние;

стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег. МВД сообщает о случае, когда мошенник был на связи с потерпевшим порядка двух часов.

У мошенников есть еще одна уловка. Зарегистрированы случаи, когда мошенники звонили **несовершеннолетним** и сообщали, что их родители попали в ДТП, просили срочно найти и передать курьеру все имеющиеся в квартире деньги.

КАК ПОСТУПИТЬ В ТАКОЙ СИТУАЦИИ:

- **Ни в коем случае не поддавайтесь панике и под любым предлогом прекратите разговор с незнакомым.**
- **Перезвонить родственнику, о котором шла речь. Если телефон отключён, постарайтесь связаться с его коллегами и друзьями для уточнения информации.**
- **Не следует передавать (перечислять) деньги незнакомым людям.**

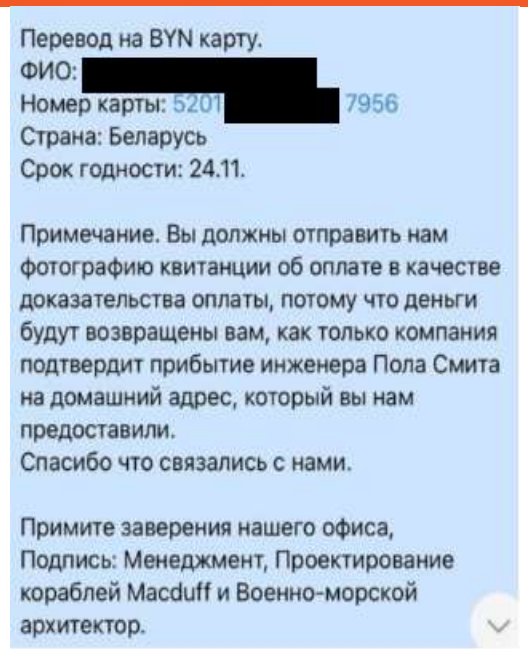
*Дорожно-транспортное происшествие.

Схема: «Капитан дальнего плавания»


[redacted]
5 марта в 09:12

Уважаемая [redacted]
мы получили ваш адрес приглашения нашего клиента, инженера Пола Смита, который приедет провести отпуск с вами в Беларуси. Это процедуры, принятые для утверждения отпуска наших клиентов. Мы взимаем с наших клиентов плату за отпуск в зависимости от месяцев, которые он / она собирается провести но месяцы не должны быть продлены более чем на (3) месяца. Это следующие: мы берем месяц (6200 долларов), два месяца (9400 долларов) и 3 месяца (11100 долларов). Примечание: «Деньги получены в результате дорожные расходы нашего клиента, и это необходимо для того, чтобы убедиться, что человек, которого он / она едет, чтобы встретиться, является финансово жизнеспособным, чтобы заботиться о нашем клиенте, поскольку его / ее жизнь очень важна для нас. В разделе (109) вы должны произвести платеж до утверждения отпуск будет предоставлен вашему инженеру-жениху Полу Смиту. Чем раньше вы сделаете платеж, тем лучше, потому что у нас есть лимит нашего клиента, разрешенного ежегодно для отпуска, когда вы встречаетесь с командировочными расходами. Вы должны отправить деньги нашему казначею. в головном офисе нашей компании Филиал: Через этот Бела rus Рублевая карта: Вот адрес.

Перевод на BYN карту.
ФИО: [redacted]
Номер карты: 5201 [redacted] 7956


Перевод на BYN карту.
ФИО: [redacted]
Номер карты: 5201 [redacted] 7956
Страна: Беларусь
Срок годности: 24.11.

Примечание. Вы должны отправить нам фотографию квитанции об оплате в качестве доказательства оплаты, потому что деньги будут возвращены вам, как только компания подтвердит прибытие инженера Пола Смита на домашний адрес, который вы нам предоставили.
Спасибо что связались с нами.

Примите заверения нашего офиса,
Подпись: Менеджмент, Проектирование кораблей Macduff и Военно-морской архитектор.

Как правило, мошенник сразу вычисляет тех, кто потенциально «попадет на удочку», а точнее, на сообщение.

Вариант 1 (наиболее распространенный): ценная посылка от «хорошего иностранного знакомого» задержана на границе.

С получательницей («жертвой») связывается третье лицо с предложением выкупить почтовое отправление на ее имя, которое задержано на границе «в связи с наличием в нем крупной суммы наличной валюты».

Вариант 2: Иностранный знакомый едет в Беларусь, но по пути попадает в беду (например, в аварию).

Вариант 3: Иностранный знакомый планирует поездку в Беларусь, но сталкивается с неожиданными трудностями (невозможностью оформить приглашение, купить авиабилеты, забронировать отель), в связи с чем просит «жертву» оплатить «небольшой счет», например, пошлину за подачу приглашения.

Во всех трёх вариантах «жертву» просят перечислить деньги на определенный счет или карточку.

Рекомендуем быть осторожными, если новый знакомый:

- практически в самом начале переписки ненавязчиво выясняет ваше материальное положение;
- рассказывает жалостливые истории жизни (больной ребенок, попал в больницу, вынужден искать политическое убежище и др.);
- отказывается присылать фотографии из обычной, повседневной жизни;
- просит перевести определенную сумму денег для решения каких-либо его проблем.

Что и как можно проверить?

- попросите у нового знакомого ссылку на профиль в соцсети, изучив его страницу можно сделать соответствующие выводы;
- предложите общение через скайп или любой другой видеомессенджер – вы сразу же увидите соответствует ли действительности размещенные в анкете (в соцсети, на сайте знакомств) фотографии;
- пропустите фотографию знакомого через поисковую систему Интернета.

Кто такой «дроппер»?

Дроппер («дроп», «мул») - физическое лицо, которое помогает мошенникам обналичивать украденные денежные средства через свои банковские счета, карточки. Зачастую также используется в качестве звена в цепочке вывода денежных средств за пределы страны.

Кого могут рассматривать мошенники в качестве потенциального дроппера?
Основная группа риска – граждане, у которых шаткое материальное положение:

- безработные, малоимущие, студенты, учащиеся;
- переехавшие в большой город из маленького населенного пункта;
- представители экономически и социально уязвимых групп населения: многодетные семьи, сироты и т.д.
- лица с низкой социальной ответственностью.

Как оплачивается «труд» дроппера?

- определенный незначительный процент от части обналиченных либо переводимых средств;
- единоразовая выплата денег либо иная форма поощрения.

Зачастую мошенники направляют предложения о «работе» посредством сообщений в социальных сетях, мессенджерах.
Необходимо настороженно относиться к предложениям о работе, в которых:

- суть работы заключается в переводе денег с карточки на карточку / электронный кошелек;
- работодатель требует передать ему вашу банковскую платежную карточку или ее реквизиты;
- работа предполагает только онлайн взаимодействие с работодателем (без личного общения).

При согласии на такую работу человек становится **соучастником преступления**.
Ответственность: от штрафа до лишения свободы, а также несут обязанность по возмещению материального ущерба, причиненного потерпевшим.

Спасибо за внимание!

белагропромбанк