SCS SBER CYBER SECURITY

Не дайте себя обмануть!

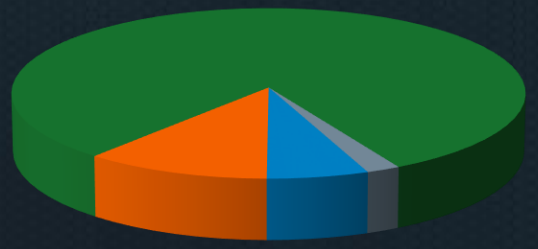
УРОК КИБЕРГРАМОТНОСТИ

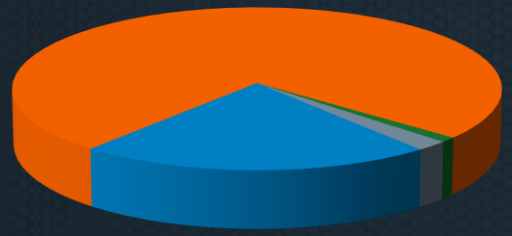
SCS SBER CYBER SECURITY

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Социальная инженерия - угроза №1

	2012	2017	2020
Социальная инженерия	11%	75%	91%
Фишинг	2%	2%	8%
Вирусы	6%	22%	1%
Скимминг	81%	1%	





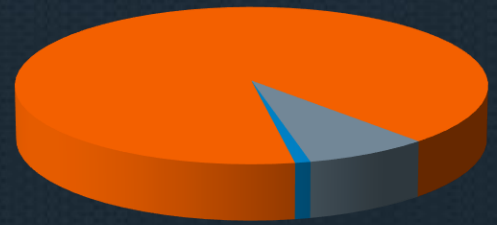


СХЕМА: Использование ПО удаленного управления

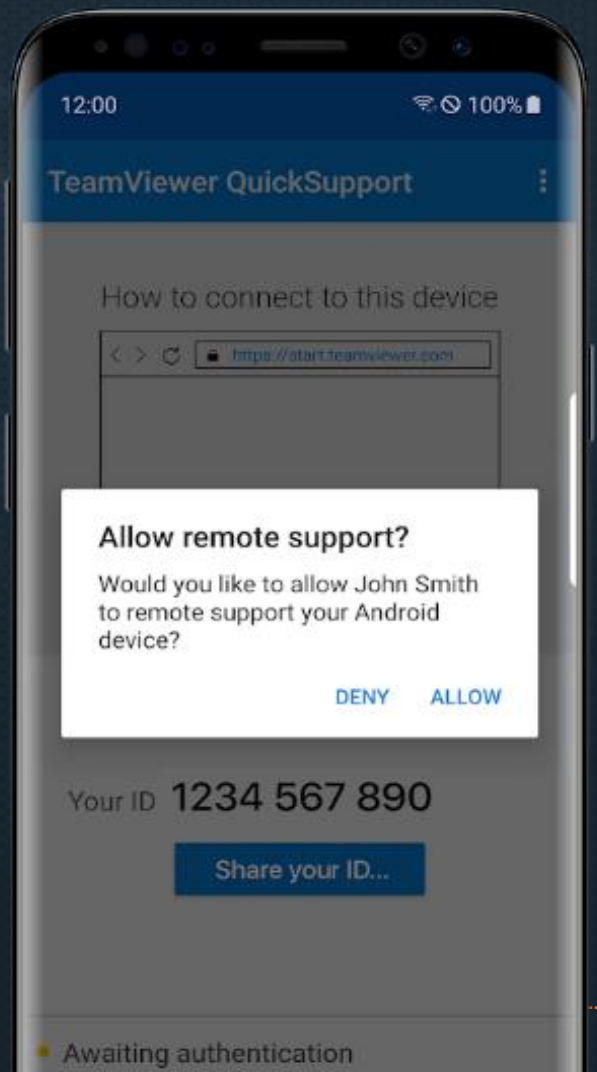
1. Звонок от сотрудника «Службы безопасности» Сбербанка и сообщение о попытке совершения операции по его карте.

2. Вас убеждают установить на мобильное устройство приложение удаленного управления Quick Support и разрешить подключение к устройству «сотруднику банка». Чаще всего предлогом для установки бывает удаление вирусов с устройства клиента, помощь в спасении средств .

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

4. В это время злоумышленники проводят списания через мобильное приложение.

5. Если мобильное приложение не позволяет проводить удаленное управление через Quick Support, а только транслировать экран, злоумышленники убеждают вас перевести средства на «безопасный счет».



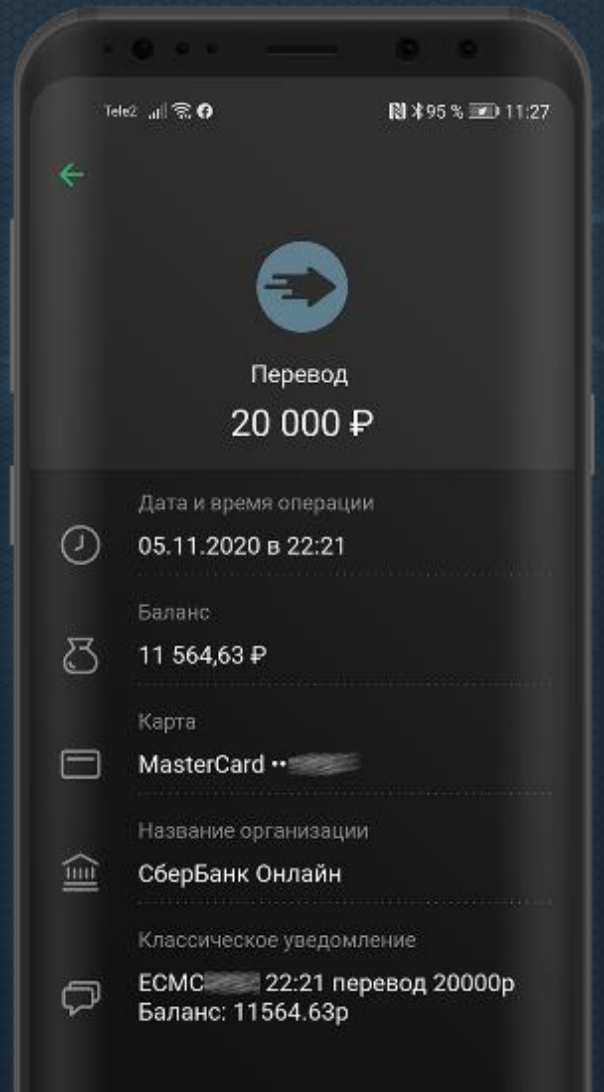


СХЕМА: Перевод на «безопасный счет»

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

- Ваши средства находятся в опасности. Для исключения возможности финансовых потерь необходимо перевести сбережения на «защищенную ячейку»/ «безопасный счет», открытую на ваше имя («сотрудника банка»).

Данной ячейкой может являться счет физического лица, счет юридического лица, индивидуального предпринимателя, карты Сбербанка и других банков.

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

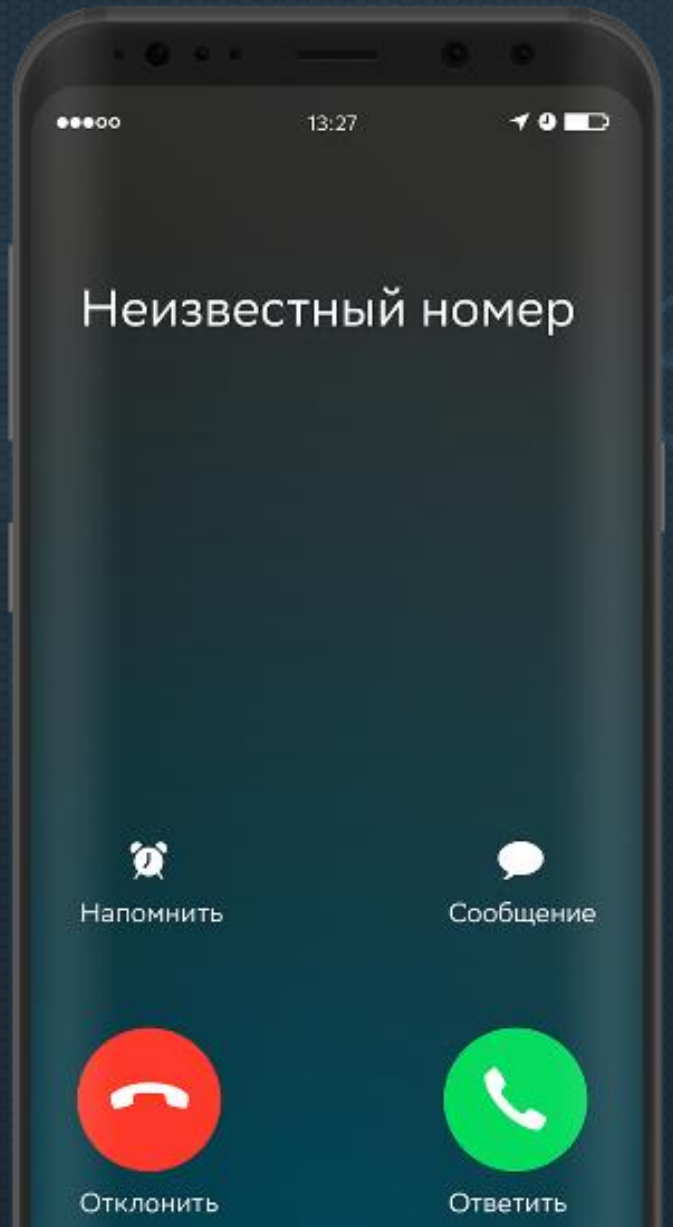


СХЕМА: Токенизация карты

1. Звонок клиенту под видом работника банка либо под видом покупателя по ранее размещенным объявлениям в сети Интернет.

2. Используя методы социальной инженерии, мошенник вводит клиента в заблуждение для получения реквизитов банковских карт и одноразовых паролей из SMS-сообщений.

3. На своем мобильном устройстве мошенник осуществляет регистрацию в приложении Wallet (Кошелек), либо осуществляет регистрацию нового мобильного приложения СБОЛ.

4. Получив доступ в СБОЛ, мошенник переводит денежные средства со счетов клиента на карту и далее совершают покупки и снятие наличных по токенизированной карте клиента с использованием своего мобильного устройства.

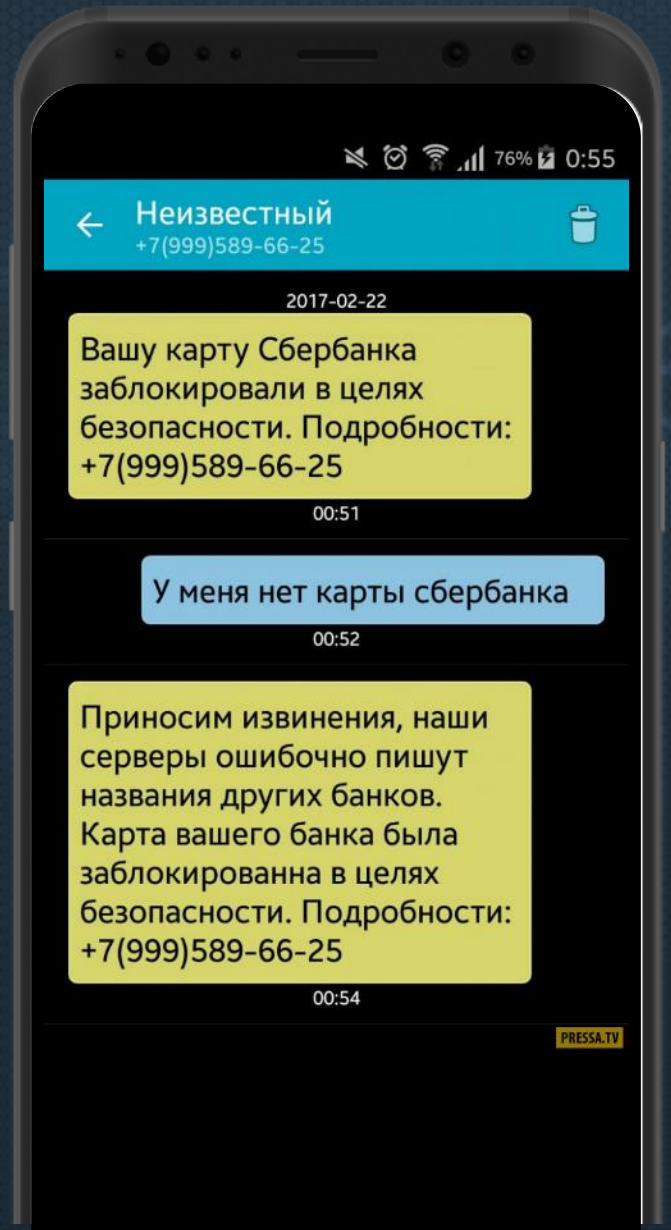
Разнообразие тем телефонного мошенничества

1. Звонок из Генпрокуратуры – Примите участие в расследовании

2. Звонок из Службы безопасности –
   - Помогите поймать нечестного сотрудника…
   - Продиктуйте код для отмены мошеннической операции…
   - На Вас оформили кредит…
   - С Вашего счета хотят перевести деньги в другом городе…

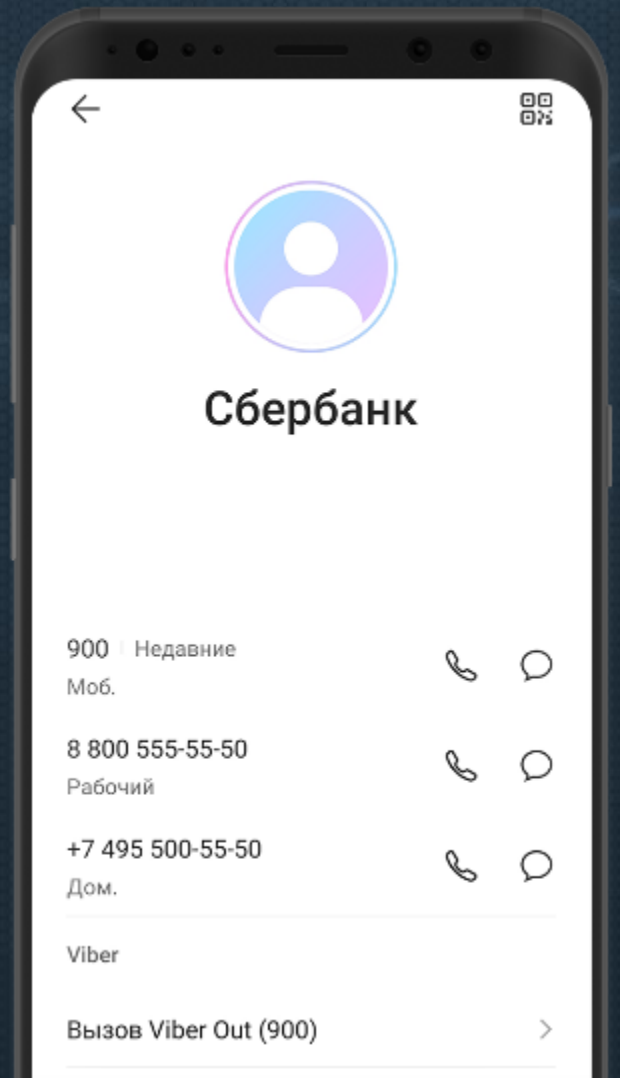
3. Звонок робота – карта заблокирована, перезвоните, пожалуйста по номеру

4. Голосовой помощник – сообщите смс-код



Как защитить себя: Телефонное мошенничество

1. Внимательно проверяйте входящий номер
2. Сохраните номера Сбербанка в адресной книге. Если звонок будет с другого номера, он отобразится как неизвестный
3. Не совершайте никаких операций по инструкциям звонящего
4. Сразу заканчивайте разговор. Работник банка никогда не попросит у вас CVV/CVC-код, логин, пароль от СберБанк Онлайн или коды из СМС
5. Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся



Слышите такое в телефоне? Бросайте смело трубку

SCS SBER CYBER SECURITY

Продиктуйте код из СМС

Так вы даете доступ к своему счету – и пока-пока, деньги!

Загрузите безопасное приложение

Это «безопасное приложение – пропуск для мошенников к вашему счету

В другом городе был совершен подозрительный перевод

Так вовлекают в «расследование», после которого со счета снимают все деньги

На вас оформили кредит

Для его «отмены» узнают ваши данные и оформят уже настоящий кредит ☺

Помогите поймать сотрудника

Ловушка для сторонников правосудия. Никого не поймают, а ваши деньги спишут

Отправьте деньги на защищенный счет

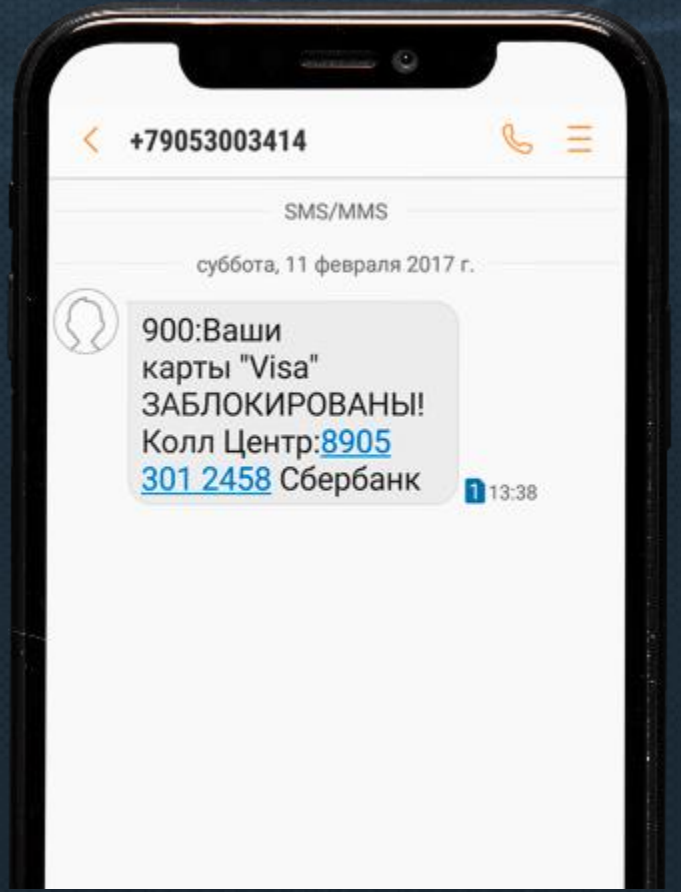
Все ваши средства будут под «защитой» мошенников!

SMS-МОШЕННИЧЕСТВО
СХЕМА: Срочно следуйте инструкциям…

1. Веерная SMS-рассылка по номерам телефонов. Наиболее распространены варианты сообщений — о блокировке карты или о совершении операции по карте. В сообщении указан телефон, по которому клиента просят перезвонить.

2. Представляются:
   - сотрудниками «Службы безопасности» СберБанка;
   - специалистами службы технической поддержки;
   - менеджером контактного центра;
   - сотрудниками платежной системы и пр.

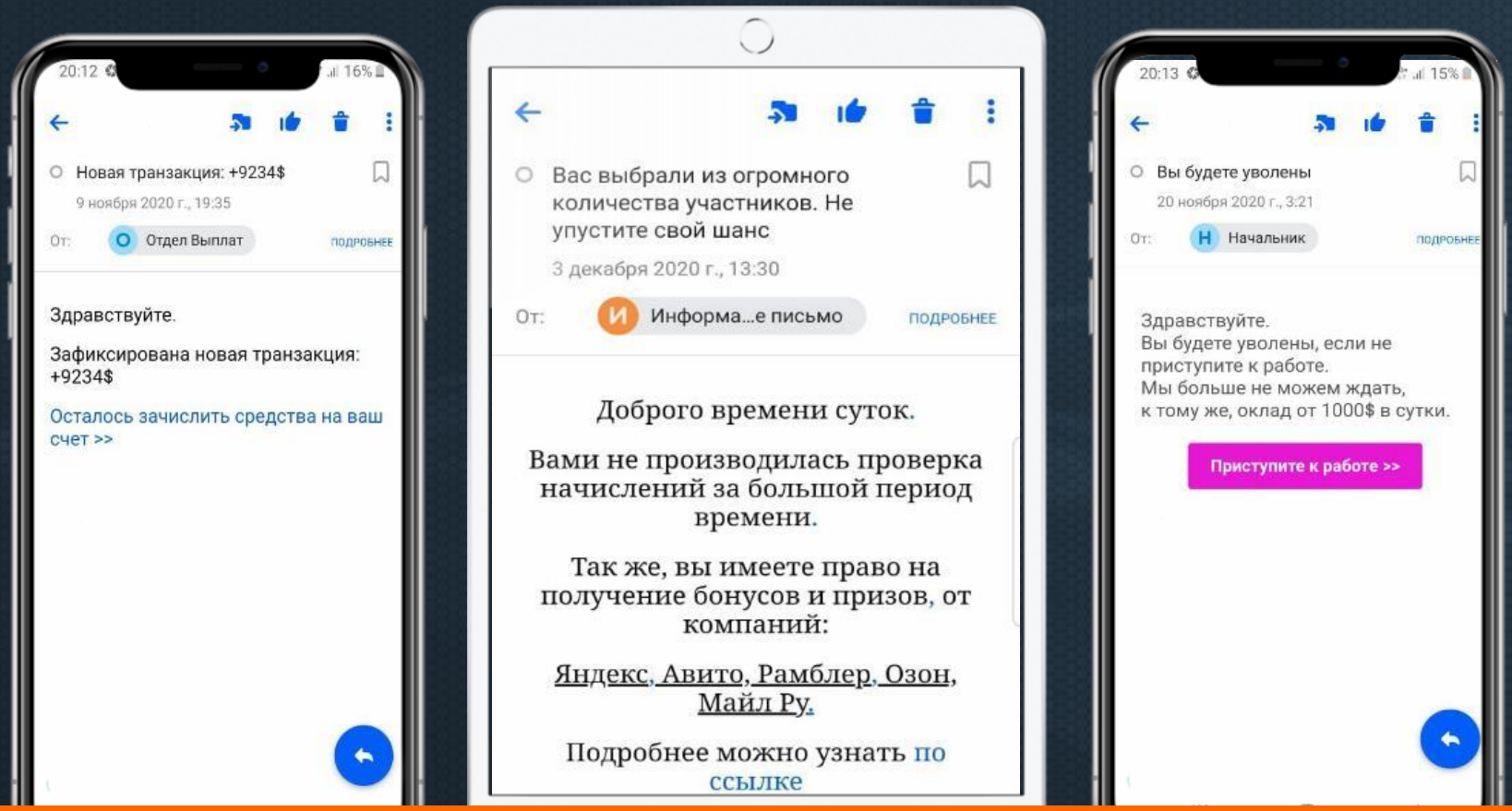
3. В убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п. Клиенты выполняют получаемые по телефону инструкции.



SCS SBER CYBER SECURITY

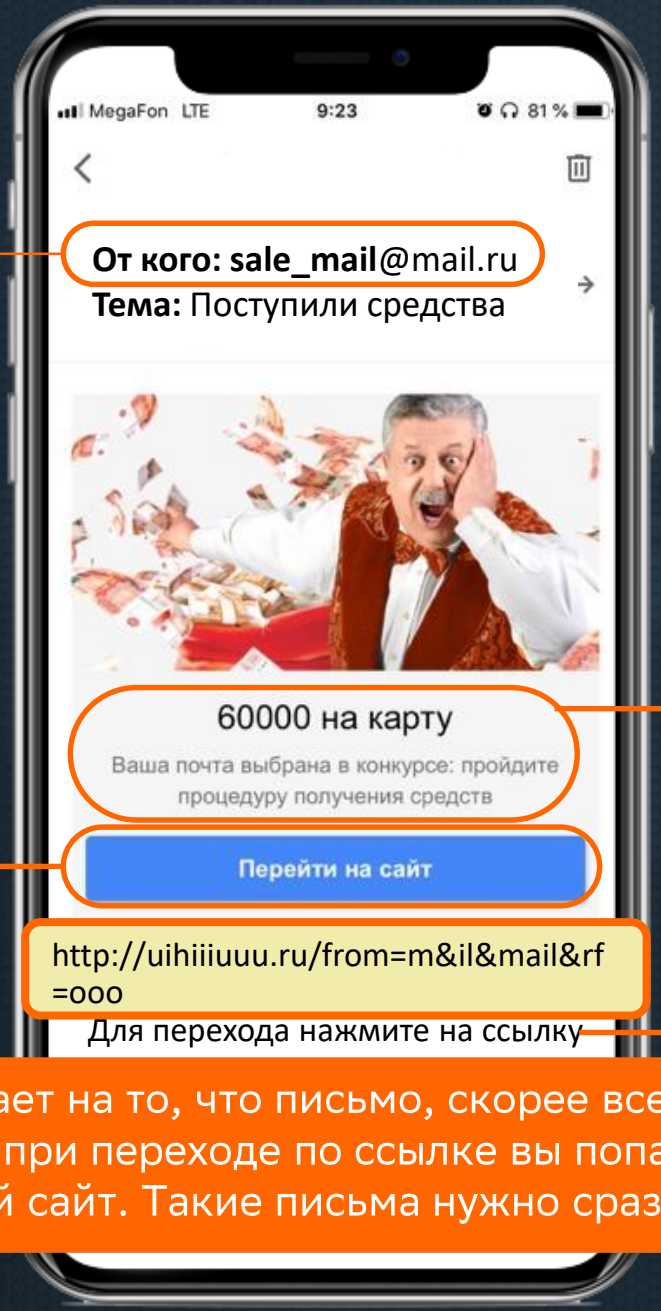
ФИШИНГОВЫЕ ПИСЬМА

Как понять, что письмо фишинговое?



Фишинг - вид интернет-мошенничества с использованием рассылок вредоносных электронных писем с целью получения доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.)

Фишинг: проверим себя



Общедоступный домен

Отсутствует персональное обращение, обещают приз в конкурсе, в котором вы не участвовали

Предлагают перейти по подозрительной ссылке

Отсутствуют подпись и контакты

Все это указывает на то, что письмо, скорее всего, фишинговое, и при переходе по ссылке вы попадете на мошеннический сайт. Такие письма нужно сразу удалять

СХЕМА: Официальное письмо

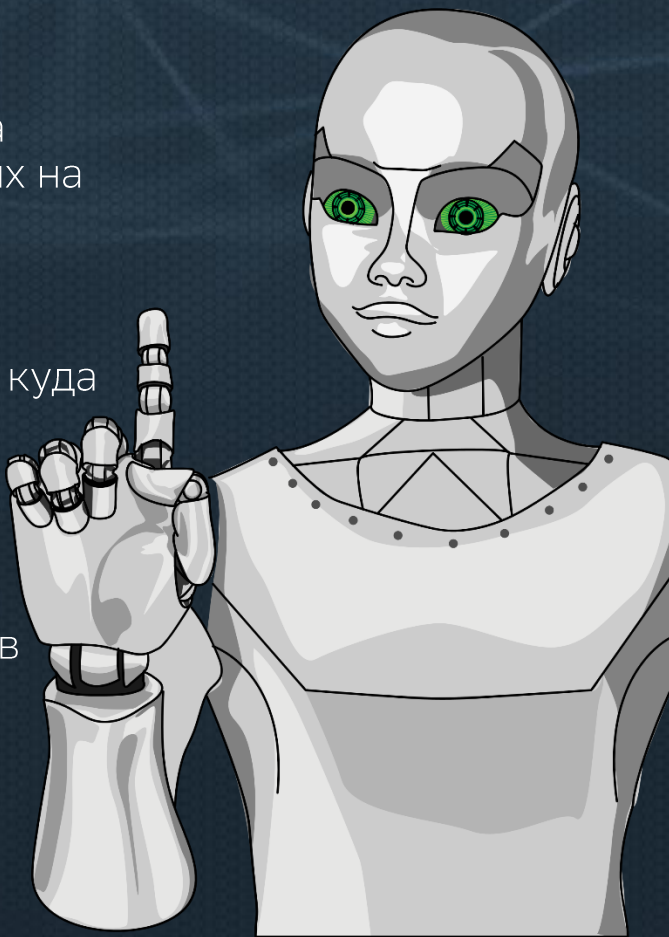
1. Фальшивый документ с поддельными подписью и печатью на бланке кредитной организации. Такое письмо могут отправить как по электронной почте, так и по обычной.
2. Письмо содержит персональное обращение с указанием имени, отчества и фамилии.
3. В тексте письма будет сказано, что вы стали жертвой мошеннических действий и для обеспечения безопасности нужно «выполнить процедуру обновления единого номера лицевого счёта».
4. Формулировки могут варьироваться, но суть неизменна: в письме будет указан номер счёта, на который нужно перевести деньги.

Необходимо помнить: перевести ваши деньги на другой счёт под предлогом их спасения предлагают только мошенники, СберБанк так никогда не поступает.

Как защитить себя: Фишинговые письма

SCS SBER CYBER SECURITY

1. Обращайте внимание на домен. Мошенники обычно используют общедоступные почтовые домены gmail.com, mail.ru и т.п., или покупают похожие на официальные имена компаний, чтобы ввести вас в заблуждение.
2. Вас должно насторожить, если тема, контент письма или название файлов побуждают вас к немедленному действию.
3. Обращайте внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга. Контакты могут быть недостоверные, проверьте их на официальном сайте компании.
4. Не переходите по ссылкам, не кликайте на подозрительные объекты. Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.
5. Будьте осторожны с вложениями, открывайте только те, которые ждали.
6. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы.
7. Не отвечайте на подозрительные письма.



МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

Что знает о вас интернет:

Интернет-магазины

- Предпочтения
- Платежная информация
- Физические параметры (размеры обуви и одежды)

Службы доставки

- Место жительства и работы
- Уровень дохода

Поисковые системы

- История запросов
- Действия на сайте
- Выбор товаров и услуг
- Идентификаторы устройств
- Файлы cookie
- Данные об учетных записях

Такси и каршеринг

- Время и маршруты поездок

Социальные сети

- Друзья и знакомые
- Политические и религиозные убеждения и активности
- Хобби

Билеты

- Данные о перелётах, поездках и попутчиках

Государственные услуги

- Паспорт и другие документы
- Состав семьи
- Состояние здоровья

Карты и навигаторы

- Местоположение и передвижения
- Любимые места
- Модели поведения

Любое наше действие в сети оставляет цифровой след

ЦИФРОВОЙ СЛЕД

РЕГИСТРАЦИЯ НА САЙТАХ

ЛАЙКИ В СОЦ.СЕТЯХ

ПОСТЫ И РЕПОСТЫ

КОММЕНТАРИИ К ПОСТАМ

ФОТО И ВИДЕО

ЦИФРОВОЙ ПОРТРЕТ

КНОПКИ В ИНТЕРНЕТЕ НЕТ

ИНФОРМАЦИЯ, ПОПАВШАЯ В СЕТЬ, ОСТАЕТСЯ ТАМ НАВСЕГДА!

СХЕМА: Компрометация реквизитов карты через фишинговый сайт

1. Злоумышленники создают в сети Интернет фишинговые сайты для сбора персональных данных.
2. Вы заходите на фишинговый сайт и вводите данные своей банковской карты.
3. Мошенник, получив данные карты клиента, совершает покупки в интернет-сервисах, не поддерживающих технологию оплаты с подтверждением одноразовым паролем.
4. Операции списания в основном выполняются с помощью бота.

Пример:

Проверь себя и свою семью на коронавирус

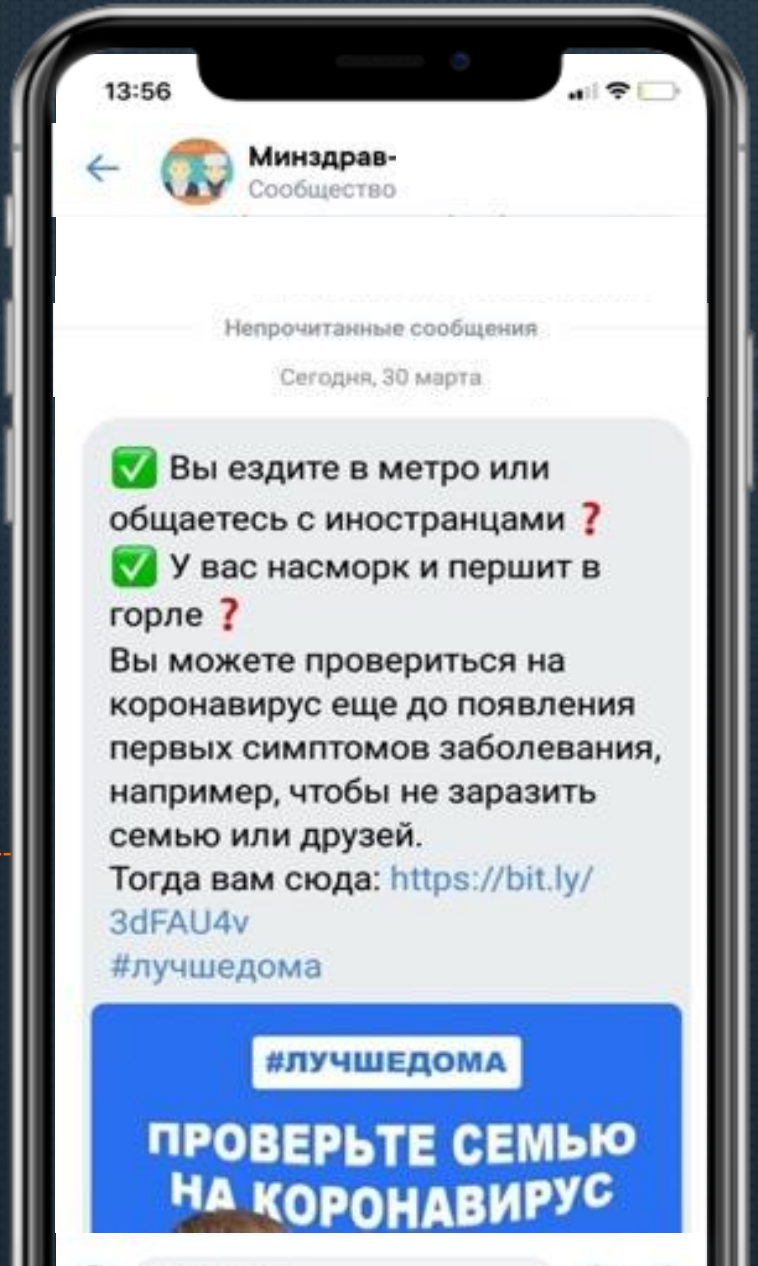


СХЕМА: Покупка в Интернет по выгодной цене с предоплатой

1. Мошенники размещают фиктивное объявление о продаже товара по очень выгодной цене

2. Клиент связывается с мошенником, который сообщает, что на данный товар несколько покупателей, и для того, чтобы забронировать товар, клиент должен внести предоплату.

3. Покупатель осуществляет перевод в пользу неизвестных

4. После внесения предоплаты продавец перестает отвечать на звонки и сообщения от покупателя.

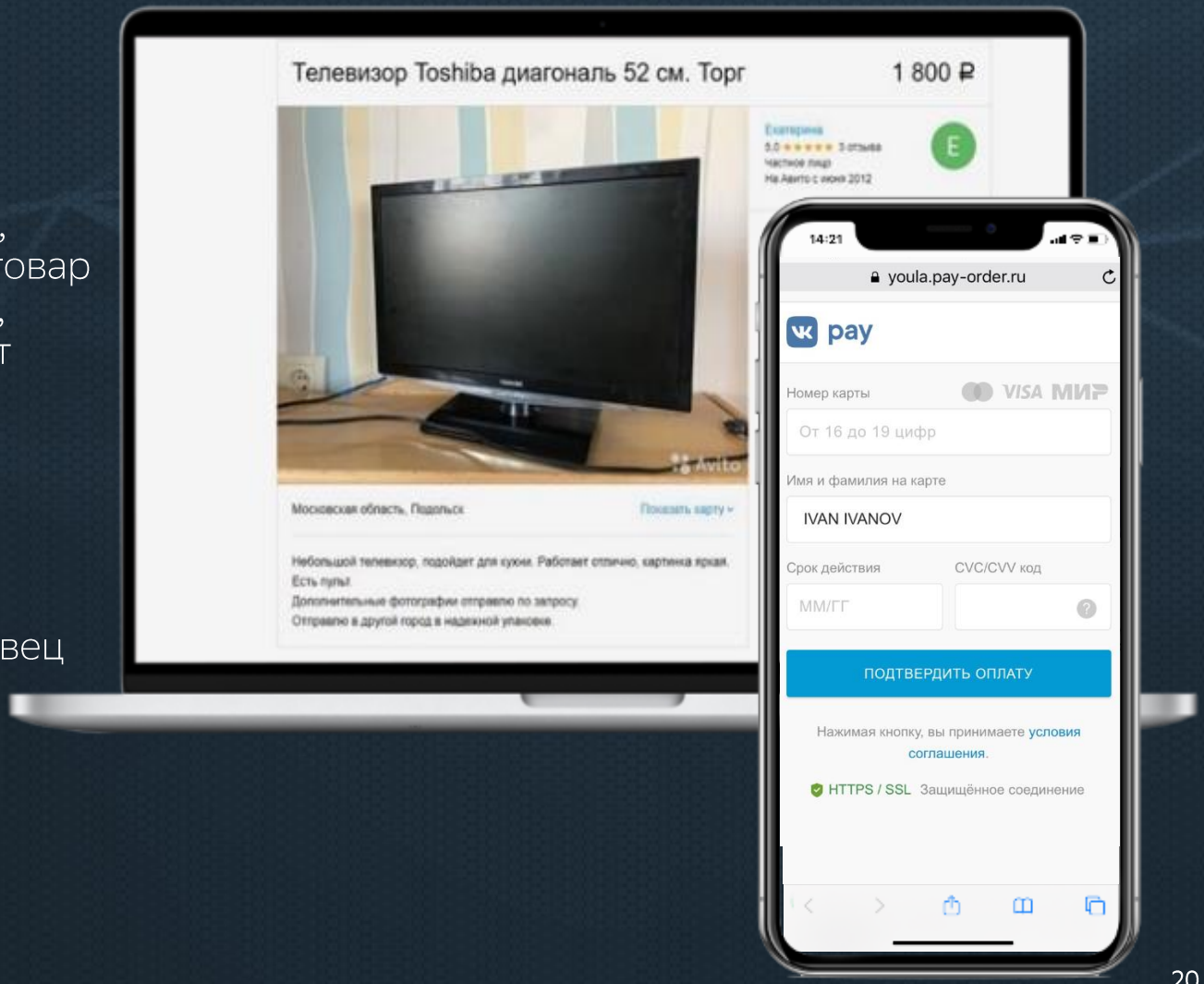


СХЕМА: Помощь в получении кредита

1. Объявление в интернете о помощи в получении кредита в Банке.
2. После вашего обращения через сайт связывается «сотрудник банка». В процессе общения с жертвой мошенники сообщают, что для успешного получения кредита ему необходимо оплатить:
   - комиссию ЦБ РФ, комиссию банка
   - налог
   - оплату за работу инкассаторов
   - страховой взнос
3. Для успешного прохождения заявки необходим оборот по счетам и сумма на вкладе. Надо выпустить карту (если ее нет), внести денежные средства на вклад. Вклад останется в Банке до одобрения кредита, а по карте будет сделан необходимый для одобрения кредита оборот.
4. Данные клиента для входа в СБОЛ и проведения операций для достижения необходимого оборота. Мошенники входят в СБОЛ по карте клиента и похищают денежные средства с вклада, которые клиент внес для одобрения заявки на кредит.

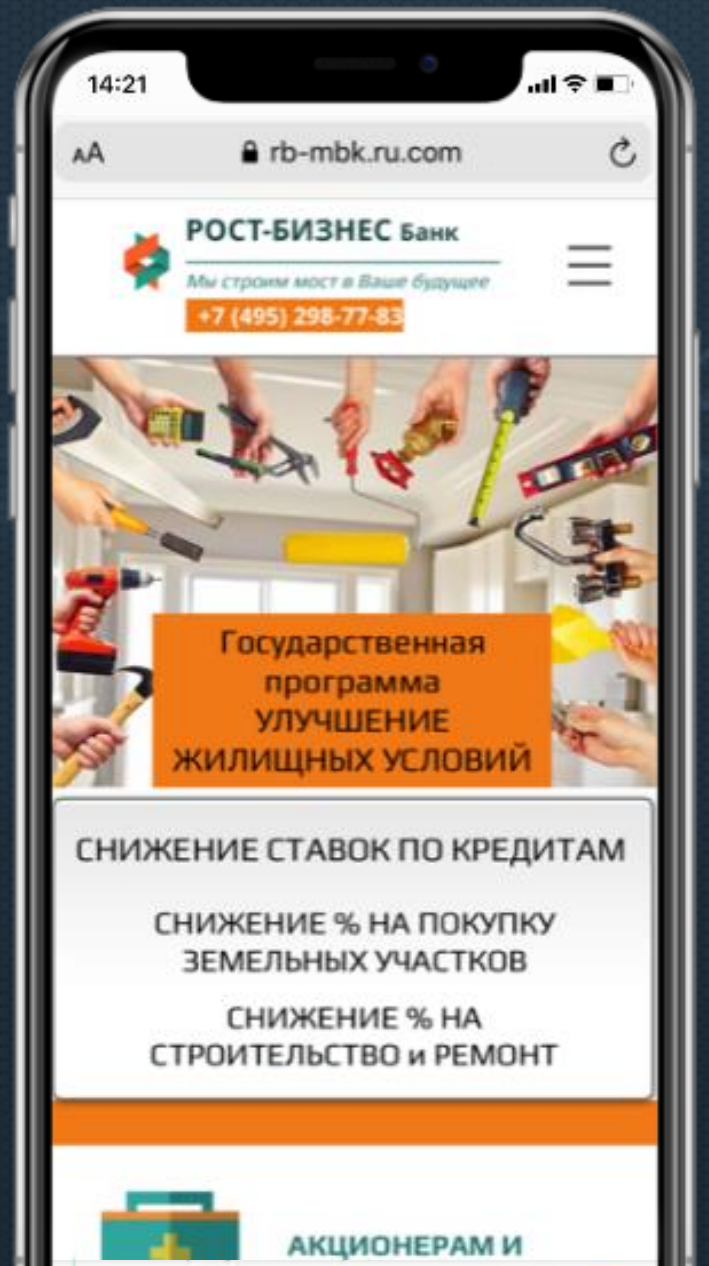


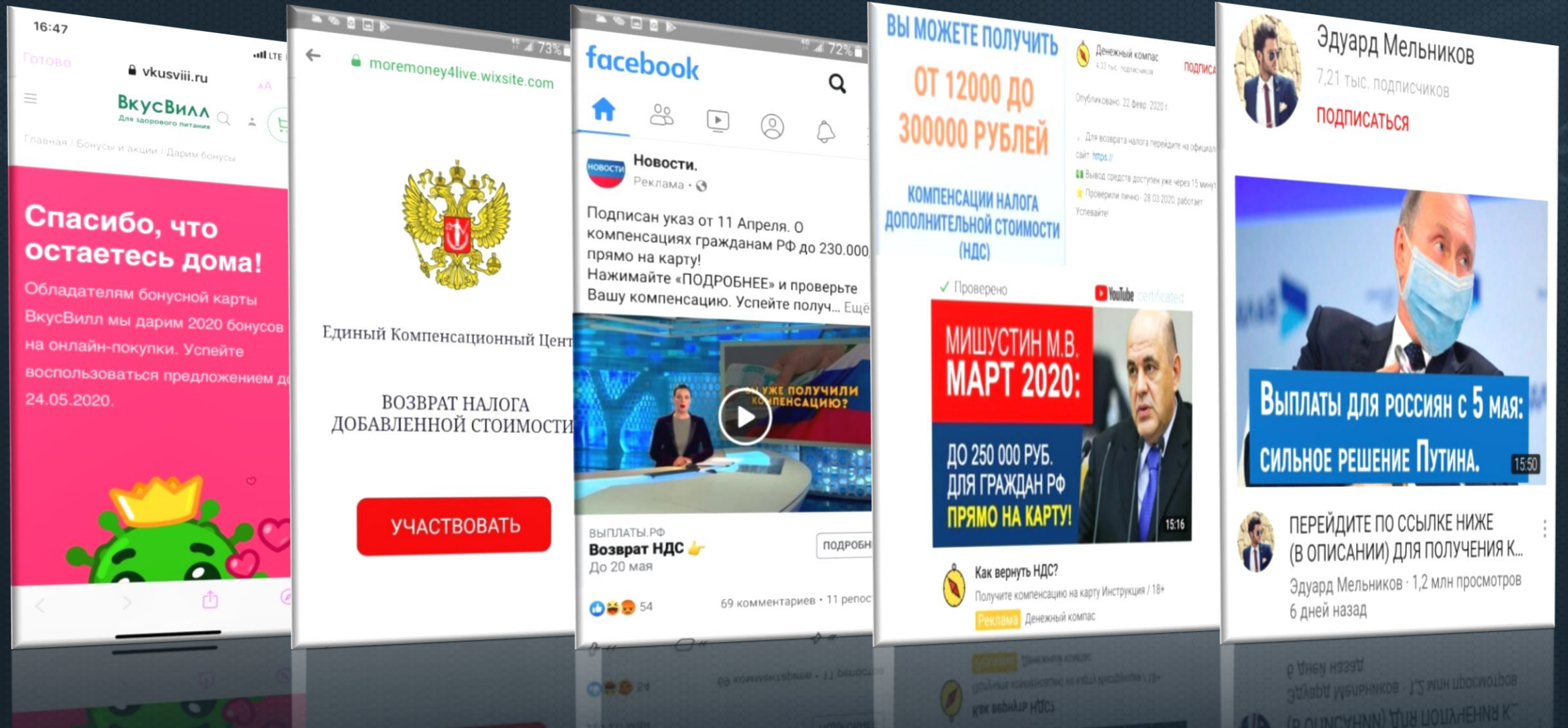
СХЕМА: Фиктивные опросы/выплаты/компенсации

1. Сайт с использованием символики официальных органов РФ, обещающий крупное вознаграждение или помощь в получении выплат/компенсаций.
 Под различными предлогами клиента убеждают провести оплату за услуги, связанные с оформлением вознаграждения/выплаты/компенсации.

2. На сайте необходимо пройти регистрацию, чтобы найти вас в системе. Далее сообщают о крупном выигрыше или возможности получения солидной компенсации.

3. Для получения денежных выплат клиент самостоятельно проводит оплату услуг специалистов, якобы помогающих в оформлении документов

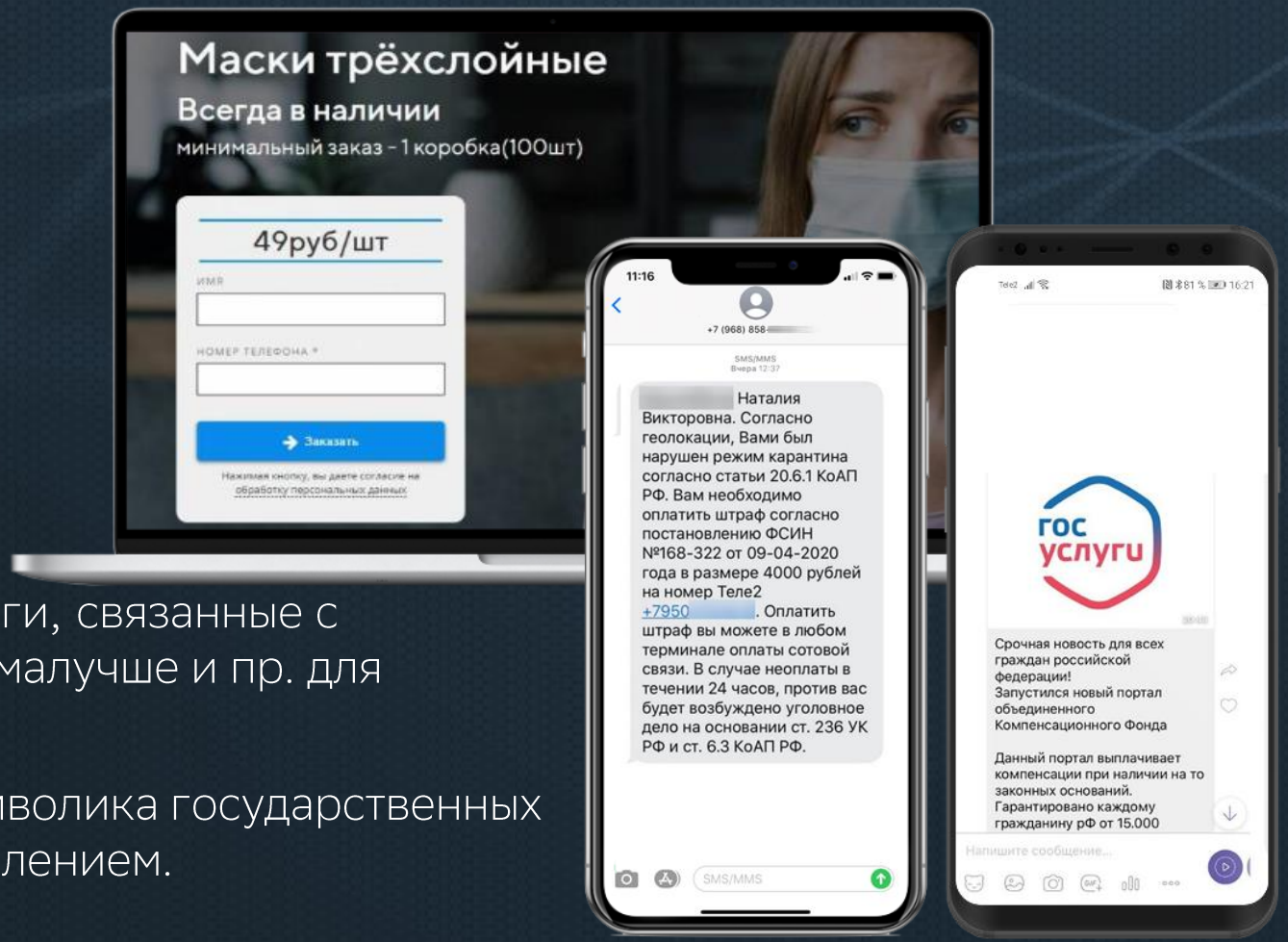
Мошенничество на фоне пандемии COVID-19



Мошенничество на фоне пандемии COVID-19

Мошенник размещает в сети Интернет объявления о продаже индивидуальных средств защиты (масок/перчаток), тестов на COVID, электронных пропусков, а также с предложением заработка/работы, получения компенсации.

- Лечение
- Лекарства
- Компенсации
- Заработок
- Помощь «безвозмездная»
- ВАКЦИНАЦИЯ!



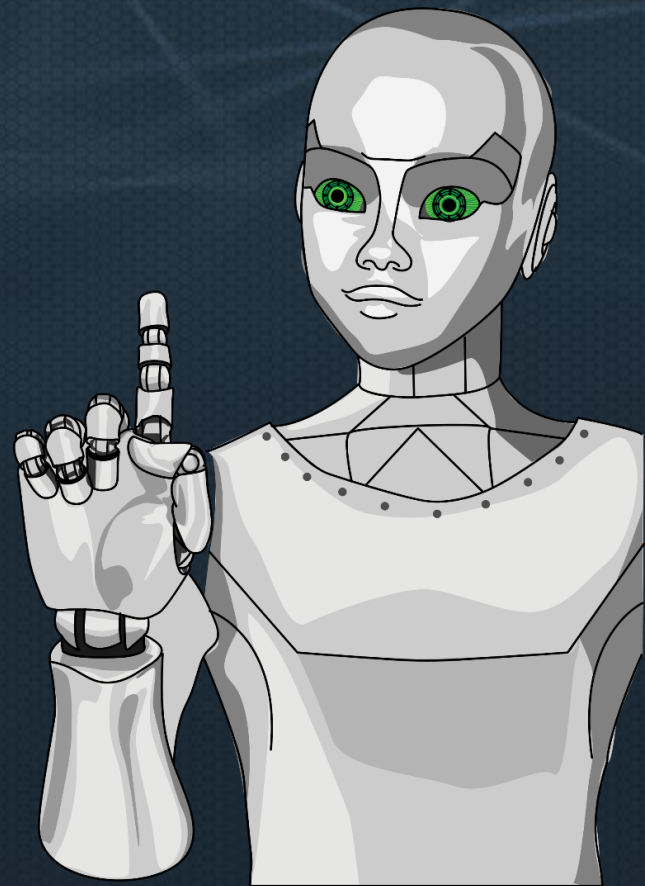
Используются популярные хештеги, связанные с самоизоляцией: #сидидома, #домалучше и пр. для привлечения пользователей.

Используются наименования/символика государственных организаций, работающих с населением.

Как защитить себя: Мошенничество в сети Интернет

SCS SBER CYBER SECURITY

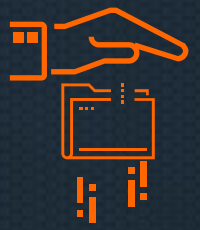
1. Не сообщайте номер своей банковской карты, срок действия, CVV-код и код из СМС
2. Как правило, со всеми акциями можно ознакомиться на их официальных сайтах и страницах в социальных сетях. Если вы не нашли предлагаемую активность на официальных ресурсах, откажитесь от участия
3. Если для получения большой суммы денег вам сначала предлагают потратить сравнительно небольшую, будьте осторожны, это мошенничество
4. Рекомендуется завести несколько адресов электронной почты, например: частный — для личной переписки публичный — для открытой деятельности в социальных сетях и т.д.
5. Отправляя кому-либо личную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает



SCS SBER CYBER SECURITY

МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ

Как «утекают» ваши персональные данные



При размещении данных на сайте вы фактически теряете контроль за их использованием и распространением

В пользовательских соглашениях есть пункты, которые гласят:

Instagram

«В случае перехода прав собственности или контроля над всеми или частью наших Продуктов или их активов к другому лицу мы можем передать вашу информацию новому владельцу.»

twitter

«Публично размещая контент посредством Твитов, вы, тем самым, указываете нам раскрывать эту информацию в объеме настолько широком, насколько это возможно.»

«Мы делимся вашими данными с нашими сторонними поставщиками услуг, которых мы используем, чтобы предоставлять вам доступ к Платформе. Мы также предоставляем вашу информацию нашим деловым партнерам, рекламодателям, операторам аналитических и поисковых систем.»

«Администрация Сайта считает, что Пользователь осознает, что информация на Сайте, размещаемая Пользователем о себе, может становиться доступной для других Пользователей Сайта и пользователей Интернета, может быть скопирована и распространена такими пользователями.»

СХЕМА: Знакомство (скаммеры!)

1. Под видом романтических отношений: знакомства через Интернет, социальные сети, службы подбора «невест по переписке», предлагают потратить средства на любимого человека:
2. Оплатить:
   - пересылку подарка,
   - налоги на таможне для доставки подарка,
   - переезд,
   - деньги в долг
3. После получения средств злоумышленники перестают отвечать на звонки и сообщения.

4. Чаще всего жених и невеста проживают в разных странах. Все схемы имеют одну цель — побудить человека к отправке денежных средств.

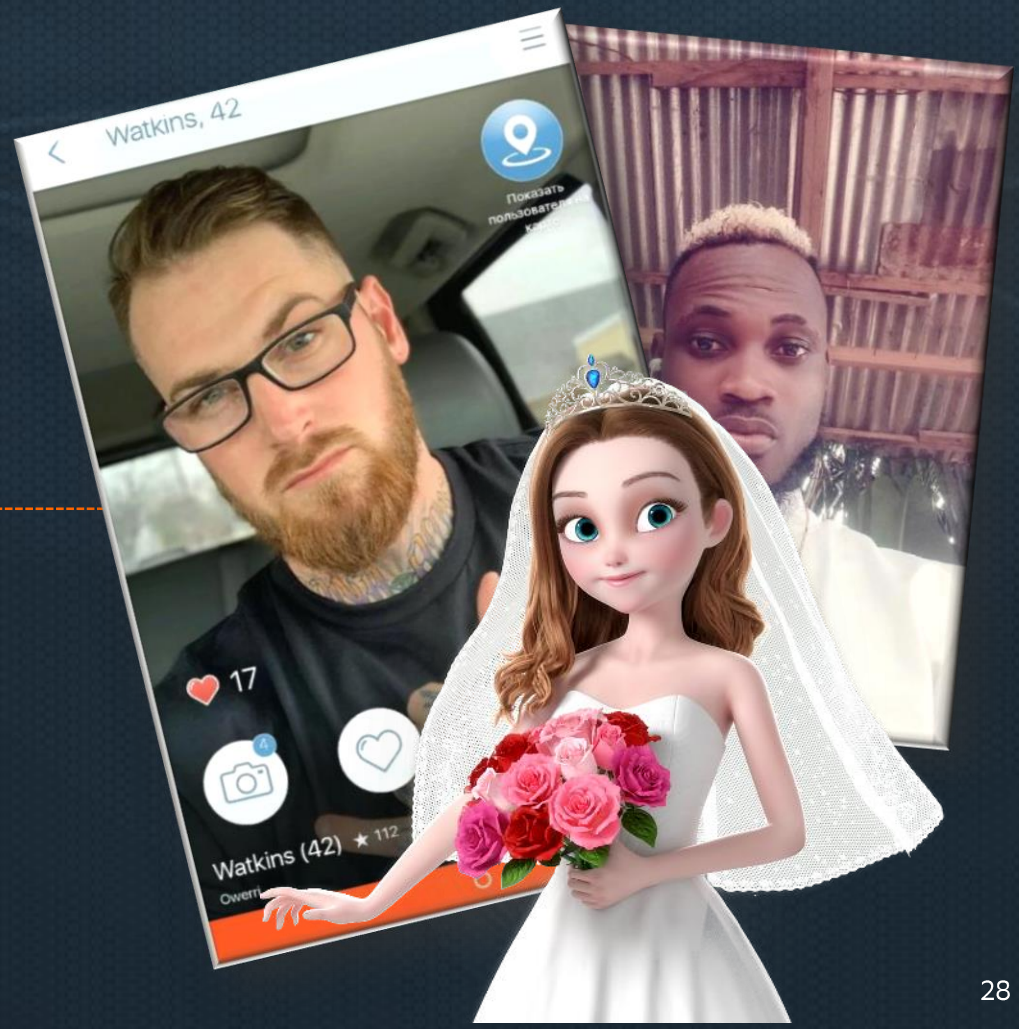
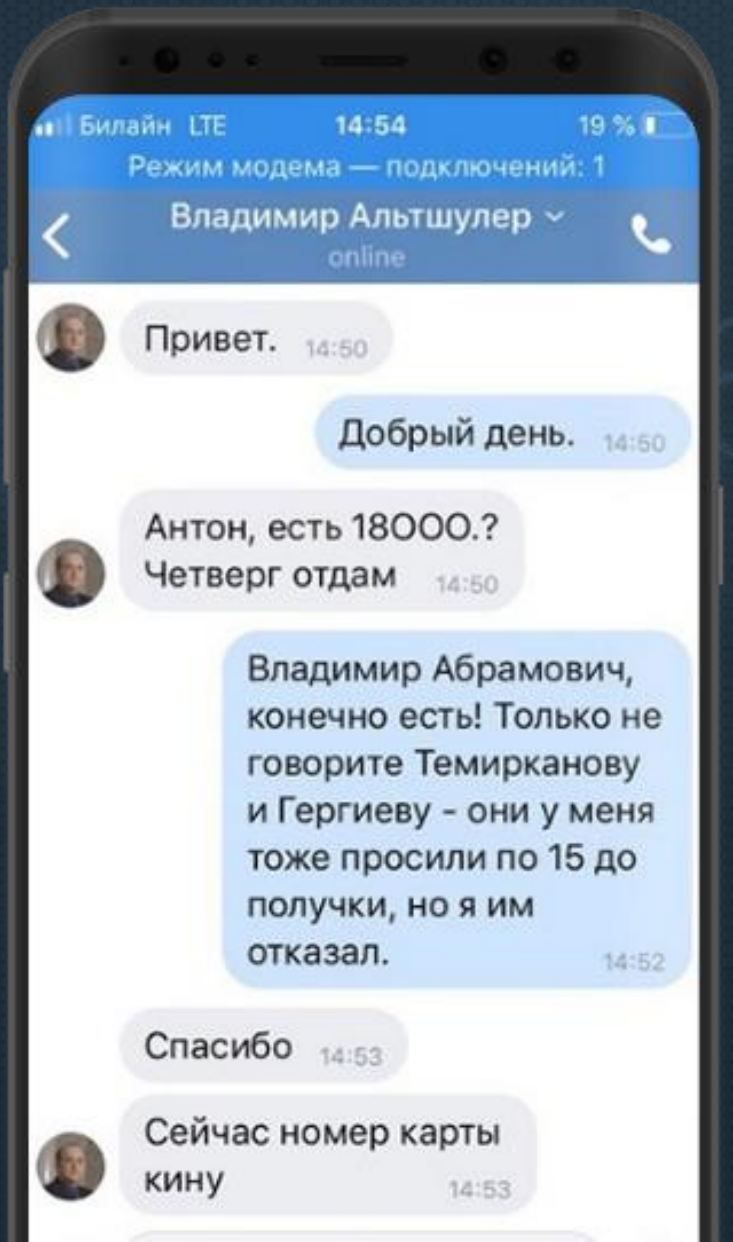


СХЕМА: Взлом аккаунта

1. Сообщение в социальных сетях со взломанного аккаунта родственника/друга.
2. В сообщении просят перевести деньги или сообщить номер карты и пароли, чтобы вывести деньги с платежных инструментов (например, интернет-кошельков).
3. Деньги нужны попавшему в беду близкому человеку, чтобы оплатить билет на самолет, залог или медицинское обслуживание, взятку за урегулирование проблем при аварии.

Варианты развития событий:

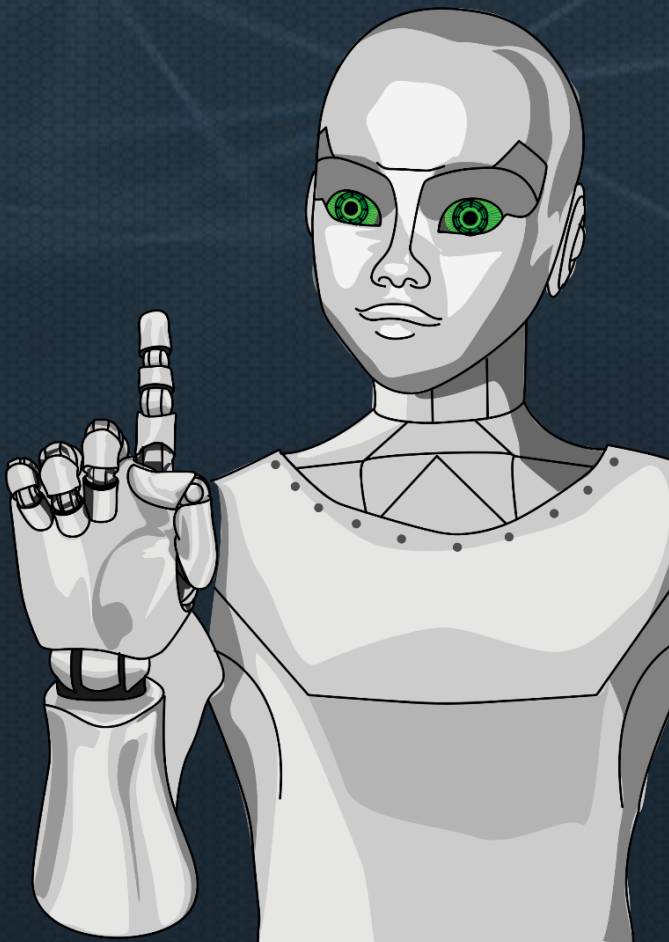
- клиент направляет деньги, после чего узнает, что аккаунт взломан;
- клиент разглашает запрошенные данные, после чего мошенник регистрируется в личном кабинете клиента и совершает неправомерные списания.



Как защитить себя: Мошенничество в социальных сетях

SCS SBER CYBER SECURITY

1. Установите на свои аккаунты сложные пароли
2. Проверьте настройки устройства и приложений – что, как и куда сохраняется, передается, с чем синхронизировано. При необходимости меняем настройки
3. Не указывайте в профиле личные, не общедоступные контактные данные (номер телефона, адрес личной электронной почты). Личные данные видят только пользователи, которые входят в круг «друзей».
4. Если необходимо сделать запись открытой для всех, настройку «по умолчанию» можно отменить для одной определенной записи
5. Не отправляйте в личных сообщениях видео и фотографии пользователям, которых ты не знаешь в реальной жизни
6. Отправляя кому-либо личную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает
7. Будьте бдительны



Советы по защите персональных данных в соц.сетях

Обнови настройки приватности

НЕ делись большим объемом информации

НЕ выкладывай фото документов

НЕ размещай информацию о родственниках

НЕ добавляй незнакомцев в друзья

НЕ используй метки и хештеги геолокации

SCS SBER CYBER SECURITY

Помогут сервисы кибербезопасности

Cybersecurity HUB. Сервисы кибербезопасности

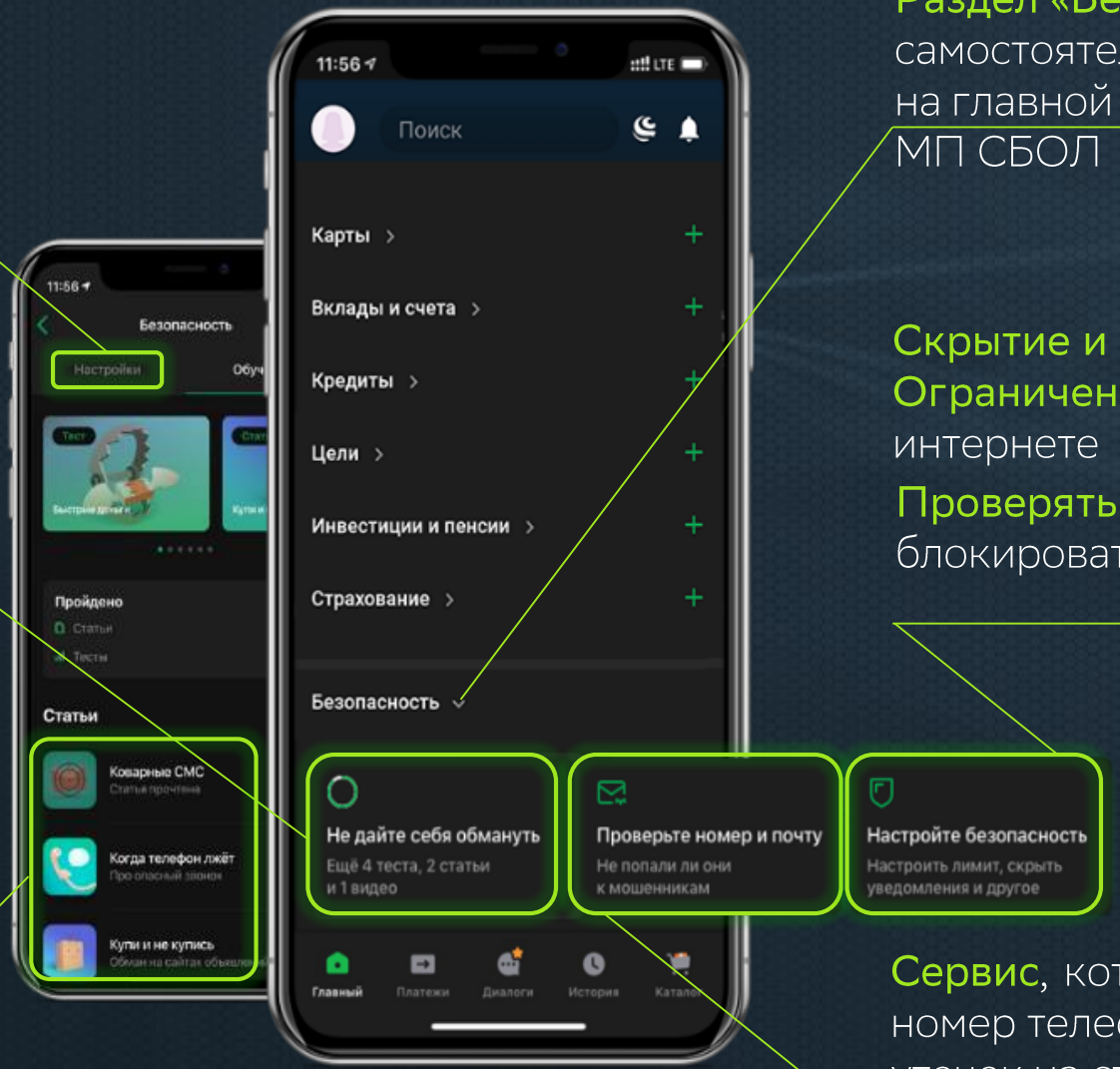
SCS SBER CYBER SECURITY

Настройки безопасности в мобильном приложении СберБанк Онлайн

Раздел «Безопасность» самостоятельный раздел на главной странице в МП СБОЛ

Раздел «Не дайте себя обмануть» простым и понятным языком о том, как не попасться на уловки мошенников

Скрытие и отображение карт, счетов и вкладов
Ограничение суточного лимита и оплат в интернете
Проверять входящие звонки позволяет блокировать мошеннический звонок



Сервис, который позволяет проверить ваш номер телефона и адрес e-mail на предмет утечек на сторонних ресурсах

Ежемесячное обновление обучающего контента

Подпишитесь на канал «Осторожно, мошенники!» в Сбербанк Онлайн

В канале **«Осторожно, мошенники!»** регулярно публикуются самые актуальные мошеннические схемы и способы защиты от них

2 новых поста

каждую неделю

Раздел «Ваша безопасность» на сайте Сбера

Мы собрали для вас самые полезные материалы по правилам кибербезопасности (статьи, тесты, памятки, шпаргалки, FAQ)

«Сообщить о мошенничестве»

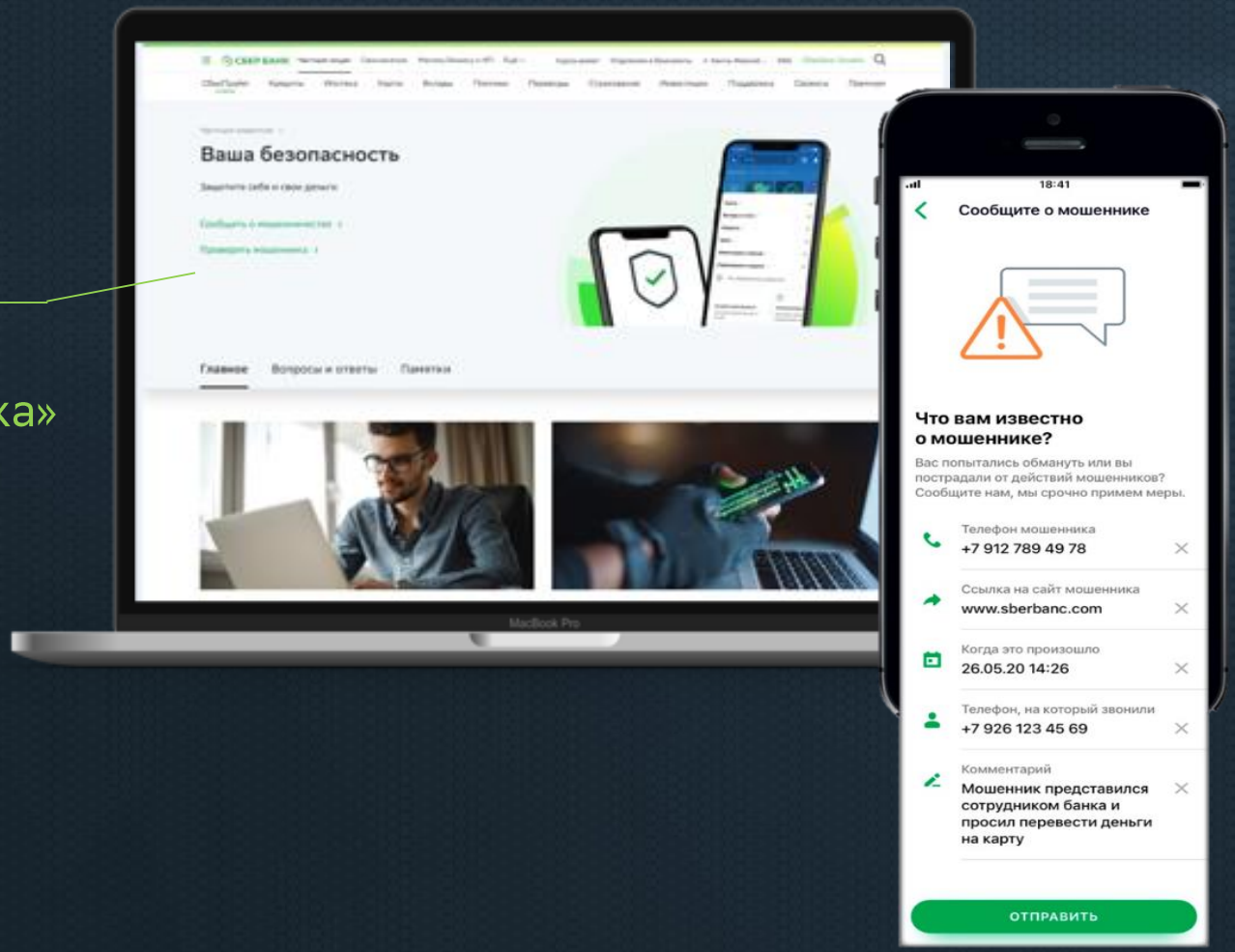
Форма обратной связи.

Защитите себя и свои деньги: сообщите об инциденте

«Проверить мошенника»

Форма обратной связи.

Проверьте телефон и сайт предполагаемого мошенника



Будьте бдительны!

1. Запишите номера банка 900 и 8-800-555-55-50 в телефонную книгу
2. Не сообщайте номер своей банковской карты, срок действия, CVV-код и код из СМС
3. Не совершайте никаких операций по инструкциям звонящего
4. Не открывайте ссылки из сообщений от незнакомых номеров
5. Установите на свои аккаунты сложные пароли
6. Устанавливайте на свои устройства программное обеспечение только из официальных источников
7. Перепроверяйте все акции на официальных сайтах и страницах в социальных сетях
8. Если для получения большой суммы денег вам сначала предлагают потратить сравнительно небольшую, будьте осторожны, это мошенничество
9. Заведите несколько адресов электронной почты для разных целей
10. Не отправляйте незнакомым людям кому-либо личную информацию
11. Проверяйте настройки устройства и приложений
12. Будьте осторожны с вложениями, открывайте только те, которые ждали
13. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы