ЧАСТО ВСТРЕЧАЮЩИЕСЯ СХЕМЫ МОШЕННИЧЕСТВА –

КАК ВЫЯВИТЬ И КАК ЗАЩИТИТЬСЯ

- 2024

Звонки. Предложение продлить срок действия СИМ-карты/пролонгации договора сотовой связи.

Человеку от имени сотового оператора сообщается о необходимости продления сим-карты/договора на сотовую связь по причине завершения срока их действия.
Под этим предлогом злоумышленник пытается получить данные для входа в личный кабинет абонента, а также одноразовые коды для проверки.

Если это удастся сделать, мошенники настраивают переадресацию СМС на свой номер. И начнут получать все сообщения, в т.ч. от любых сервисов и банков.
В результате мошенники смогу добраться до личного кабинета человека и украсть из него деньги.

Как защититься:

Всегда помнить, что у сим-карт нет срока действия и их не нужно продлевать. По всем вопросам, связанным с мобильной связью, нужно обращаться или в салон сотовой связи, или по официальным контактам оператора.
Никогда и никому не передавать логины и пароли, а также одноразовые пароли из СМС.

Звонки. Звонок из Социального фонда и соцслужб.

В последнее время популярностью пользуется еще один вид мошенничества. В основном он нацелен на пенсионеров. Мошенники притворяются соц.работниками и предлагают обновить социальные карты/карты жителя (как на телефонном звонке, так и в ходе личного контакта
с пенсионером).

Пенсионеры с радостью соглашаются на такую помощь – ведь им самим сложно вникнуть в технические нюансы.
Они называют код и номер банковской карточки. Украв данные, злоумышленники получают доступ в мобильный банк и могут легко списать все денежные накопления.

Как защититься:

Не сообщайте номер карты, код из СМС и, тем более, паспортные данные незнакомцам. При необходимости лучше обратиться в отделение Банка и на месте решить финансовые вопросы.

Звонки. Звонок мошенников через приложение сайтов объявлений (Авито/Юла/иные).

Мошенники придумали новый способ обмануть людей, которые продают товары на площадках объявлений. Теперь мошенники не просят перейти в мессенджер для обсуждения деталей, а звонят прямо в приложении сервиса.
Популярные сайты с объявлениями используют скрывание реальных номеров продавцов в целях безопасности. При этом продавец и покупатель могут созвониться с помощью встроенного сервиса на площадке.

Именно доверие людей к официальному приложению и используют мошенники: человек больше склонен верить, что с ним связался реальный покупатель. На самом деле звонит мошенник, который предлагает внести предоплату за товар. Для этого ему нужны данные карты продавца
и код из СМС – «для подтверждения перевода». С таким набором данных мошенник может войти в интернет-банк собеседника.

Как защититься:

Мошенники, действующие по такой схеме, обычно не спрашивают про товар, не просят дополнительные фото и не торгуются.
Вас должна насторожить просьба прислать данные карты и, тем более, одноразовый пароль из СМС/PUSH. Об этом могут попросить только мошенники.

Звонки. Схема с «безопасным счетом» в ЦБ – новый поворот.

Начало этой мошеннической комбинации точно известно многим. Мошенник звонит от имени сотрудника банка или полиции и говорит, что ваши деньги под угрозой и их нужно срочно перевести на «безопасный счет» в ЦБ.

А вот дальше – новинка. По словам мошенника, после окончания расследования эти деньги вам вернут наличными в Общественной приемной Банка России.
И чтобы вы этому поверили, мошенники действительно записывают Вас на прием в Центробанк.

В результате Вам приходит СМС с официального номера ЦБ и временем записи.

Как защититься:

Никаких специальных «безопасных» счетов не бывает.
Если Вы «беспокоитесь» за сохранность своих денег, надо позвонить на горячую линию своего банка (номер 1000 для Банка ВТБ). Кем бы не представлялись незнакомцы, нельзя переводить деньги по их уловке.

Если Вам пришло СМС-подтверждение записи на прием в Центробанк, хотя сами Вы на него не записывались, просто игнорируйте это сообщение.

Звонки. Схема с МИР Pay и наличными.

Мошенники убеждают клиента, что деньги нужно перевести на безопасные счета.

Для этого:
1. Сначала просят снять наличными все деньги со счета в банке, где они у него есть.
2. Затем просят добавить в Mir Pay карты, открытые якобы на имя клиента, убеждают, что это и есть безопасные, резервные счета.
3. Далее просят внести наличные на эти карты в АТМ, используя Mir Pay.
4. Мошенники выводят поступившие на карту деньги практически одновременно с внесением.

Карты, которые злоумышленники выдают за безопасные счета, на самом деле оформлены на третье лицо, клиент переводит деньги мошенникам.

Как защититься:

Если вас просят перевести деньги на безопасный счет – будьте уверены, вы имеете дело с мошенниками.
Не добавляйте в приложения по бесконтактной оплате карты, которые сами не выпускали. Чтобы проверить, действительно ли на ваше имя открыта карта, обратитесь в банк по официальному номеру горячей линии (номер 1000 для Банка ВТБ).

Мессенджеры. Подарок на День рождения.

Ситуация: у клиента действительно День рождения.

Клиенту поступает поздравление с Днем рождения от крупной компании (М.Видео, Эльдорадо, МТС, ВТБ и др.). Предлагают получить бонусы, деньги, огромные скидки на бытовую технику и т.п.

Клиент переходит на фишинговый сайт с большими скидками.

Для оплаты или получения денежного подарка предлагают ввести данные банковской карты, либо QR-код СБП.
В процессе оплаты могут появляться ошибки (цель – списать больше денег).

Клиент переходит на фишинговый сайт, вводит данные карты либо QR-код СБП и теряет деньги.
Клиент может говорить, что оплачивает товар в магазине, а фактически в ВТБ Pro на подтверждении будет перевод СБП или P2P физ. лицу.

Как защититься:

Не вводить данные карт на сомнительных ресурсах

Не открывать подозрительные электронные письма, СМС и сообщения из мессенджеров с вложенными ссылками.

Мессенджеры. Сообщение от «работодателя».

Клиенту приходит сообщение в Телеграмм, в качестве отправителя указаны ФИО руководителя с его текущего места работы.

В сообщении указано, что по работе произошла утечка данных, деньги переводятся террористам, по данному факту ведется проверка и что сегодня/завтра с клиентом свяжется такой-то сотрудник.

Клиенту звонят с неизвестного номера и представляются сотрудником Службы безопасности, напоминают, что руководитель должен был предупредить о такой коммуникации.

Далее ведется диалог о работе, своевременной выплате ЗП, коллегах и прочее. Усыпив бдительность, мошенники уточняют, в каких банках у клиента есть деньги, в каких офисах было последнее обслуживание, оформлялись ли кредиты.

Мошенники убеждают клиента, что деньги нужно вывести на безопасные счета ЦБ, просят установить стороннее приложение на телефон. Деньги обычно снимают
и переводят через АТМ на сторонние счета.

Звонившие просят сохранять чеки, так как с ними нужно будет явиться в указанную дату в ФСБ. На e-mail клиента присылают повестку. Также устанавливается фейковое приложение банка с указанием баланса клиента, с якобы спасенными денежными средствами, чтобы убедить
клиента в их сохранности.

В ходе диалога мошенники могут меняться на сотрудников МВД, ЦБ и пр. Звонящие запрещают вести диалог, если рядом кто-либо находится, пугают уголовной ответственностью за разглашение информации.

Требуют вслух повторять информацию, которую они предоставили, чтобы проверить понимание клиента ситуации. Запрещают завершать диалог или не отвечать
на звонки, аргументируя тем, что клиент сам попадет
под следствие.

Мошенники благодарят за помощь, напоминают
о явке в ФСБ и далее не выходят на связь.

Получая сообщение, клиент не сверяет контакт отправителя с реальным номером телефона руководителя, верит названию контакта, так как ФИО совпадают.

Мошенники вытягивают данные о банковских продуктах клиента, запугивают уголовной ответственностью, вводят
в «гипноз» и заставляют переводить им деньги.

Как защититься:

Не сообщать свои данные при поступлении звонка, якобы, от службы безопасности Банка, МВД, ЦБ и прочее.

Не устанавливать приложения по просьбе незнакомых лиц.

Маркетплейсы. Предложение работы на маркетплейсах/Авито.

Новая мошенническая ловушка – заманивание людей легким заработком на маркетплейсах. Мошенники отправляют сообщение с предложением о трудоустройстве в Ozon, Wildberries и других крупные сервисы.

Пользователям сулят огромные деньги (до 100 тысяч рублей) за легкую работу с занятостью буквально два-три часа в день. Задания очень простые, например, написать пару отзывов (за товар, или отель) или выложить фото товара на сайт – в общем то, с чем справится любой человек без опыта.

Но не все так просто – бесплатный сыр бывает только в мышеловке. Чтобы приступить к работе, мошенник просит заплатить символический взнос. Сумма может быть разной — от 500 до 2 000 рублей. Именно этот взнос мошенник и собирается украсть.

Как защититься:

Помните, что бесплатный сыр бывает только в мышеловке. Не переводите деньги незнакомым лицам, ни при каких обстоятельствах.

Мессенджеры. Звонок в мессенджере о налоговой задолженности.

Клиенту поступает звонок/сообщение через мессенджеры. Ему сообщают о наличии налоговой задолженности и просят сразу оплатить. Сообщение может содержать ссылку для проверки задолженности.

Клиент переводит деньги мошенникам, думая, что оплачивает задолженность по налогам.

Как защититься:

Помнить, что сотрудники Федеральной налоговой службы не используют такой способ связи как мессенджеры.

Проверить задолженность всегда можно в личном кабинете налоговой службы.

Соцсети. Мошенничество с авиабилетами: как защититься.

На каникулах и праздниках многие планируют поездки в другие города, регионы и страны. Путешественников может подстерегать набирающая популярность уловка злоумышленников.

Они мониторят публичные чаты и группы в соц.сетях, посвященные путешествиям, находят там людей, интересующихся скидками и акциями на покупку билетов. Мошенник пишет пользователю, представляясь представителем известной авиакомпании, турагентства или билетного агрегатора. Он предлагает человеку воспользоваться его большой корпоративной скидкой за скромное вознаграждение. Как только «путешественник» переведет деньги «за билеты», фейковый «помощник» тут же пропадет.

Как защититься:

Выбирайте для покупки билетов официальный сайт перевозчика или проверенный, зарекомендовавший себя билетный сервис. Перед покупкой внимательно изучите страницу: посмотрите, совпадают ли название сайта в адресной строке и бренд, указанный на странице, все ли кнопки работают, нет ли множества грамматических ошибок и неточностей на странице.
Не вступайте в переписку с соц.сетях или мессенджерах с людьми, которые говорят, что являются представителями авиакомпании или турагентства.

Соцсети. Использование искусственного интеллекта для подделки голоса близкого/знакомого.

Злоумышленники взламывают аккаунт в соцсетях или мессенджерах, находя в переписках записанные человеком голосовые сообщения. После этого, используя искусственный интеллект, создают аудиозаписи якобы от лица владельца аккаунта.

Когда все готово, через соц.сеть или мессенджер человека, чей профиль взломали, направляется запрос на одалживание денег/помощь в сложной жизненной ситуации. Просьбу в т.ч. подкрепляют отправлением сгенерированного голосового сообщения.

Как защититься:

Подключить двухфакторную аутентификацию во всех сервисах, где это возможно.
Если знакомый в мессенджере или соц.сети обращается с просьбой прислать денег, всегда нужно перепроверять информацию, позвонив ему по телефону.

Мессенджеры. Розыгрыш билетов.

Концерты, шоу, спектакли – неотъемлемый атрибут любых праздников. Чтобы выманить деньги у желающих отдохнуть, мошенники делают массовые рассылки в мессенджерах.
В сообщениях предлагается поучаствовать в бесплатном розыгрыше билетов на представление. Для этого нужно перейти по ссылке из сообщения, заполнить «заявку»
и ввести данные карты якобы для оплаты небольшой комиссии.
Если человек доверится и сделает это, то потеряет и платежные данные карты, и деньги.

Как защититься:

Покупайте билеты на мероприятия только на официальных сайтах организаторов или в проверенных билетных сервисах (Афиша.ру, Тикетлэнд, Яндекс.Афиша, МТС Live)
Не участвуйте в розыгрышах, условия которых требуют поделиться платежными данными или деньгами.

Трудоустройство. Видеособеседование с целью кражи одноразовых паролей на вход в личный кабинет Банка.

Новая схема мошенничества – предложение пройти видеособеседование с работодателем. В ходе видеособеседования кандидату поступает PUSH/СМС-сообщение от обслуживающего Банка, которое отображается на экране видеоконференции с «работодателем».
Оно доступно/видно мошенникам, которые с его помощью входят в личный кабинет собеседника и похищают денежные средства.

Как защититься:

Игнорируйте подобные сообщения. Искать работу лучше на проверенных ресурсах, например, HH.ru, SuperJob, Работа.ру. и других.
Выбирайте работодателя с высоким рейтингом, давно зарегистрированного и известного на рынке. Изучите отзывы о компании в интернете. При их отсутствии
или сплошь отрицательных отзывах высокая вероятность встретить мошенников.

Проводите видеособеседования или со стационарных компьютеров, или с телефона, к которому не привязаны мобильные приложения банков.

НОВОЕ В ЗАЩИТЕ КЛИЕНТОВ С 25.07.2024 – 2 ДНЯ ПЕРИОД ОХЛАЖДЕНИЯ

Изменения в Федеральный закон 161-ФЗ в связи с вступление в действие 369-ФЗ
(совершенствование механизма борьбы с хищением денежных средств со счетов граждан)*

ИЗМЕНЕНИЯ 25.07

КЛИЕНТ

совершает перевод (ненадежный получатель)

БАНК

- СВЕРКА С ДАННЫМИ ЦБ
- ОТКЛОНЕНИЕ И БЛОКИРОВКА, ЕСЛИ ПОЛУЧАТЕЛЬ В БАЗЕ ЦБ

КЛИЕНТ

обращается в КЦ / ТП за разъяснениями

СОТРУДНИК ТП

- ПРИЧИНА БЛОКИРОВКИ ПОЛУЧАТЕЛЬ ПЕРЕВОДА В БАЗЕ ЦБ
- ИНФОРМИРУЕТ КЛИЕНТА: «БАНК ОБЯЗАН ДАТЬ 2 ДНЯ (48 ЧАСОВ) ПОДУМАТЬ И ПРИНЯТЬ РЕШЕНИЕ О ПЕРЕВОДЕ»
- ПРОВОДИТ ВИЗУАЛЬНУЮ ОЦЕНКУ
- ПРОСТАВЛЯЕТ РЕЗОЛЮЦИЮ КЛИЕНТА (ВТБ ПРО)
- СНИМАЕТ БЛОКИРОВКУ ВТБ ОНЛАЙН

КЛИЕНТ

- подтверждает в КЦ/ТП необходимость перевода, повторно проводит операцию тому же получателю на ту же сумму.
- операция будет технически отклонена для предоставления клиенту 2-х дней (48 часов) на принятие решения
- при необходимости проводит операцию через 2 дня (48 часов) в течение 24 часов тому же получателю на ту же сумму.

ЦЕЛЕВАЯ СХЕМА

КЛИЕНТУ

- СМС – нотификация об отклонении/приостановке операции
- Отсутствие блокировок
- Баннеры в ВТБО с причиной приостановки/отклонения

СОТРУДНИКУ

- Возможность просмотра причины отклонения/приостановки перевода

Получатель перевода, попавший в неблагонадежные списки ЦБ/МВД, может подать заявление на исключение из списков в интернет-приемной Банка России /ТП Банка ВТБ

*Федеральный закон «о национальной платежной системе» от 27.06.2011 №161-ФЗ Федеральный закон «о внесении изменений в федеральный закон «о национальной платежной системе» от 24.07.2023 №369-ФЗ