Генеральная прокуратура Российской Федерации
Прокуратура Иркутской области

«Уловки мошенников, на которые попадаются умные люди»

г. Иркутск, 2024

«Звонок из банка»

Мошенническая схема:

поступает телефонный звонок от имени сотрудника банка, который сообщает сведения об оформлении кредитной заявки на имя собеседника, настаивает на получении данного кредита в целях закрытия заявки и невозможности дальнейшего получения мошенниками второго кредита в рамках отведенного для клиента кредитного лимита, полученные денежные средства собеседник просит оперативно перевести на «безопасный, резервный, специальный» счёт для обеспечения их сохранности.

Как себя защитить:

- ✓ Запомните!!! Банки, ЦБ РФ, **с такими предложениями не звонят!**
- ✓ **Не спешите отвечать** на звонки с незнакомых номеров, перезванивать по пропущенным вызовам с незнакомых номеров.
- ✓ Если Вы поняли, что разговариваете с мошенником – **немедленно прекратите разговор,** на повторные звонки не отвечайте! Не продолжайте разговор в целях развлечения!
- ✓ Никогда, никому и ни при каких обстоятельствах **не сообщайте** по телефону: пин-код карты, срок действия карты, код безопасности, СМС-код

«Родственник в беде»

Мошенническая схема:

поступает телефонный звонок, собеседник представляется сотрудником правоохранительных органов, сообщает о дорожно-транспортных происшествиях, произошедших по вине их близких родственников и о возможности избежать уголовной ответственности за определенное вознаграждение. Деньги просят передать сотрудникам, которые прибудут к Вам. О разговоре просят никому не сообщать, чтобы еще больше не навредить родственнику или ссылаясь на тайну следствия.

Как себя защитить:

- ✓ «Золотое правило»: **сохранять спокойствие и рассудительность!**
- ✓ Запомните!!! Правоохранители **с такими предложениями не звонят!**
- ✓ Постарайтесь, чтобы разговор слышал кто-то из рядом присутствующих.
- ✓ Уточните, когда и где произошло ДТП.
- ✓ Скажите, что уточните информацию и положите трубку!
- ✓ **Перезвоните родственнику!**
- ✓ Позвоните на «горячую линию» или «телефоны доверия» органов полиции, подробно опишите сложившуюся ситуацию, уточните алгоритм своих действий.
- ✓ Не переводите деньги мошенникам!

«Сказочные инвестиции»

Мошенническая схема:

вдохновившись уровнем дохода людей, получающих прибыль от инвестиционной деятельности, на просторах Интернета находите фирму, которой распространяется информация об осуществлении легальной деятельности финансового посредника (форекс-дилера). Лицо, выступая от имени такой компании, злоупотребляя доверием граждан к легальным финансовым институтам, обещая им получение высоких доходов путем торговли на международном финансовом рынке, предлагает перечислить денежные средства на счета определенных организаций, после чего денежные средства похищаются, общение с гражданами-инвесторами прекращается.

Как себя защитить:

- ✓ **На сайте ЦБ РФ** проверьте является ли компания, которую Вы планируете выбрать в качестве финансового посредника, профессиональным участником рынка ценных бумаг, имеет ли лицензии на осуществление брокерской, дилерской, депозитарной деятельности, управление ценными бумагами!
- ✓ Если Вы заинтересовались инвестиционной деятельностью внимательно и всесторонне изучите данный вопрос, обратитесь к проверенным финансовым консультантам.
- ✓ Оцените все существующие риски данного вида деятельности!
- ✓ Объективно оцените реальность обещанного дохода!

«Сайты-двойники»

Мошенническая схема:

для входа в онлайн-банкинг Вы вводите его название в поисковике и переходите по ссылке, внешний интерфейс страницы очень схож с тем, который Вы привыкли видеть, далее вводите свои данные для входа в онлайн-банкинг или данные банковской карты. После ввода всех данных появляется сообщение об «ошибке оплаты».

Аналогичная ситуация может возникнуть с сайтами-«двойниками» известных онлайн-ритейлеров, маркетплейсов.

Как себя защитить:

- ✓ Не переходите по подозрительным ссылкам!
- ✓ Официальные сайты банков в популярных поисковиках отмечены специальным значком **(синий кружочек с галочкой).**
- ✓ Безопасность соединения гарантируют: зашифрованный протокол связи – **«http://..» и замочек в адресной строке.**
- ✓ **Зарплатная карта ≠ расчетная!**
- ✓ В случае возникновения подозрительных ситуаций («ошибка системы», «прервана связь с банком», «переход на резервную страницу» и т.д.) прекратите платежную операцию, позвоните на горячую линию банковской организации.

«Онлайн-курсы»

Мошенническая схема:

заинтересовавшись тренингом личностного роста, онлайн-курсом по психологии (кулинарии похудению), марафоном стройности (правильного питания, полезных привычек), вводите контактные данные. После чего с Вами связывается продавец услуг и предлагает осуществить перевод через мобильный банк, после чего на звонки не отвечает.

Как себя защитить:

- ✓ Найдите отзывы о предлагаемой Вам услуге.
- ✓ Подробно расспросите оферента о форме, сроках проведения мероприятия, способах получения доступа к учебным материалам.

«Фейковые объявления»

Мошенническая схема:

на известных сайтах: «Авито», «Юла» и др. размещаются объявления о продаже техники, автозапчастей, сдаче загородного дома в аренду на выходные/праздники. При выходе на продавца им предлагается перейти для обсуждения деталей сделки и цены в другой мессенджер, перевести оплату за товар/аренду в полном объеме (или частично) через мобильный банк. После чего Ваш номер заносится в «чёрный список», технику/запчасти Вы не получаете, объекта недвижимости, запланированного Вами к аренде, не существует.

Как себя защитить:

- ✓ Прочитайте отзывы о продавце!
- ✓ Попросите прислать дополнительные фото/видео товара, объекта недвижимости.
- ✓ Проверьте существуют ли реально такой адрес/объект недвижимости!
- ✓ Не переходите для общения в другие мессенджеры.
- ✓ Воспользуйтесь доставкой, предлагаемой непосредственно сайтом объявлений.
- ✓ С настороженностью отнеситесь к объявлениям, в которых цена существенно отличается от среднерыночной.

«Предоплата»

Мошенническая схема:

увидев в Интернете рекламу нового салоны красоты (оздоровительного центра), Вы связываетесь через мессенджер с администратором по указанному номеру для записи на процедуру. В целях подтверждения записи, ссылаясь на большую очередь желающих попасть на данную процедуру, Вас просят перевести предоплату. После перевода денег- Вас блокируют в мессенджере. Вы в назначенное время приезжаете по указанному адресу, однако, такого салона красоты не существует.

Как себя защитить:

- ✓Убедитесь, что действительно в Вашем городе открылось указанное заведение (загляните в справочные системы, сравните приведённые номера телефонов).
- ✓Предложите, нарочно отдать предоплату.

«Пенсионные юристы»

Мошенническая схема:

«Вам положена пенсия больше, чем получаете сейчас», «Поможем в перерасчете» сообщают пожилым людям мошенники, представляющиеся юридическими фирмами, помогающими составить обращения в Пенсионный фонд за вознаграждение от 20 до 250 тысяч рублей. В результате оказывается, что перерасчет по закону не положен, а сами обращения составлены некорректно.

Как себя защитить:

- ✓ Если вам позвонили «пенсионные юристы», отвечайте, что уточните информацию в ПФР, и сразу кладите трубку.
- ✓ Не поддавайтесь на уговоры, которые могут быть убедительными и многообещающими.
- ✓ Не переходите по рекламным ссылкам на сайты, предлагающие услуги несуществующих юридических центров, не начинайте общение во всплывающих чатах-помощниках, чтобы получить, якобы, бесплатную консультацию.

«Старый приятель»

Мошенническая схема:

порой мошенникам удается выстроить телефонный разговор таким образом, что **собеседник сам делает предположение кто ему звонит** (старый приятель, родственник, с которым давно не общались), убедившись, что разговор ведется в доверительном русле злоумышленники могут попросить небольшую сумму в долг.

Как себя защитить:

- ✓ При поступлении подобного звонка всегда давайте возможность собеседнику представиться самому.
- ✓ Не стесняйтесь задать уточняющий или ложный вопрос.
- ✓ Не переводите деньги малознакомым людям!

«Вам звонят из библиотека»

Мошенническая схема:

мошенники в ходе телефонного звонка представляются пожилым людям работниками библиотек и, ссылаясь на то, что когда-то читателем не были возвращены книги, требуют оплатить компенсацию, предлагают направить своего представителя для получения денег непосредственно по месту жительства. В противном случае, грозят обратиться в суд или высказывают иные угрозы.

Как себя защитить:

- ✓Скажите, что уточните информацию непосредственно в библиотеке и кладите трубку!
- ✓Не поддавайтесь на угрозы и требования мошенников!
- ✓Ни в коем случае не сообщайте свой домашний адрес!

«Успеть сохранить свой абонентский номер»

Мошенническая схема:

поступают звонки, якобы, от сотовых операторов, ссылающихся на истечение срока пользования сим-картой, для сохранения своего абонентского номера просят назвать код из СМС или данные документов.

Как себя защитить:

- ✓ Сказать собеседнику, что Вам неудобно сейчас говорить и Вы сами перезвоните службу поддержки мобильного оператора!
- ✓ Не сообщайте никакие данные и коды!

«Налоги»

Мошенническая схема:

Поступают письма на электронные адреса граждан, в которых требуется перейти по ссылке и заполнить декларацию или рассылают письма со ссылкой предупреждения, что со счетов вскоре спишут новый налог. Перейдя по ссылке, открывается поддельный сайт банка, где требуется ввести персональные данные гражданина.

Как защитить себя:

- ✓ При поступлении подобного письма не переходите по ссылке указанной в письме
- ✓ не заполняйте указанную в нем декларацию
- ✓ Не переходите по ссылке указанной в письме
- ✓ Зайдите на официальный сайт личного кабинета налогоплательщика и проверьте начисление налогов.

«Нужды на СВО»

Мошенническая схема:

Поступает сообщение от банка о том, что в связи с распоряжением Правительства будет ежемесячно списываться сумма на нужды СВО, если отсутствует согласие, то необходимо перейти по ссылке, указанной в сообщении и отказаться от ежемесячного взноса

Как защитить себя:

- ✓Запомните!!! Банки не направляют подобные сообщения. Распоряжений Правительства РФ подобного формата **не существует**
- ✓Не переходите по ссылке указанной в письме

«Звонок о продлении договора»

Мошенническая схема:

Представляясь специалистами известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту гражданина на «Госуслугах».

Злоумышленник звонит жертве и утверждает, что действующий договор заканчивается и его необходимо продлить. При этом мошенники уверяют, что все можно сделать по телефону и не идти в офис, достаточно продиктовать код из СМС, перейти по ссылке, где ввести еще один код. Таким образом человек путем обмана предоставляет мошенникам данные для входа в личный кабинет «Госуслуги».

Как защитить себя:

- ✓Прекратите телефонный звонок
- ✓Не сообщайте коды из СМС
- ✓Не переходите по ссылке
- ✓Обратитесь в офис компании, с которой заключен договор, и уточните информацию