Информация о способах совершения мошенничеств и методах защиты от них

Самые распространенные виды мошенничества.

Схема 1. Операторы сотовой связи. («действие вашей сим-карты заканчивается», «какой у вас оператор связи?», «продиктуйте код из СМС»)

На ваш смартфон поступил звонок якобы от "Оператора сотовой связи" и сообщают вам, что срок вашего договора истек и теперь появилась возможность продлить его на более выгодных условиях.

Доверчивые жители региона соглашаются на заманчивое предложение и, по рекомендации собеседника, устанавливают на смартфон приложение, с помощью которого якобы можно будет активировать тарифный план.

Затем злоумышленники просят продиктовать код доступа из СМС, с помощью которого получают возможность удаленно управлять вашим смартфоном, а также могут получить доступ к вашим приложениям кредитных учреждений!

Помните: Операторы сотовой связи, никогда не будут предлагать вам продлить договор дистанционным способом! Прервите разговор и положите трубку! Не в коем случае не устанавливайте сторонние-неизвестные приложения на ваш смартфон! Не сообщайте посторонним людям коды, которые приходят вам из СМС! Обратитесь лично в службу поддержки оператора сотовой связи или сообщите в полицию!

Схема 2. Предложения от лжеброкеров. («откроем брокерский счет для получения прибыли», «оплатите страховой взнос за инвестиции», «продиктуйте свои данные для регистрации в нашей брокерской компании»)

В сети Интернет жители нашего региона находят объявление о сверхдоходном бизнесе, да еще с процентной надбавкой. Переходят по предложенной ссылке, регистрируются и спустя некоторое время с ними на связь выходит якобы "аналитик торговой платформы". Он предлагает скачать программу электронной биржи, открыть индивидуальный брокерский счет, внести первый взнос, а затем просто следить за тем, как преумножаются ваши доходы.

Ваши доходы начинают на глазах увеличиваться, вы чувствуете уверенность в своих силах и начинаете инвестировать более крупные суммы.

Когда же вы выразите желание забрать заработанные средства, работники платформы попросят вас оплатить "страховой взнос за инвестиции" либо предъявить «промо-код», который приобретается за дополнительные денежные средства. Так как дополнительных денежных средств у вас нет, вы прибегает помощи к кредитной организации и продолжаете снова и снова отправлять злоумышленникам денежные средства!

Помните: доверять заманчивым предложениям о получении быстрого и легкого заработка не нужно! Задача злоумышленников, с помощью манипуляции завладеть всеми вашими денежными средствами! Прекратите общение с "брокером" и обратитесь в полицию!

Схема 3. Звонки или сообщения от знакомых. («я в беде, связи нет, говорить не могу, нужны деньги», «проголосуйте за мою племяшку вот по этой ссылке», «посмотри хороший материал - пройди по ссылке»)

Среди ночи вам раздается телефонный звонок, неизвестный (он может представиться сотрудником правоохранительных органов) сообщает, что ваш родственник попал в беду. Требуется помощь – деньги. Цель мошенников – воспользоваться вашей растерянностью, удерживать на телефоне до тех пор, пока вы не переведете или не передадите деньги курьеру.

Помните: В этом случае нужно под любым предлогом прекратить разговор! Перезвонить своему родственнику или людям, которые точно могут знать, где он сейчас находится (жена, дети). Если же по какой-то причине вы не можете сразу связаться с родственником, не паникуйте, будьте бдительны, ни в коем случае не торопитесь переводить и не передавать никому деньги, пока не выясните правд

Схема 4. Звонки и сообщения из банка. («на вас кто-то прямо сейчас оформляет кредит», «прямо сейчас у вас списываются деньги», «замечаем в последние дни странные операции по вашей карте», «вам надо опередить мошенников и спрятать свои средства на безопасном счету»)

Вам звонят с неизвестного номера (или присылают сообщение в мессенджере) и представляются сотрудниками правоохранительных органов или центрального банка и сообщают, что на ваше имя злоумышленники пытаются оформить кредит. Чтобы остановить данную операцию, необходимо оформить "Зеркальный заем".

Помните: если вы получили данное сообщение или вам поступил подобный звонок, не нужно паниковать! Представители данных учреждений, никогда не будут пытаться с вами связаться, через мобильное устройство. В первую очередь необходимо прервать данный разговор! Положите трубку!

Если у вас есть подозрения, что кто-то, пытается оформить на ваше имя кредит, необходимо лично перезвонить в службу поддержки кредитного учреждения, номер телефона которого, указан на обороте вашей банковской карты! Либо обратиться лично в ближайшее отделение или обратиться в полицию!

Не в коем случае по телефону не сообщайте никаких персональных данных! И не переводите деньги на неизвестные вам банковские счета!

Схема 5. Покупка товаров по привлекательной цене. (Вы увидели в продаже на популярной интернет-площадке нужную вам вещь, вам в ответ предлагают внести предоплату на банковскую карту, при этом еще всячески торопят, мотивируя высоким спросом.)

Как правило, такие сайты маскируются под известные бренды, но название их может отличаться одной буквой, будьте очень внимательны. Изучите все возможные способы оплаты, почитайте информацию о доставке.

Никогда не делайте предоплату и не переводите деньги незнакомому человеку. Нормальный честный продавец предложит вам сначала приехать и посмотреть интересующую вас вещь, и только потом уже расплатиться, передав деньги и товар из рук в руки.

Помните: если же вы все-таки решили приобрести товар онлайн или с помощью доставки! Не в коем случае не переходите по сторонним ссылкам и не оплачивайте товар с помощью сторонних программ. Оплачивайте сделку только на официальных интернет-ресурсах! Такой «продавец» собирает деньги с покупателей, а после закрывает страницу и исчезает.

Схема 6. Звонки и сообщения от государственных ведомств. («вам звонит следователь/дознаватель/судебный пристав/оперативник ФСБ...», «на вас заведено уголовное дело», «продиктуйте ваши данные, я все проверю»)

Услышали по телефону такие слова? Положите трубку. Скорее всего вам звонит мошенник! Чтобы развеять сомнения, сами перезвоните знакомому или в организацию, откуда поступил звонок.

ПОМНИТЕ! У аферистов тысяча лиц и всегда одна цель - выманить ваши деньги.

Схема 7. Вам пришло смс-сообщение с информацией, что ваша банковская карта заблокирована. (по всем вопросам предлагают обратиться по указанному в сообщении телефону.)

Не спешите перезванивать по номеру, указанному в сообщении. Если вы действительно являетесь держателем банковской карты, на ней должен быть официальный номер банка, по которому можно позвонить и проверить полученную информацию. Если вы все же звоните по номеру мошенников, и у вас просят ваши персональные данные, лучше прервать разговор!

Представляясь сотрудниками банка, преступники под различными предлогами выясняют у вас номера карт, одноразовые пароли и коды доступа, необходимые для проведения операций по банковским картам.

Помните, что сотрудники банка не будут спрашивать у вас реквизиты, они у них и так есть! Никому не сообщайте пин-, CVC- или CVV- коды банковской карты и одноразовые пароли.

Общие рекомендации по обеспечению безопасной работы в сети Интернет

- никому не передавать конфиденциальные данные (логин, пароль), в том числе родственникам, коллегам;
- использовать сложные пароли, состоящие из букв, цифр и специальных символов, исключить использование паролей по умолчанию, (второй год подряд самым популярным паролем в мире является «123456»);
- регулярно осуществлять смену паролей, обеспечить их конфиденциальность;
- использовать в работе лицензионное программное обеспечение с установленными обновлениями безопасности;
- на всех устройствах, должно быть установлено лицензионное антивирусное программное обеспечение с актуальными обновлениями;
- не использовать общественные беспроводные сети и устройства для работы с личной информацией;
- не использовать программные продукты, полученные из сомнительных источников (пиринговые и файлообменные сети), модифицированные программные продукты, не посещать ресурсы с сомнительной репутацией;
- личную информацию вводить только при безопасном соединении (URL веб-сайт должен начинаться с «https://», в интерфейсе браузера должна появиться иконка замка);
- выполнять резервное копирование важной информации.

Чтобы не стать жертвой злоумышленников при пользовании банковскими картами необходимо придерживаться следующих правил:

- никому не сообщать пин-, CVC- или CVV- коды банковской карты и одноразовые пароли;
- в торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты. В противном случае мошенники могут получить реквизиты карты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки;
- в случае потери банковской карты немедленно позвонить в банк для блокировки — это поможет сохранить денежные средства;
- подключить услугу смс-информирование — это обеспечит контроль за проведением любых операции по карте. При получении смс о несанкционированном списании средств со счета, заблокировать карту;
- установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удалённо - в интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте;
- при вводе ПИН-кода прикрывать клавиатуру. Вводить ПИН-код быстрыми отработанными движениями — это поможет в случае, установки скрытых видеокамер мошенников;
- выбирать для пользования терминалы и банкоматы, которые расположены непосредственно в отделениях банка или других охраняемых учреждениях;
- использовать банковскую карту в торговых точках, не вызывающих подозрений;
- перед тем как вставить карту в «карт приёмник» внимательно осмотреть банкомат на предмет наличия подозрительных устройств, проверить, надежно ли они закреплены. Если очевидно, что накладное устройство смонтировано кустарно (можно увидеть остатки клея, ненадежность конструкции и неравномерность крепления), то необходимо позвонить на горячую линию банка, сообщить о данном факте и воспользоваться другим банкоматом;
- в случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - рекомендуется отказаться от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.