Уважаемые граждане!

ГУ МВД России по Волгоградской области предупреждает

«Осторожно мошенники!»

В настоящее время на территории Волгоградской области продолжают регистрироваться случаи краж денежных средств с банковских счетов и мошенничеств, совершенных с использованием средств связи и сети «Интернет». Каждое 3-е преступление на территории региона совершается с использованием информационно-телекоммуникационных технологий.

Наиболее распространёнными способами хищения является:

1. Социальная инженерия, где работает человеческий фактор: злоумышленник получает всю необходимую информацию от пользователя путем введения его в заблуждение. Вам на телефон позвонил неизвестный и представился сотрудником безопасности Банка, сообщает информацию о том, что якобы с вашей банковской карты фиксировались попытки кражи денежных средств злоумышленниками, или же сообщает выдуманную операцию перевода денежных средств с вашей банковской карты и называет вымышленные данные человека, в чей адрес якобы осуществлялся перевод. С целью предотвращения вымышленного перевода, вас вводят в заблуждение и ведут переговоры. В ходе разговора вас предупреждают о конфиденциальности и предупреждают об уголовной ответственности за разглашение информации, полученной в процессе диалога с вымышленным сотрудником. Для введение в заблуждение и придания правдоподобности, мошенники могут высылать вам поддельные фотографии документов с удостоверениями, доверенностями и т.д., в подтверждение, что они действительно являются сотрудниками, например ЦБ РФ. Цель мошенников - вывести ваши денежные средства на «безопасные счета», открытые якобы в ЦБ РФ. В действительности же ваши денежные средства поступают на счета, подконтрольные мошенникам.

Схем данного вида преступления множество, а цель одна: завладеть вашими денежными средствами, заставить получить кредит в мобильном приложении банка или в отделении банка, а затем всю сумму перевести мошенникам.

Важно: мошенники могут просить вас установить сторонние приложения для удаленного доступа через ваш мобильный телефон, отправиться в ближайший банкомат и перевести денежные средства со всех ваших банковских карт на «безопасные счета». Угрозы, запугивание, оказание морального давления - это неотъемлемые инструменты преступника. Помните, мошенники используют методы социальной инженерии, которые включают в себя психологические приемы и «запудривание мозгов».

Внимание: Настоящий сотрудник банка никогда не обратится к Вам с подобной просьбой! Не сообщайте свои личные данные, данные банковских карт, пин-код, трехзначный код на обороте банковской карты, 'поступившие пароли по СМС сообщению и т.д. не соглашайтесь устанавливать на свое мобильное устройство или персональный компьютер программы удаленного доступа (Any Desk и Rust Desk).

Срочно прервите разговор и позвоните на номер горячей линии, указанный на обороте Вашей банковской карты для уточнения информации. В мобильном приложении вашего банка вы можете сообщить об абонентских номерах, с использованием которых пытались совершить мошенничество в отношении вас, тем самым вы предотвратите других людей от возможного совершения мошенничества.

2. Телефонное мошенничество под предлогом «Родственник в беде». Вам на сотовый или стационарный телефон позвонил неизвестный и представился вашим родственником или знакомым, сообщает о том, что нарушил правила дорожного движения или совершил преступление, и для решения вопроса с представителями правоохранительных органов о не привлечении к установленной ответственности просит перевести или передать денежные средства курьеру. В процессе разговора для придания правдоподобности передает трубку якобы сотруднику полиции. Как и в прошлом виде развода вас предупреждают о конфиденциальности разговора и предупреждают об уголовной ответственности за разглашение информации. Сценарий может меняться, «актеры-мошенники» будут подстраиваться под ситуацию, но цель одна: заполучить ваши денежные средства.

Внимание: Чтобы не попасться на подобные уловки мошенников:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных лиц;
- в разговоре задайте вопросы личного характера, помогающие обличить и разоблачить мошенника;
- под любым предлогом постарайтесь прервать беседу, положить трубку и самим связаться с' родственниками или знакомыми, о которых идет речь, для уточнения информации;
- не переводите и не передавайте свои денежные средства незнакомым людям ни под каким предлогом, иначе Вы рискуете их лишиться.

3. «Биржевое мошенничество» - это противоправная схема, используемая для обмана трейдеров, при которой они убеждаются в том, что могут рассчитывать на получение высокой прибыли, торгуя на фондовом рынке акциями, облигациями, валютами и криптоволютами. Другими словами, это псевдопрофессиональные участники финансового рынка, которые активно рекламируют свои услуги по организации торговли на фондовом рынке.

Этот вид мошенничества может занимать большое количество времени, до момента, пока потерпевший не поймет, что вложил свои денежные средства на биржу, а прибыль не получит.

Попасть «в биржевые сети» можно, например, при поиске работы, наткнувшись на объявление легкого заработка с минимальными вложениями.

Откликнувшись на объявление, вас пригласят на собеседование в офис. По прибытию, с вами составят договор, в котором все риски вы возьмете на себя, а также поставите свою подпись в знак согласия. Затем, для правдоподобности, вам необходимо будет пройти стажировку в районе месяца, осуществлять псевдо игру на бирже на сайте клоне, где весь алгоритм биржи заранее настроен на исключительно получение вами прибыли. Вдохновившись лёгкостью использования программы фондового рынка и быстрого получения прибыли, вас понудят вложить большую сумму денег.

организации для оформления кредита. После чего, полученные в кредит деньги вы переведёте на счет брокерской компании, внезапно ваша ставка не сыграет и вы останетесь без денег, с обязанностью выплачивать ранее взятый кредит.

Впоследствии обманутым окажетесь не только вы, а еще десятки людей. В свою очередь, брокерская компания покинет офис и переедет в другой регион России для продолжения противоправной схемы.

Помните: При оформлении договора с брокерской компанией все риски вы берете исключительно на себя.

4. Вам поступило ***СМС-сообщение с текстом «Ваша карта заблокирована», «Перевод денег отменен», «Списание денежных средств прошло успешно. Если вы не совершали покупку или перевод, звоните по номеру телефона» и т.д.***

Внимание: При получении подобных СМС сообщений ни в коем случае не перезванивайте по указанным абонентским номерам, а незамедлительно позвоните на номер горячей линии, указанный на обороте Вашей банковской карты для уточнения информации.

5. Покупка - продажа товаров, аренда жилья на сайтах бесплатных объявлений «Авито», «ЮЛА» и интернет - магазинах.

Внимание: Мошенники могут выступать как в роли покупателя, так и в роли продавца. Главное оружие кибермошенников - выуживание конфиденциальных данных: паролей, реквизитов карт, счетов для кражи денег дистанционным способом.

- вы заподозрили интернет-продавца или покупателя в недобросовестности, оставайтесь бдительными, не принимайте поспешных решений и при первых подозрениях откажитесь от сделки;
- встречайтесь с продавцом в общественном месте, так как это наиболее безопасный способ совершения покупки;
- никогда не переводите деньги незнакомым лицам, а также продавцам на непроверенных торговых интернет площадках, в качестве предоплаты и не сообщайте дополнительные данные банковских карт для внесения предоплат за реализуемый товар;
- защитите свой компьютер, мобильное устройство от вирусов;
- выбирайте безопасные сайты, интернет-магазины существующие продолжительное время и имеющие положительные отзывы реальных покупателей;
- используете систему безопасных платежей;
- заведите отдельную карту для покупок в интернете, и не держите на ней крупные денежные сбережения;
- подключите услугу смс - оповещения.

6. Сообщения в социальных сетях «Одноклассники, ВКонтакте, Инстаграмм и тд.», мессенджерах «Вотсап, Телеграм, Вайбер».

Внимание! Вам поступило сообщение от имени родственника или знакомого с просьбой занять денежные средства путем перевода на банковскую карту, не торопитесь предпринимать ни каких действий! Свяжитесь по телефону с родственниками или знакомыми, о которых идет речь, для уточнения информации.

Вас попросили проголосовать за ребенка или знакомого в конкурсе? Не делайте этого. Ссылка для голосования - фишинговая, вас попросят авторизоваться для дачи голоса, при этом вы введете свои конфиденциальные данные и укажите код-пароль, который вам придет на телефон. После чего мошенники завладеют вашим аккаунтом и начнут производить по вашим контактам рассылку сообщений аналогичного характера, а также производить переписку от вашего имени.

Внимание: не переходите по подозрительным ссылкам, не вступайте в диалог с мошенниками. Позвоните своему знакомому, от чьего имени вам поступило сообщение и сообщите ему об этом.

В случае если вы все-таки стали жертвой кибермошенников МВД Центральный банк России рекомендует:

- незамедлительно заблокировать Вашу карту;

- опротестовать операцию (в тот же день, когда вам поступило уведомление о незаконной операции, обратитесь в отделение банка, запросите выписку по счету и напишите заявление о несогласии с операцией, которую не совершали. Экземпляр заявления с отметкой банка, что оно принято, оставьте себе);

- обращайтесь в полицию с заявлением.

7. Сообщения в мессенджерах (чаще Телеграмм) от вашего руководителя.

Схема совершения дистанционных мошенничеств выглядит следующим образом: мошенники с использованием смс - мессенджера «Телеграмм» создают от имени руководителей государственных учреждений фейковые аккаунты, через которые осуществляют переписку с сотрудниками с указанием организовать взаимодействие
с якобы кураторами от ФСБ или вышестоящего государственного органа (Министерства (комитета) финансов, здравоохранения и т.д.). После чего поступает звонок
от мошенника, который представляется сотрудником ФСБ или вышестоящего государственного органа и сообщает о необходимости принять участие в оперативно-розыскных мероприятиях по изобличению мошенников в банковской сфере, которые пытались оформить кредит на сотрудника. В свою очередь, сотрудник предупреждается о неразглашении данной информации и далее, по указанию участников преступной схемы, с целью сохранения своих денежных средств, его отправляют в различные банки, где последний должен получить кредиты и перевести деньги на «безопасные счета», которые в действительности принадлежат мошенникам. Для придания правдоподобности мошеннических действий, злоумышленники могут направлять сотрудникам различные уведомления от имени Центрального банка, а также изображения служебных удостоверений.'

Внимание: не вступайте в диалог, информацию о поступлении сообщения от вашего руководителя вышеуказанного характера незамедлительно передайте своему непосредственному руководителю. Организуйте оповещение коллег самым быстрым способом, с целью предотвращения совершения преступлений. Обратитесь с

8. Аферисты обманывают волгоградцев под предлогом продления срока действия сим-карты

Человеку поступает звонок якобы от мобильного оператора. Ему сообщают, что срок действия его сим-карты истекает или уже закончился. Для продления необходимо назвать код из СМС. Мошенники убеждают, что, если этого не сделать, карту заблокируют и доступ к мобильной связи, приложениям, онлайн сервисам будет заблокирован.

Сообщив код, гражданин дает злоумышленникам доступ в личный кабинет портала Госуслуг. Там аферисты меняют пароли и могут беспрепятственно переводить деньги, оплачивать товары, оформлять кредиты. Владелец номера ничего не подозревает в этом случае, так как сообщения приходят уже на другой номер.

По данным Управления уголовного розыска, количество жертв новой схемы обмана за последние дни сентября возросло.

Полицейские обращаются к гражданам: ни под каким предлогом не называйте неизвестным коды и пароли, пришедшие в смс-сообщениях, даже если звонившие представляются сотрудниками банков, операторов мобильной связи и т.д. Этой информацией могут воспользоваться злоумышленники.

Помните! Сим-карта не имеет срока годности и при постоянном использовании продления не требует.

9. Полицейские напоминают: устанавливая в смартфоны по просьбе телефонных собеседников приложения, вы рискуете потерять деньги

Сотрудники полиции фиксируют факты, когда мошенники под видом работников банков звонят гражданам и убеждают установить специальные программы.

Аферисты называют их программами поддержки клиента, дополнительной защитой, антивирусным приложением и так далее.

Согласившись, потерпевшие переходят по присланным ссылкам, либо самостоятельно скачивают указанное приложение, а после чего обнаруживают списание со счетов своих сбережений.

Жертвой такого обмана стал 36-летний житель Фроловского района. Мужчина после разговора с неизвестным, представившимся работником банка, установил подобное приложение, после чего с его банковского счета были списаны почти 200 тыс. рублей.

В действительности, потерпевший, установил программу «RustDesk» - программу удаленного доступа и управления своим смартфоном, тем самым предоставив полную возможность по дистанционному входу в установленные на нем программы, в том числе в мобильное приложение своего банка.

!!Уважаемые граждане! Не верьте подобным звонкам, не переходите по неизвестным ссылкам, не устанавливайте неизвестные вам приложения. Будьте бдительны!

10. Мошенники обманывают под предлогом быстрого и гарантированного заработка

Представляясь сотрудниками крупных фондовых бирж, злоумышленники предлагают поучаствовать в торгах на финансовой бирже, убеждая перечислить денежные средства на определенный расчетный счет.

Жертвой такой преступной схемы стал 46-летний житель г. Волжского. Потерпевший с апреля т.г. переводил на указанный лжеброкером счет денежные средства, ожидая получения прибыли.

□ В общей сложности мужчина перечислил на счет мошенника 4 млн. рублей, большую часть из которых взял в кредит.

□ Обещанной прибыли, как и возврата своих средств, волжанин не дождался.

□ Помните: брокерские компании используют счета только юридических лиц.

Если же в процессе оформления перевода вы обнаружили, что деньги поступят на счет физического лица, знайте - вас хотят обмануть.