Государственное
казенное учреждение
"Центр развития и организационно-аналитического сопровождения образования Волгоградской области"
400074 г. Волгоград ул. Иркутская, 13
Тел/Факс. (8442) 59-57-83
ОГРН 1133443000492
ИНН/КПП 3460005194/346001001
e-mail: gku_education@volganet.ru

12.12.2023 № 4111

На № _____ от _____

Руководителям образовательных организаций, подведомственных комитету образования, науки и молодежной политики Волгоградской области

Уважаемые руководители!

ГКУ "Центр развития и сопровождения образования Волгоградской области" в соответствии с письмами ГУ МВД России по Волгоградской области от 07.12.2023 № 6/5829, первого заместителя Губернатора Волгоградской области – председателя комитета финансов Волгоградской области А.В.Дорждеева от 08.12.2023 № 04-15/17172 направляет информационные материалы по профилактике телефонных и иных мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий в отношении работников сферы образования, для использования в работе и размещения на информационных стендах организаций.

Приложение: в электронном виде.

Директор ГКУ "Центр развития
и сопровождения образования
Волгоградской области" Д.Е.Орехов

Кузнецова Елена Михайловна
8(8442) 59-57-66

Приложение №1
к письму ГУ МВД России
по Волгоградской области
от _____ №_____

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.

Чтобы не стать жертвой мошенников, а также не лишиться своих денежных средств, обратите внимание на основные способы и схемы совершения рассматриваемого вида преступлений. Обратите внимание, что мошенники модернизируют, усовершенствуют и видоизменяют данные способы, для того, чтоб ввести Вас в заблуждение и завладеть денежными средствами. Отнеситесь к приведенному материалу ниже с особым вниманием. Поделитесь информацией со своими близкими и родственниками. Не дайте себя обмануть.

Отличительной чертой совершения IT-преступлений является их совершение с использованием социальной инженерии, где работает человеческий фактор. Злоумышленник получает всю необходимую информацию от пользователя путем введения его в заблуждение.

Итак, наиболее распространёнными способами IT-преступлений являются следующие схемы:

1. Телефонное мошенничество под предлогом звонка сотрудника банка. Потерпевшему поступает звонок, где собеседник представляется сотрудником безопасности Банка, сообщает информацию о том, что якобы с банковской карты потерпевшего фиксировались попытки кражи денежных средств злоумышленниками, или же сообщает выдуманную операцию перевода денежных средств с банковской карты и называет вымышленные данные человека, в чей адрес якобы осуществлялся перевод. С целью предотвращения вымышленного перевода, потерпевшего вводят в заблуждение и ведут переговоры. В ходе разговора предупреждают о конфиденциальности и об уголовной ответственности за разглашение информации, полученной в процессе диалога с вымышленным сотрудником. Для введения в заблуждение и придания правдоподобности, мошенники могут высылать поддельные фотографии документов с удостоверениями, доверенностями и т.д., в подтверждение, что они действительно являются сотрудниками, например

Центрального банка Российской Федерации.[1] Цель мошенников – вывести денежные средства на «безопасные счета», открытые якобы в ЦБ РФ. В действительности же, денежные средства поступают на счета, подконтрольные мошенникам.

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

Важно: мошенники могут просить установить сторонние приложения для удаленного доступа через мобильный телефон (Any Desk и Rust Desk), убедить Вас отправиться в ближайший банкомат и перевести денежные средства со всех банковских карт на «безопасные счета». Угрозы, запугивание, осуществление морального давления – это неотъемлемые инструмента преступника.

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 попал в беду». На сотовый или стационарный телефон Вам поступает звонок от неизвестного абонента, который представляется 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, за которыми прибудет курьер. В процессе разговора для придания правдоподобности звонящий передает трубку якобы сотруднику полиции. Как и в прошлом виде преступления, потерпевший предупреждается о конфиденциальности разговора и предупреждается 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:

[1] Далее – «ЦБ РФ».

– 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. Телефонное мошенничество с использованием СМС-рассылок. На телефон потерпевшего поступают СМС–сообщения 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. При реагировании на данные сообщения, потерпевший перезванивает на телефонные номера, указанные в тексте сообщения, вступая в диалог с мошенниками. Полагая, что потерпевший ведет разговор с действительными сотрудниками сотовой связи или же банка, он выполняет все действия мошенников, направленные на вывод денежных средств на счета, им подконтрольные.

Важно: Вы должны понимать, что при получении подобных сообщений, не нужно перезванивать по указанным телефонным номерам. Необходимо сразу обращаться по телефону горячей линии для уточнения информации, или же игнорировать подобного характера сообщения.

4. Биржевое мошенничество. Данная противоправная схема используется для обмана неопытных пользователей, недавно решивших познать законы биржевого рынка и заработать легкие деньги. Роль мошенников выполняют работники трейдовой организации «однодневки». Различными доступными способами они набирают клиентов для обучения игре на биржевом рынке с гарантированной прибылью. Акцентируют внимание на короткое и легкое обучение с заработком с первого вложения, 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. Все риски для потерпевшего кроются в мелком шрифте в договоре, заключаемом между сторонами. Это длящийся вид мошенничества, на первых этапах потерпевший весьма воодушевлен рассказами о скорейшем обогащении, выполняет все указания работодателя. После прохождения обучения жертве предлагается попробовать выйти на биржевой рынок, вложить небольшую сумму денег, и продемонстрировать умения, полученные в ходе обучения. Однако, потерпевший не знает, что все действия на биржевом рынке он

производит на запрограммированной бот-версии, которая при любых ситуациях и условиях алгоритмами выведет прибыль. Воодушевляясь своими успехами, потерпевший соглашается вносить на биржу все большие суммы. Не редко встречаются случаи, когда жертва берет кредиты под залог имущества, а в последствие его лишается, так как все денежные средства, внесенные на биржу, переводятся мошенниками в офшоры или иные подконтрольные им счета.

Отличительной чертой такой трейдерской компанией является ее постоянный переезд в различные города. Отработав в одном регионе достаточное количество жертв, организация в один день переезжает в другой регион. Привлечение к уголовной ответственности работников таких организаций практически невозможно, ведь все риски потерпевший берет на себя, заключая договор.

Важно: при оформлении договора с брокерской компанией, все риски вы берете исключительно на себя.

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.

5. Мошенничество с использованием торговых интернет-площадок. В данной схеме мошенники могут выступать как в роли покупателя, так и в роли продавца. Главная задача кибермошенников – выуживание конфиденциальных данных: паролей, реквизитов карт, счетов для кражи денег дистанционным способом. Важно осуществлять какие-либо действия на данных площадках, учитывая простые правила из цифровой гигиены. Например, не переходить в сторонние мессенджеры для продолжения диалога, не передавать личную информацию, не производить предоплату, если не уверен в продавце, не переходить по подозрительным ссылкам, в следствие которого может произойти заражение вирусом мобильного устройства или персонального компьютера.

Внимание:

– 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 предоплаты 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. Мошенничество с использованием социальных сетей, мессенджеров. Зачастую, на личные страницы пользователей или в мессенджере по личному абонентскому номеру приходят сообщения от знакомых или родственников, с просьбой занять денежные средства под различными предлогами, или же с просьбой проголосовать в конкурсе за ребенка, с прикреплением фишинговой ссылки для голосования. Полагая, что потерпевший ведет диалог со своим знакомым или родственником, он выполняет все поступающие указания. В конечном итоге мошенники заполучают денежные средства, которые потерпевший сам же переводит на подконтрольные счета мошенникам.

Актуальной схемой мошенничества на сегодняшний день является ввод в заблуждение сотрудников администраций и комитетов области. Данная схема выглядит следующим образом. В мессенджере «Telegram» потерпевшему поступает сообщение якобы от руководителя государственного учреждения, в действительности фейкового аккаунта от его имени. Вступая в диалог, потерпевший подтверждает перед мошенниками свою заинтересованность, сотрудничество и готовность выполнить все указания. После чего, потерпевшему в мессенджере «Telegram» 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, потерпевший 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 переходите по подозрительным ссылкам, не вступайте в диалог с мошенниками. Позвоните своему знакомому, руководителю, от чьего имени вам поступило сообщение и сообщите ему об этом. В случае, если вы все-таки стали жертвой мошенников:

– незамедлительно заблокируйте Вашу карту;

– опротестуйте 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. Мошенничество под предлогом продления срока действия сим-карты или неправомерного доступа к порталу «Госуслуги». Вам поступает звонок якобы от мобильного оператора. Сообщают, что срок действия Вашей 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, Вы даете злоумышленникам доступ в личный кабинет портала «Госуслуг», где 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.

Важно: 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.

8. Мошенничество под предлогом установки программного обеспечения на Ваше мобильное устройство. Мошенники под видом работников банков звонят гражданам и убеждают установить специальные поддержки клиента, дополнительную защиту, антивирусные приложения и так далее. Согласившись, Вы переходите по присланным ссылкам, либо самостоятельно скачиваете указанное приложение, а после чего обнаруживаете списание с счетов своих сбережений.

Примером такой программы является приложение «RustDesk» - программа удаленного доступа и дистанционного управления смартфоном или компьютером. Скачивая данное приложение и называя код доступа для соединения устройств, Вы тем самым предоставляете полную возможность по дистанционному входу на ваше устройство, даете доступ на установленные в нем программы, в том числе в мобильное приложение своего банка.

Важно: Не верьте подобным звонкам, не переходите по неизвестным ссылкам, не устанавливайте неизвестные вам приложения. Устанавливая в

смартфоны по просьбе телефонных собеседников приложения, вы рискуете потерять деньги.