Внимание, мошенники!

Общие рекомендации МВД России 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.

Предупреждён – значит, вооружён!

Мошенничества с платежными картами

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

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 картоприемник 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.

Совершение покупок в сети Интернет

Какие существуют мошеннические схемы, связанные с привлечением средств граждан под предлогом инвестирования и покупки товаров в интернет – магазинах с предоплатой?

Уважаемые граждане, обращаем Ваше внимание, что на протяжении последних лет увеличилось количество противоправных действий мошеннического характера с использованием сети Интернет путем вовлечения в сомнительные схемы, такие как доверительное управление денежными средствами, участие, в так называемых «бинарных аукционах» и покупки товаров в интернет – магазинах с предоплатой.

Для осуществления своей преступной деятельности мошенники используют социальные сети, а также создают для этих целей интернет – магазины. Участие в подобных схемах подразумевает наличие всевозможных рисков и привлекает лиц имеющих намерения на противоправное завладение денежными средствами граждан.

В связи с этим обращаем внимание, что интернет – ресурсы могут быть зарегистрированы с помощью зарубежных сайтов предоставляющих услуги анонимизации, что не позволит в ряде случаев пользователю установить достоверные сведения о лицах, которым он доверил денежные средства.

Совет гражданам: совершать покупки только на проверенных сайтах, о существовании которых можно узнать от друзей и знакомых, найти отзывы в сети Интернет и т.п. Поисковые системы (типа Яндекса) публикуют рейтинги Интернет-магазинов, которые тоже являются показателем надежности торговой площадки. Не нужно ничего покупать в социальных сетях. Не доверяйте брокерам, которые получают от граждан денежные средства для игры на бирже без заключения письменных контрактов.

Почему опасно вносить предоплату при покупках товаров в сети Интернет?

Мошенники привлекают потенциальных жертв низкими ценами на товары известных брендов. Покупателей просят внести предоплату, как правило, перевести денежные средства на электронный кошелек. В течение нескольких дней магазин обещает скорую доставку товара, после чего бесследно исчезает.

Схожий способ мошенничества используется при продаже товаров или услуг на электронных досках объявлений, интернет-аукционах, форумах, сервисах бронирования недвижимости. Как и в случае с интернет-магазинами, мошенники привлекают своих жертв низкими ценами и требуют перечисления предоплаты на электронный кошелек или банковскую карту.

Как действуют мошеннические схемы при оформлении полиса ОСАГО через Интернет, либо при покупке авиабилетов онлайн?

Мошенники регистрируют доменное имя, содержащее в названии слово «osago» или напоминающее доменное имя одной из известных страховых компаний. На этом домене размещается фишинговый сайт, страницы которого практически полностью копируют оформление оригинального веб-ресурса, принадлежащего страховой компании. Для расчета стоимости страхования пользователю необходимо заполнить небольшую анкету - указать имя, дату рождения, номер водительского удостоверения, данные об автомобиле, номер телефона и электронную почту для связи. После введения данных покупателю предлагают оплатить электронный полис ОСАГО с помощью банковской карты: указать номер карты, дату окончания ее действия и CVC/CVV-код. Мошенники перенаправляют пользователя на поддельную страницу подтверждения оплаты, где просят ввести полученный от банка код подтверждения оплаты. В случае успеха злоумышленники обходят двухфакторную аутентификацию и получают деньги.

Аналогичную схему обмана можно встретить при покупке авиабилетов онлайн.

Выигрыш в лотерею

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей. На мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Ключевые слова: **«Вы победили! Заберите приз! Оплатите лишь налог 13%. Сообщите реквизиты и код карты».**

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения; грамотно убеждает в честности акции. Объясняет, что для получения приза необходимо предоставить реквизиты карты и заплатить налог на доходы физических лиц, выплатить таможенные пошлины или транспортные расходы.

Мошенничества под предлогом благотворительности

Мошенники размещают в социальных сетях или на форумах подложные объявления о сборе средств тяжелобольным детям или бездомным животным или делают репосты реальных объявлений, но с подложными банковскими реквизитами.

Мошенничества, направленные на заражение устройства пользователя вредоносной программой

Мошенники, используя электронные адреса, схожие с адресами легальных организаций, рассылают от их имени сообщения, содержащие ссылку на скачивание открытки, музыки, картинки, архива или программы. Запуск вложения или переход по ссылке может инициализировать установку на устройство вредоносносной программы (вымогателя-блокиратора, шифровальщика, троянской программы) или же оформление подписки на платную услугу.

Пример хищений денежных средств со счетов с использованием вредоносных программ:

В сматрфон или компьютер жертвы тайно устанавливаются вредоносное ПО. Вредоносная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в СМС или ММС сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты. Одним из признаков наличия вредоносных программы на мобильном телефоне является направление «пустых» СМС или ММС сообщений на телефоны, имеющихся в контактах устройства. При открытии адресатом такого СМС или ММС сообщения, происходит дальнейшее заражение вирусом телефонов, получившее данное сообщение. Это могут быть троянские программы, которые не размножаются и не рассылаются сами, они ничего не уничтожают. Задача троянской программы - обеспечить злоумышленнику доступ к устройству жертвы и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений.

Если к смартфону подключена услуга «Мобильный банк», то сведения о доступе в Личный кабинет становятся известны преступнику. Тайно входя в чужие Личные кабинеты он может перечислять денежные средства сотен потерпевших на свои счета, а затем обналичивать.

Тактика борьбы достаточно проста:

Не допускать, чтобы вредоносные программы попадали на компьютер или смартфон (чаще всего страдают владельцы смартфонов с ОС Андроид). Если они все-таки попали, ни в коем случае не запускать их. Принять меры, чтобы, по возможности, они не причинили ущерба. Использовать специальные антивирусные программы. Отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ. **Если деньги все-таки списались,** разработан алгоритм действий потерпевшего: Немедленно прекратить любые действия с сотовым телефоном, принудительно отключить его, извлечь СИМ карту. Обеспечить сохранность (целостность) сотового телефона, как возможного средства совершения преступления. Не предпринимать никаких действий для самостоятельного или с привлечением посторонних ИТ-специалистов поиска и удаления вирусов, восстановления работоспособности сотового телефона, не отправлять сотовый телефон в сервисные службы ИТ для восстановления работоспособности.

Незамедлительно обратиться в свой банк по телефону горячей линии с поручением о блокировки операции с расчетным счетом и отзывом криминального перевода.

Незамедлительно обратиться в свой банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк» (приложение 2). Заявление может быть направлено в банк по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк в течение одного дня. Оформляется в 2-х экземплярах.

Согласно полученной в банке детализации с расчетного счета обратиться в банк получателя (используемого преступником) по телефону с заявлением о приостановке исполнения платежа и возврате средств.

В течение одного дня обратиться с заявлением в правоохранительные органы о факте хищения денежных средств. Для полиции понадобиться документальное подтверждение хищения денежных средств, в том числе выписка по банковскому счету, справка из банка, иные документы, подтверждающие списание заявленной суммы ущерба. Существует возможность получение этих данных из «личного кабинета» пользователя услуг сотовой связи, банк-онлайн с письменного согласия потерпевшего. Эта информация может быть зафиксирована протоколом осмотра места происшествия.

Оперативно обратится в банк с заполненной справкой по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания (приложение 3), которое оформляется в 2-х экземплярах.

Справочно: *ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе» предусматривает процедуру обращения в банк после незаконной транзакции и дает право на возмещение незаконно списанных денежных средств со счета. Так, п. 11 ст. 9 гласит «В случаи утраты электронного средства платежа и (или) его использования без согласия клиента, клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно, после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции».*

В п. 15 ст. 9 указано «В случае, если оператор по переводу денежных средств исполняет обязанность по уведомлению клиента - физического лица о совершенной операции в соответствии с частью 4 настоящей статьи и клиент - физическое лицо направил оператору по переводу денежных средств уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных средств должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления. В указанном случае оператор по переводу денежных средств обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента - физического лица».

Телефонное мошенничество

Телефонное мошенничество получило развитие с начала 2000-х годов, когда сотовый телефон стал массовым и доступным.

В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом. Чаще всего в сети телефонных мошенников попадаются пожилые или доверчивые

люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Обман по телефону: родственник попал в беду, требование выкупа.

Звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство. Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку. Цена вопроса от тысячи рублей до 30 тыс. долларов США.

В организации обмана по телефону с требованием выкупа могут участвовать несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.

После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

Рекомендации гражданам:

Первое и самое **главное правило – прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён – связаться с его коллегами, друзьями и родственниками для уточнения информации.** Следует задать уточняющие вопросы, ответы на которые посторонним не известны. Спросить, из какого отделения полиции звонящий. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда. Требование взятки является преступлением.

Телефонный номер-грабитель

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того, как потерпевший перезванивает, долго держат на линии. В результате оказывается, что со счёта списаны крупные суммы. Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

Совет гражданам: не звонить по незнакомым номерам.

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: ***«Вам пришло MMS-сообщение. Для получения пройдите по ссылке...»***. **При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.**
Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер.... для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Существует множество вариантов таких мошенничеств. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.

Совет гражданам: не следует звонить по номеру, с которого отправлен SMS.

Простой код от оператора связи

Потерпевшему поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки оператора мобильной связи. Обоснования этого звонка или SMS могут быть: предложение подключить новую эксклюзивную услугу; для перерегистрации во избежание отключения связи из-за технического сбоя; для улучшения качества связи; для защиты от СПАМ-рассылки; предложение принять участие в акции от вашего сотового оператора. Предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п. на самом деле код, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только его наберёт потерпевший, злоумышленник получает доступ к счёту.

Для граждан: любая упрощённая процедура изменения тарифных планов должна вызывать подозрение, необходимо перезванивать своему мобильному оператору по телефону горячей линии для уточнения условий или открыть соответствующие разделены на официальном сайте оператора (в мобильном приложении).

SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт. Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие. **Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.**

Памятка о возможных видах и способах мошенничества и порядке обеспечения личной финансовой безопасности (для участников СВО)

В повседневную жизнь все больше внедряются разнообразные цифровые технологии в качестве платежных систем: пластиковые карты, смартфоны

и компьютеры. Одновременно с развитием таких устройств и сервисов появляются виды мошенничеств, позволяющие присвоить денежные средства граждан, в том числе участников СВО и их родственников. Чтобы не стать жертвой, необходимо соблюдать правила безопасного пользования цифровыми устройствами, содержащими личные данные, а также данные о банковских картах, счетах. Проанализировав типичные случаи мошенничества в отношении участников СВО и их родственников, специалисты МВД России подготовили для вас памятку. Предлагаем внимательно ознакомиться с ее содержанием и придерживаться изложенных рекомендаций. Это поможет вам сберечь денежные средства от возможных хищений.

Способы мошенничества:

1. SMS с просьбой о помощи участникам СВО
2. Сообщение в социальных сетях о помощи в поиске военнопленных, пропавших без вести.
3. Сообщение об оформлении кредита
4. Предложение скачать на мобильный телефон (используемый для покупок или оплаты) программу для удаленного доступа банка к гаджету
5. Телефонный звонок покупателя
6. SMS или звонок из банка о блокировке карты
7. Происшествие с родственником
8. Ошибочный перевод средств
9. Компенсация за лекарственные препараты
10. Сообщение от неизвестного абонента.

ЕЩЕ РАЗ НАПОМИНАЕМ!

Если звонят подозрительные лица, то немедленно прервите разговор! При длительном разговоре мошенники внушат необходимость исполнить их требования! Для этого разговор будет вестись в темпе «давления» (чтобы Вы не могли прервать разговор), Вас будут запугивать негативными последствиями (денежные средства нужно немедленно обезопасить от похищения), требовать немедленных действий без предоставления возможности обдумать их результаты.

Никогда и никому не сообщайте пароли и секретные коды, которые приходят вам в сообщении от банка. Только мошенники спрашивают эти пароли и коды. Помните: хранение реквизитов и ПИН-кода в тайне — это Ваша ответственность и обязанность! Никто, ни банк, ни правоохранительные органы, не вправе требовать ваш ПИН-код и пароль!

Оперативно-розыскные действия, следственные мероприятия по телефону не проводятся! Службы безопасности банков и сотрудники правоохранительных органов никогда не звонят гражданам с сообщениями о необходимости взять кредит и перевести деньги на «безопасный» или «резервный» счет! Никогда не совершайте никаких переводов и не передавайте деньги третьим лицам.

Не перезванивайте по телефонам и не переходите по подозрительным ссылкам, которые указаны в СМС сообщениях, сообщениях из социальных сетей и электронной почты! Не открывайте сообщения с незнакомых адресатов! Там могут содержаться шпионские программы, помогающие похитить ваши банковские данные! Они дают доступ к управлению телефоном и беспрепятственному управлению банковскими счетами! Мошенники могут перевести ваши деньги в другой банк, а доказать это будет невозможно, т.к. с банком взаимодействовал Ваш телефон.

Оказывайте помощь или ведите поиск участников СВО через Министерство обороны Российской Федерации, публичные органы власти или организации, которые этим официально занимаются.

При получении фото- и видеоматериалов с изображением участников СВО или их родственников не предпринимайте поспешных действий, они могут быть сгенерированы программным обеспечением. Постарайтесь связаться с ними или выяснить судьбу через Министерство обороны Российской Федерации.