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.

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 средствсо 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».

Совершение покупок в сети Интернет

Что делать, если при совершении сделок купли-продажи товаров через Интернет после их оплаты ни товаров, ни денег обратно получить не удается?

В случае, если вы стали жертвой интернет-мошенников, необходимо обращаться в правоохранительные органы по месту жительства для проведения необходимых проверок и возбуждения уголовного дела.

Если вы все-таки решили приобрести товары в сети Интернет, не стоит торопиться предпринимать действия, навязываемые неизвестными продавцами, тем более, если они требуют перевода денежных средств каким-либо способом. Через Интернет вам могут предложить приобрести все что угодно, а распознать подделку при покупке через всемирную компьютерную сеть бывает сложно. Однако, соблюдая некоторые правила предосторожности, можно оградить себя от возможных неприятностей.

Прежде чем что-либо приобрести на неизвестном вам сайте, проверяйте полную информацию о нем, поищите отзывы, почитайте форумы. Наведите справки о продавце, изучите отзывы о его работе и только после этого принимайте решение.

Вас должна насторожить слишком низкая цена на товар, а также отсутствие фактического адреса или телефона продавца. В этом случае, скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Сегодня мошенничество в Интернете развито очень хорошо. Постоянно появляются новые способы обмана людей. В этой связи необходимо быть бдительными и осторожными.

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.

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.

ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) В БАНК ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И ОТКЛЮЧЕНИИ СИСТЕМЫ МОБИЛЬНЫЙ БАНК

Экз №

_____
должность руководителя

_____
наименование банка

_____

Фамилия И.О.

Уважаемый (ая) _____
имя, отчество руководителя

«___» _____ 201__ года с моего расчетного счета, открытого в Вашем банке, по системе «Мобильный банк» были похищены денежные средства, которые, по имеющейся информации переведены по следующими реквизитам (абонентским номерам):

Указываются абонентские номера, полученные из детализации банка, либо иные реквизиты по ниже приведенному образцу:

Дата платежа: _____

Наименование банка потерпевшего: _____

ИНН потерпевшего: _____

Номер счета потерпевшего: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____

Прошу Вас заблокировать мой расчетный счет, оказать содействие в возврате денежных средств, отключить услугу «Мобильный банк».

Заявитель: _____/_____/

Дата: _____**/Телефон:** _____

ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Экз. №

«___» _____ 201__ года с моего расчетного счета, открытого в Вашем банке, по системе «Мобильный банк» были похищены денежные средства, которые, по имеющейся информации переведены по следующими реквизитам (абонентским номерам):

Указываются абонентские номера, полученные из детализации банка, либо иные реквизиты по ниже приведенному образцу:

Дата платежа: _____

Наименование банка потерпевшего: _____

ИНН потерпевшего: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____

Иная информация, имеющая отношение к инциденту: _____
_____
_____

☐ Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

Заявление в правоохранительные органы принято в ТОВД _____
_____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

и зарегистрировано за № _____ в КУСП

☐ Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству предупрежден.

Заявитель: _____/_____/

Дата: _____**/Телефон:**

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.

Пришло СМС от банка о блокировке карты или звонят из банка и спрашивают номер карты, пароль и код доступа. Что делать?

Этот способ мошенничества является наиболее новым. Злоумышленники оформляют облачную АТС на одноразовую сим-карту, а затем через веб-интерфейс меняют телефонный номер своей станции на телефонный номер банка. Представляясь сотрудниками банка, преступники обзванивают клиентов и под различными предлогами выясняют у них номера карт, одноразовые пароли и коды доступа, необходимые для проведения операций по банковским картам. Также с номера-двойника банка мошенники массово рассылают клиентам банка смс-сообщения о блокировке карты. Для разблокировки им предлагают перевести деньги на счет или отправить смс-сообщение на короткий номер.

ПРИМЕР: Сообщение «Ваша банковская карта заблокирована». Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда жертва звонит по указанному телефону, ей сообщают, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. На самом деле злоумышленникам нужен номер карты жертвы и ПИН-код. Как только потерпевший их сообщает, преступники получают возможность управлять счетом.

Для граждан: не сообщать реквизиты карты никому. Представители банка их знают! Ни одна организация, включая банк, не вправе требовать ПИН-код! Для

того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

Фишинг и поддельные ("зеркальные") сайты

Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к аккаунтам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Для кражи персональных данных фишеры массово рассылают электронные письма от имени государственных органов или известных компаний, например, крупных банков или онлайн-магазинов. Их цель - заставить получателей перейти по указанной в письме ссылке на поддельный сайт компании, интерфейс которого внешне не отличим от настоящего сайта, и ввести свои личные данные. Для привлечения внимания к письму в теме указывается на перспективу большой выгоды или на проблему, требующую срочного разрешения.

Подставные страницы действуют недолго - как правило, не более одной недели, ввиду частого обновления базы антифишинговых программ и фильтров. Однако мошенники, следуя отлаженной схеме, создают всё новые и новые сайты-фальшивки для сбора персональных данных.

Так, спамеры активно рассылали по всему миру фальшивые уведомления о выигрыше в лотереях, приуроченных к Чемпионату Европы по футболу, Олимпиаде в Бразилии и Чемпионатам мира по футболу в 2018 и 2022 годах. Для получения денег получателю письма предлагалось ввести на сайте несуществующей лотереи персональную информацию.

Данный способ возможен, когда потерпевший пользуется **«личным кабинетом»** на сайте банка. Преступниками создается сайт, адрес которого и внешнее оформление страниц трудноотличимы от официального сайта банка. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто в поисковой системе набирает название банка, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен выход на «зеркальный сайт», то вводимыми данными для входа в личный кабинет банка (логин и пароль), могут воспользоваться злоумышленники и войти на настоящем сайте от имени потерпевшего в его личный кабинет. Далее возможен перевод денег со счета потерпевшего из личного кабинета или подключение к его счету услуги «мобильный банк» на любом абонентском номере.

Примеры:

Оформление полиса ОСАГО

- 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.**

- Жители России получали письма, замаскированные под уведомления от Федеральной налоговой службы и Пенсионного фонда РФ, примерно следующего содержания: «Уважаемый налогоплательщик! У вас выявлена задолженность. Срок погашения долга до 23.12.2016 г. Подробнее Вы можете ознакомиться, перейдя по ссылке… » или «Осуществлен перерасчет пенсионных накоплений. Обязательно ознакомьтесь по ссылке…». После перехода на поддельный сайт государственного органа для получения более подробной информации пользователю предлагалось ввести свои персональные данные.

ВНИМАНИЕ: Основным признаком, что клиент зашел на «зеркальный» сайт банка является то, что **после ввода логина и пароля на странице появляется надпись о техническом обслуживании сайта или любая информация, в которой будет указано о том, что обратится на сайт можно позднее**. При этом на телефон не поступает СМС-сообщение от банка о входе в личный кабинет, если такая форма оповещения предусмотрена.
Совет гражданам: при наступлении вышеописанных событий незамедлительно обратиться в банк по телефону горячей линии и заблокировать счет. Разблокировать его со сменой пароля можно при личном обращении в отделение банка с паспортом и картой.

Что такое "скимминг" (вид мошенничества с платежными картами)?

Считывание данных карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру.

Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты.

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.