**ПАМЯТКА**

**по профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий**

К наиболее распространенным видам дистанционных мошенничеств, совершенных на территории г. Санкт-Петербурга и Ленинградской области, относятся:

- «фишинг» – вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

- «фарминг» - процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг;

- «двойная транзакция» (при оплате товаров и услуг продавец сообщает об ошибке, предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций)

- «траппинг» (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).

I. Основные схемы телефонного мошенничества:

1. Обман по телефону.

Мошенник звонит с незнакомого номера и представляется родственником (знакомым) и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвиняется 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 правоохранительных органов, который уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перевести на определенный расчетный счет или передать какому-либо человеку. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам, но нередко человек, которому звонит мошенник, сам случайно подсказывает имя того, кому нужна помощь.

Аналогичным образом могут звонить мошенники сотрудникам государственных органов либо предпринимателям и, представляясь, например, руководителем какого-либо государственного органа (правоохранительного, надзорного, контролирующего), под предлогом приезда комиссии проверяющих требуют организовать либо «теплый прием» в форме бесплатного предоставления услуг (питание, подарки, организация отдыха и т.д.), либо перечислить определенную сумму денежных средств на указанный расчетный счет для организации досуга проверяющих или достижения необходимых положительных результатов проверки.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, нужно связаться с его коллегами, друзьями и родственниками для уточнения информации. Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он правоохранительного органа (другого ведомства). После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

Само требование взятки должностным лицом является преступлением.

2. SMS-просьба о помощи.

SMS-сообщения позволяют упростить схему обмана по телефону. 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.

***На SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.***

3. Телефонный номер-грабитель.

На телефон 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 Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счета списаны крупные суммы. Существуют сервисы с платным звонком, как правило 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.

***Единственный способ обезопасить себя от телефонных мошенников - не звонить по незнакомым номерам.***

4.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. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона.

***Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.***

5. Выигрыш в лотерее или какого-либо приза.

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 Ваш мобильный телефон – как правило, в ночное время – приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего упоминаются известные иностранные модели и марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации». Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

7. Простой код от оператора связи.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Перезвонить своему мобильному оператору для уточнения условий, а также узнать какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

9. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

**МОШЕННИЧЕСТВА С БАНКОВСКИМИ 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.

1. Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

Злоумышленникам нужен лишь номер Вашей карты и ПИН-код, как только Вы их сообщите, деньги будут сняты с Вашего счета.

***Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.***

1. Если Вы утратили карту немедленно ее блокируйте.
2. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.
3. Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.
4. Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.
5. В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.
6. Хищения с карт, подключенных к опции бесконтактных платежей. Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Как обезопасить себя от мошенников:

1. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
2. Не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
3. Используйте пароли не связанные с Вашими персональными данными.
4. Не сообщать данные карты, пароли и другую персональную информацию.
5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.
6. По всем возникающим вопросам обращаться в банк, выдавший карту.
7. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.
8. Не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.
9. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки).
10. Не перезванивать по номерам, которые приходят на e-mail или по SMS.

Будьте бдительны!

**ПАМЯТКА**

**«Телефонные мошенничества»**

Основные способы дистанционных хищений денежных средств, при которых мошенники вводят граждан в заблуждение посредством телефонных звонков:

**Вариант № 1** (звонок сотрудника банка), когда неизвестный представляется сотрудником службы безопасности какого-либо банка и сообщает, что с Вашего банковского счета происходят операции по несанкционированному списанию денежных средств, и в целях безопасности счета предлагает перевести сбережения на «резервный» или «безопасный» счет. Распространены случае сообщения информации об оформлении на Вас кредита и необходимости пройти в приложении онлайн-Банка по определённой ссылке для его аннулирования (выполнить иные инструкции).

**Вариант № 2** (звонок сотрудника правоохранительных органов), когда неизвестный представляется сотрудником полиции, следователем и т.д. и сообщает, что проводится спецоперация по поимке мошенников и для этого необходимо перевести деньги на «специальный» счет. При этом требует не звонить в банк, так как сотрудники банка заодно с мошенниками.

**Вариант № 3**, когда неизвестный сообщает, что Ваш родственник, либо близкий человек попал в беду (например, машиной сбил человека или обвиняется в совершении преступления), и задержан сотрудниками полиции, и что для освобождения необходимо перевести на счет денежные средства либо для примирения с пострадавшим либо в качестве взятки сотрудникам полиции. Возможны варианты, при которых в разговоре может принять участие якобы сотрудник полиции, который будет подтверждать сказанное.

**!!!ВАЖНО ЗНАТЬ!!!** – это звонят **мошенники** (не обращайте внимание на то, что определившийся на Вашем телефоне номер может соответствовать номеру телефона Вашего банка или правоохранительных органов, зачастую – Московского региона (499, 495… и т.д.), так как при помощи специальных устройств мошенники меняют номера на абсолютно любой номер – так называемые подменные номера), сотрудники банков **никогда** не звонят своим клиентам, и тем более, **никогда** не требуют переводить с личного счета деньги. Представители правоохранительных органов могут звонить **только** для вызова в помещения правоохранительных органов с целью получения объяснений, истребования документов по находящимся в производстве уголовным делам и материалам проверок.

**ПРАВИЛО**: **незамедлительно прервать разговор, ни в коем случае не сообщать свои персональные данные (**ФИО, в каких банках у Вас или у Ваших близких открыты счета**), реквизиты счетов, пин-коды банковских карт, ни при каких условиях не выполнять инструкции звонившего; перезвонить родственнику, от лица которого поступил звонок и перепроверить информацию (**будьте уверены, что она не подтвердится**).**

**И помните, мошенники отличные психологи, они прекрасно юридически и технически подготовлены, всегда очень убедительны, дружелюбны и**

**с первых секунд разговора с легкостью могут в него увлечь.**

**НЕ ДАВАЙТЕ МОШЕННИКАМ ЭТОЙ ВОЗМОЖНОСТИ !!!**

**НИ В КОЕМ СЛУЧАЕ НЕ ВСТУПАЙТЕ С**

**МОШЕННИКАМИ В РАЗГОВОР!!!**

Прежде чем принять любые решения посоветуйтесь с родными и друзьями, проверьте информацию и не предпринимайте действий в первые сутки, обдумайте последствия и все варианты развития событий. Основное требование мошенников – немедленные требования, немедленные действия.

**Профилактика детского дорожного травматизма**

**Уважаемые родители**, не напрасно говорят, что взрослые в ответе за всё, что делают дети, это касается и поведения детей на улицах!

Важнейшее место в работе по профилактике детского дорожно-транспортного травматизма занимают родители. В семье формируется у ребенка сознательное отношение ко всему, что его окружает.

Систематическая повседневная тренировка движений, наблюдения, с постоянным личным примером родителей может создать у ребенка важные навыки наблюдения, спокойствия и отсутствия спешки при переходе улицы, внимательности.

Для того, чтобы обучение детей основам безопасности движения было эффективным, обязательно необходимо соблюдение следующих принципов: систематичности, последовательности и наглядности.

**Помогите вашим детям сохранить жизнь и здоровье на дороге!**

Расскажите детям следующие правила дорожного движения:

-  переходить улицу только на зеленый свет светофора,

-  не играть на дороге или около проезжей части,

- переходить улицу только по пешеходному переходу,

- при переходе улицы сначала посмотреть налево, а дойдя до середины – направо,

- знать устройство проезжей части,

- знать некоторые дорожные знаки для пешеходов и водителей,

- знать правила поведения в транспорте,

- знать и соблюдать правила поведения во дворе.

Для того, чтобы ребенка легче было увидеть на улице, одевайте его в одежду неоновых цветов с отражающими полосками или специальными отражателями.

Родители, помните следующие простые и важные правила для профилактики детского дорожного травматизма:

- Выходите из дома заблаговременно, чтобы ребёнок привык ходить по дороге, не спеша!

- Не рекомендуется ускорять шаг или бежать вместе с ребёнком на остановку транспорта. Приучите ребенка, что это опасно, лучше подождать следующего автобуса!

- При переходе проезжей части, не говорите с ребёнком, чтобы он привык, что при переходе нужно не разговаривать, внимательно, не отвлекаясь наблюдать за дорогой, движением транспорта.

- Следите за тем, чтобы переходить проезжую часть не наискосок, а прямо, строго перпендикулярно, для лучшего наблюдения за движением транспорта.

- На остановках транспорта держите ребёнка крепко за руку.

- Переходите проезжую часть только на пешеходных переходах и только на зелёный сигнал светофора!

Объясните ребёнку, что переходить дорогу на зелёный мигающий сигнал уже нельзя!

**Профилактика терроризма и экстремизма - полезные телефоны по вопросам борьбы с терроризмом. Общие рекомендации.**

Уважаемые жители, эту информацию необходимо знать всем, для того, чтобы защитить себя, уберечь свое здоровье и жизнь, жизнь родных, близких и друзей в случае возникновения чрезвычайной ситуации.

Любой человек должен точно представлять свое поведение и действия в экстремальных ситуациях и быть готовым к самозащите. Обращайте внимание на подозрительных людей, предметы, на любые подозрительные мелочи. Никогда не принимайте от незнакомцев пакеты и сумки, не оставляйте багаж без присмотра.

Не будьте равнодушными, ваши своевременные действия могут помочь предотвратить террористический акт и сохранить жизни окружающих!

Единый телефон службы спасения: 01

При звонке с мобильного телефона – 112

ГУ МВД России по Санкт-Петербургу и Ленинградской области – 02

ОМВД России по Пушкинскому району Санкт-Петербурга:

- 470-02-02;

- 573-18-90.

Дежурная служба УФСБ по Санкт-Петербургу и Ленинградской области

– 438-71-10.

Общие рекомендации

В последнее время часто отмечаются случаи обнаружения гражданами подозрительных предметов, которые могут оказаться взрывными устройствами. Подобные предметы обнаруживают в транспорте, на лестничных площадках, около дверей квартир, в учреждениях и общественных местах.

Как вести себя при обнаружении? Какие действия предпринять?

Если обнаруженный предмет не должен, по вашему мнению, находиться в этом месте, не оставляйте этот факт без внимания. Если вы обнаружили забытую или бесхозную вещь в общественном транспорте,

спросите людей, находящихся рядом. Если хозяин вещи не установлен, немедленно сообщите о находке водителю (машинисту).

Если вы обнаружили неизвестный предмет в подъезде своего дома, опросите соседей, и, если владелец не установлен, немедленно сообщите о находке в отделение полиции.

Если вы обнаружили неизвестный предмет в учреждении, немедленно сообщите о находке администрации или охране.

Во всех перечисленных случаях: не трогайте, не передвигайте, не вскрывайте обнаруженный предмет, зафиксируйте время обнаружения предмета.

Помните: внешний вид предмета может скрывать его настоящее назначение. В качестве камуфляжа для взрывных устройств используются самые обычные бытовые предметы: сумки, пакеты, коробки, игрушки, сигаретные пачки, мобильные телефоны.

Помните, любой предмет, найденный на улице или в подъезде, может представлять опасность!

Избегайте больших скоплений людей. Не присоединяйтесь к толпе, как бы ни хотелось посмотреть. Если оказались в толпе, позвольте ей нести вас, но попытайтесь выбраться из нее. Любыми способами старайтесь удержаться на ногах. Двигаясь, поднимайте ноги гораздо выше. Если упали, постарайтесь как можно быстрее подняться на ноги. Старайтесь сохранять спокойствие!

**Угон или кража?**

Присвоение чужого имущества это одно из самых распространенных преступлений в современном обществе.

Сегодня мы обратимся к квалификации преступлений, связанных с присвоением автотранспортного средства.

Угон автомобиля и кража автотранспортного средства при внешней идентичности, все же имеют ряд характерных отличий.

Преступники, достаточно часто завладевают транспортными средствами, преследуя при этом разные цели: от желания просто покататься на автомобиле и до желания продать этот автомобиль.

Такие действия могут быть квалифицированы либо как кража, либо как угон транспортного средства.

Итак, что же объединяет эти преступления, предусмотренные ст. 158 УК РФ (кража) и ст. 166 УК РФ (угон)?

Данные преступления – это преступления против собственности, то есть как при хищении чужого транспортного средства (краже), так и неправомерным завладением транспортного средства без цели хищения (угоне) нарушается право собственности.

В обоих случаях, лицо привлекаемое к ответственности на момент совершения преступления достигло 14 –летнего возраста.

Тем не менее данные составы имеют существенные различия.

Итак, из определения кражи (ст. 158 УК РФ) следует, что это тайное хищение чужого имущества, то есть кража включает в себя либо изъятие автомобиля, либо его обращение в свою пользу или в пользу третьих лиц. При этом необходимо, чтобы лицо действовало тайно, так как это отличающий признак кражи. При краже автомобиля необходимо наличие корыстной цели, которая является неотъемлемой составляющей тайного хищения.

Под угоном (ст. 166 УК РФ) понимается неправомерное завладение транспортным средством без цели его хищения.

Угон – это такое завладение, которое не предполагает присвоение автомобиля. Иными словами угон характеризуется тем, что лицо пользуется транспортным средством временно, а затем либо возвращает его на то же самое место, либо оставляет его в другом месте.

В завершении можно сделать вывод, о том, что важно различать виды преступлений, предусмотренные Уголовным Кодексом Российской Федерации в отношении пропажи автомобиля. Во избежание потери автомобиля следует внимательно отнестись к противоугонным системам и страхованию своего имущества.

Прокуратура Пушкинского района