МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный геологоразведочный университет имени Серго Орджоникидзе»
(МГРИ)

ПАМЯТКА

рекомендации по защите от действий мошенников с использованием высокотехнологичных устройств

Телефонное мошенничество

1. Обман по телефону.

Как организованно:

Вам 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 составляет от одной до тридцати тысяч долларов США.

Как поступать в ситуации:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму – это мошенник. 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 отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

2. SMS-просьба о помощи.

Как организованно:

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.

Как поступать в ситуации:

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

Телефонный номер-грабитель. Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

Как организованно:

Вам 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 счёта списаны крупные суммы.

Как поступать в ситуации:

Не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

3. Телефонные вирусы.

Как организованно:

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.

Как организованно:

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 счёт они снимаются с телефона.

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

4. Выигрыш в лотерее.
Как организованно:

На Ваш 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.

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры:
- просит представиться и назвать год рождения;
- грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.); спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);
- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер, куда надо перезвонить;
- поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа купить экспресс-карту, то все равно должен позвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора – сообщить свои коды. Якобы оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего присваивает ему персональный номер, с которым «победитель» должен ехать за призом.

Но если Вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании, то это объявят нарушением правил рекламой акции.

Как организованно:

Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счет карточкой экспресс-оплаты. Но прежде чем совершить оплату, Вы должны будете сообщить оператору личный ПИН-код, перезвонив на определенный номер.

Как поступать в ситуации:

Активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на карточке, а личный код никому никогда не сообщается.

Если Вам поступило предложение от радиостанции активировать карточки эксперес-оплаты – не верьте. Радиостанции никогда не требуют активировать карточки экспресс-оплаты при проведении лотереи.

«Вы выиграли машину, нужны деньги для её оформления»

Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

Как организованно:

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 это Audi A6, но упоминаются и другие 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 телефона, к примеру, 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».

Как поступать в ситуации:

Если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

5. Простой код от оператора связи

Как организованно:

Вам поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными:

- 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.

Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

Как поступать в ситуации:

Любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать своему мобильному оператору для уточнения условий.

SMS-сообщения могут быть самыми разными. Советуем Вам критически относиться к таким сообщениям и не спешить выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, 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.

6. Штрафные санкции и угроза отключения номера

Как организованно:

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что произошло нарушение условий договора:

- абонент сменил тарифный план, не оповестив оператора;
- не внес своевременно оплату;
- воспользовался услугами роуминга без предупреждения и так далее.

Чтобы предотвратить отключение номера, Вам предлагается:

- купить карты экспресс-оплаты и сообщить их коды;
- перевести на свой номер сумму штрафа и набрать код;
- перевести средства на указанный номер.

После этого Вы якобы сможете доказать свою невиновность и при этом сохраните свой номер.

Как поступать в ситуации:

Перезвонить своему мобильному оператору для уточнения условий.

Помните, что у Вас, как у потребителя услуг связи, есть права, которые защищаются законом. Никакой оператор связи не может требовать выплачивать ему штрафы до тех пор, пока Ваша вина не будет доказана.

7. Ошибочный перевод средств

Как организованно:

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок, и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

Как поступать в ситуации:

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

8. Доступ к SMS и звонкам

Как организованно:

В Интернете или прессе публикуется объявление, в котором Вам предлагается изучить содержание SMS-сообщений и список входящих и исходящих звонков интересующего Вас абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента.

Как поступать в ситуации:

Управление «К» МВД России предупреждает: предложение о предоставлении данной услуги является мошенничеством, так как такая услуга может оказываться исключительно операторами сотовой связи и в установленном законом порядке!

Мошенничество с банковскими картами

1. Владельцам пластиковых банковских карт

Как организованно:

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.

Как поступать в ситуации:

Не торопитесь сообщать реквизиты вашей карты! 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.

ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ.

Никогда и никому не сообщайте ПИН-код Вашей карты.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД.

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить

реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте.

Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

В торговых точках, ресторанах и кафе, развлекательных учреждениях все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Правила поведения в интернете

1. Виды вредоносных программ

Вредоносные программы – любое программное обеспечение, которое предназначено для скрытного (не санкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом *«вирусы»*.

Вредоносные программы можно разделить на три группы:

- компьютерные вирусы;
- сетевые черви;
- троянские программы.

Компьютерные вирусы – это программы, которые умеют размножаться и внедрять свои копии в другие программы, т. е. заражать уже существующие файлы. Обычно это исполняемые файлы (*.exe, *.com) или файлы, содержащие макропроцедуры (*.doc, *.xls), которые в результате заражения становятся вредоносными.

Сетевые черви – это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальным сетям и Интернету (например, через электронную почту). Особенность червей – чрезвычайно быстрое «размножение». Червь без Вашего ведома может, например, отправить «червивые» сообщения всем респондентам, адреса которых имеются в адресной книге Вашей почтовой программы. Помимо загрузки сети в результате лавинообразного распространения, сетевые черви способны выполнять опасные действия.

Задача троянской программы – обеспечить злоумышленнику доступ к Вашему компьютеру и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Просто однажды Ваша частная переписка может быть опубликована в Интернете, важная информация продана конкурентам, а баланс лицевого счета у интернет-провайдера или в электронных платежных системах неожиданно окажется нулевым или отрицательным.

2. Безопасное использование электронной почты

Являясь удобным видом связи, как личной, так и деловой, электронная почта остаётся одним из самых популярных способов распространения вредоносных программ в Интернете.

Обычное сообщение электронной почты – это просто текст, сам по себе он не может быть опасен. Но к сообщению можно прикрепить файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

Тактика борьбы с вредоносными программами:

Вредоносные программы срабатывают при запуске на Вашем компьютере. Тактика борьбы с ними достаточно проста:

- не допускать, чтобы вредоносные программы попадали на Ваш компьютер;
- если они к Вам все-таки попали, ни в коем случае не запускать их;
- если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

Как запретить выполнение вредоносных программ:

Чтобы запустить файл вложения на выполнение, следует открыть сообщение в отдельном окне, дважды щелкнув по строке сообщения в списке (сообщение с вложением помечено скрепкой) и открыть файл-вложение, дважды щелкнув по имени файла в заголовке сообщения (поле «Присоединить»).

Учитывая сказанное, необходимо взять за правило:

- не открывать сообщение (дважды щелкнув мышкой), особенно если оно пришло от неизвестного отправителя. Текст можно прочитать в режиме быстрого просмотра: когда при одиночном щелчке мышкой на сообщении в списке текст сообщения отображается не в отдельном, а в основном окне программы.
- немедленно удалять все подозрительные сообщения. Никогда не открывайте сразу присланные файлы-вложения. Принимайте во внимание, что сообщения от якобы знакомых лиц могут оказаться рассылками, отправленными сетевыми червями. Также имейте в виду, что без вашего ведома ни одна уважаемая организация не будет рассылать файлы, даже если это важные данные, такие, как обновления системы или очередная защита от вирусов.

Расширение файла:

Обращайте внимание на расширение файла. Особую опасность могут представлять файлы со следующими расширениями:

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.eml, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vbs,*.vbe, *.wsf, *.wsh, *.wsc.

Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

Как правильно удалять сообщение из почтовой программы:

Будьте очень осторожны при получении сообщений с файлами-вложениями. Подозрительные сообщения лучше немедленно удалять.

Чтобы удалить сообщение в почтовой программе полностью:

- удалите сообщение из папки «Входящие»;
- удалите сообщение из папки «Удаленные»;
- выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

Защита электронной почты:

Нельзя исключать случаи, когда присылаемые файлы все-таки будут запущены. Однако и в этих случаях можно принять контрмеры.

В первую очередь, следите, чтобы у вас были установлены самые последние обновления программ. Нелишним будет установить персональный межсетевой экран (firewall). В нём следует указать исчерпывающий список программ и доступных им портов и сервисов. Как только какая-либо незнакомая программа попытается отправить почту, она тут же будет обнаружена, и зараза не распространится с Вашего компьютера дальше.

Кроме того, отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы (обращение к файлам, загрузочной области диска, системному реестру и т. п.), способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ ДЕЙСТВИЙ МОШЕННИКОВ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОТЕХНОЛОГИЧНЫХ УСТРОЙСТВ

1. Незамедлительно довести до сведения руководителя структурного подразделения Университета, в котором работник осуществляет трудовую деятельность, информацию о мошенничестве в целях принятия соответствующих мер реагирования (уведомление правоохранительных органов, Министерства науки и высшего образования Российской Федерации по необходимости).

2. Ни в коем случае не сообщать неизвестным лицам свои личные данные, сведения о структурном подразделении, сведения о деятельности Университета и Министерства.

3. При сомнениях в том, что обращающийся является действующим государственным служащим (в том числе, гражданским служащим) необходимо перезвонить на его служебный номер, согласно телефонного справочника министерств и ведомств, указанных на официальных государственных и муниципальных сайтах; или попросить перезвонить со служебного телефона государственного учреждения.

4. В случае мошенничества, преступники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. Сохраняйте спокойствие.

5. В случае мошенничества, преступник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом «да». Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить тему.

Примечание: *Памятка разработана с учетом письменных рекомендаций Министерства науки и высшего образования Российской Федерации и Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России.*