"МОБИЛЬНЫЕ" МОШЕННИЧЕСТВА

МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ СОВЕРШАЮТСЯ, В ОСНОВНОМ, ПУТЕМ СООБЩЕНИЯ ГРАЖДАНАМ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ:

ВАМ СООБЩАЮТ, ЧТО КТО-ТО ИЗ БЛИЗКИХ ПОПАЛ В НЕПРИЯТНУЮ СИТУАЦИЮ, ЕМУ МОЖЕТ ГРОЗИТЬ НАКАЗАНИЕ, И ДЛЯ «РЕШЕНИЯ ВОПРОСА» ПРОСЯТ ПЕРЕДАТЬ ДЕНЬГИ ЛИЧНО ИЛИ ЧЕРЕЗ ТЕРМИНАЛЫ ОПЛАТЫ.

ПРИХОДИТ СМС О ТОМ, ЧТО ВАША БАНКОВСКАЯ КАРТА ЗАБЛОКИРОВАНА И, ЧТОБЫ ЕЁ РАЗБЛОКИРОВАТЬ, НУЖНО ВЫПОЛНИТЬ РЯД ДЕЙСТВИЙ, НЕ ПОСЕЩАЯ ОФИС БАНКА. НИКОГДА НЕ ВЫПОЛНЯЙТЕ ПОДРБНЫЕ ТРЕБОВАНИЯ. ОБРАТИТЕСЬ В ФИЛИАЛ СВОЕГО БАНКА ЗА КОНСУЛЬТАЦИЕЙ.

ПРЕДСТАВИВШИСЬ ВРАЧОМ ИЛИ СОТРУДНИКОМ ПОЛИКЛИНИКИ, ЗВОНЯЩИЙ СООБЩАЕТ, ЧТО У ВАС ИЛИ ВАШИХ БЛИЗКИХ СЕРЬЁЗНОЕ ЗАБОЛЕВАНИЕ. ДЛЯ ИЗЛЕЧЕНИЯ ПРЕДЛАГАЮТ ЗАПЛАТИТЬ ДЕНЬГИ ИЛИ ПРИОБРЕСТИ ДОРОГОСТОЯЩИЕ ПРЕПАРАТЫ И ПРИБОРЫ.

ВЫ ПОЛУЧАЕТЕ СМС ИЛИ ЗВОНЯЩИЙ САМ СООБЩАЕТ, ЧТО ВЫ СТАЛИ ОБЛАДАТЕЛЕМ ПРИЗА ИЛИ ПОБЕДИТЕЛЕМ КОНКУРСА. ДАЛЕЕ СЛЕДУЕТ ПРОСЬБА ПЕРЕЧИСЛИТЬ ЕМУ ДЕНЬГИ ПОД БЛАГОВИДНЫМИ ПРЕДЛОГАМИ, КАК ГАРАНТИЮ ТОГО, ЧТО НАГРА ДА ПОПАДЁТ ИМЕННО К ВАМ.

ЗВОНЯЩИЙ СООБЩАЕТ ЛИЧНО ИЛИ ПРИСЫЛАЕТ СМС С ПРОСЬБОЙ ВЕРНУТЬ ДЕНЬГИ, КОТОРЫЕ ВАМ ОШИБОЧНО ПЕРЕЧИСЛЕНЫ, ЛИБО ПРОСИТ СРОЧНО ПОПОЛНИТЬ БАЛАНС ЕГО ТЕЛЕФОНА НА НЕБОЛЬШУЮ СУММУ, ИЗОБРАЖАЯ ВАШЕГО ЗНАКОМОГО.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

ПРЕСТУПНИКИ ЕЖЕДНЕВНО ПРИДУМЫВАЮТ НОВЫЕ СХЕМЫ И МАХИНАЦИИ, ЦЕЛЬЮ КОТОРЫХ ЯВЛЯЕТСЯ СНЯТИЕ ДЕНЕГ СО СЧЁТА ВЛАДЕЛЬЦА КАРТЫ. ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ АФЕРИСТОВ, НЕОБХОДИМО СОБЛЮДАТЬ СЛЕДУЮЩИЕ ПРАВИЛА:

УСТАНАВЛИВАЙТЕ НА УСТРОЙСТВА, К КОТОРЫМ ПРИВЯЗАНА КАРТА, ТОЛЬКО ЛИЦЕНЗИОННЫЕ ПРОГРАММЫ И ОБРАЩАЙТЕ ВНИМАНИЕ НА ПОЛНОМОЧИЯ, КОТОРЫЕ ВЫ ПРЕДОСТАВЛЯЕТЕ ПРОГРАММЕ. ОСОБОГО ВНИМАНИЯ ТРЕБУЮТ РАЗРЕШЕНИЯ, КОТОРЫЕ ВЫ ПРЕДОСТАВЛЯЕТЕ ПРОГРАММЕ. СЛЕДУЕТ ИСКЛЮЧИТЬ: ДОСТУП К СМС И ИХ ОТПРАВКУ, ДОСТУП К СЕТИ ИНТЕРНЕТ И Т.Д. МОШЕННИКИ СОЗДАЮТ ПРОГРАММЫ-ВИРУСЫ, КОТОРЫЕ ПОЗВОЛЯЮТ ИМ ПОЛУЧАТЬ ДОСТУП К ДАННЫМ СИСТЕМ ОНЛАЙН БАНКИНГА («МОБИЛЬНЫЕ БАНКИ») И ПОХИЩАТЬ ДЕНЬГИ С ВАШЕГО СЧЁТА.

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ И НЕ УСТАНАВЛИВАЙТЕ ПРИЛОЖЕНИЯ/ОБНОВЛЕНИЯ, ПРИШЕДШИЕ ПО СМС/ММС/ЭЛЕКТРОННОЙ ПОЧТЕ/МЕССЕНДЖЕРАМ, В ТОМ ЧИСЛЕ ОТ ИМЕНИ БАНКА. ПОМНИТЕ, ЧТО БАНК НЕ РАССЫЛАЕТ СВОИМ КЛИЕНТАМ ССЫЛКИ ИЛИ УКАЗАНИЯ ПОДОБНЫМ ОБРАЗОМ.

В СЛУЧАЕ ПОТЕРИ МОБИЛЬНОГО ТЕЛЕФОНА С ПОДКЛЮЧЕННОЙ УСЛУГОЙ «МОБИЛЬНЫЙ БАНК» , СЛЕДУЕТ СРОЧНО ОБРАТИТЬСЯ К ОПЕРАТОРУ СОТОВОЙ СВЯЗИ ДЛЯ БЛОКИРОВКИ SIM-КАРТЫ И В КОНТАКТНЫЙ ЦЕНТР БАНКА ДЛЯ БЛОКИРОВКИ САМОЙ УСЛУГИ. АНАЛОГИЧНЫЕ ДЕЙСТВИЯ НУЖНО ВЫПОЛНИТЬ ПРИ СМЕНЕ НОМЕРА ТЕЛЕФОНА.

НИКОГДА НЕ ПЕРЕДАВАЙТЕ СВОЮ КАРТУ ТРЕТЬИМ ЛИЦАМ И НЕ ПОЗВОЛЯЙТЕ ИМ СОВЕРШАТЬ С НЕЙ МАНИПУЛЯЦИИ. НЕ НАЗЫВАЙТЕ ПОСТОРОННИМ, ДАЖЕ ЕСЛИ ОНИ ПРЕДСТАВИЛИСЬ СОТРУДНИКАМИ БАНКА, ПОЛНЫЕ ДАННЫЕ О СВОЕЙ КАРТЕ: НОМЕР, ФИО ВЛАДЕЛЬЦА, СРОК ДЕЙСТВИЯ, КОД ПРОВЕРКИ (ТРИ ЦИФРЫ НА ОБРАТНОЙ СТОРОНЕ КАРТЫ). СОТРУДНИКИ БАНКА НИКОГДА НЕ СПРАШИВАЮТ ТАКУЮ ИНФОРМАЦИЮ. ХРАНИТЕ ПИН-КОД И КАРТУ РАЗДЕЛЬНО, А ЛУЧШЕ - ЗАПОМНИТЕ ЕГО НАИЗУСТЬ.

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

НАИБОЛЕЕ ЧАСТО ГРАЖДАНЕ ПОПАДАЮТСЯ НА УДОЧКУ МЕШЕННИКОВ, КОГДА СОВЕРШАЮТ ПОКУПКИ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ ИЛИ НАРУШАЮТ МЕРЫ БЕЗОПАСНОСТИ ПРИ СОВЕРШЕНИИ ОНЛАЙН ПЛАТЕЖЕЙ.

ПРИ ЗАКАЗЕ ТОВАРОВ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ (ОНЛАЙН МАГАЗИНЫ, СОЦ.СЕТИ, РЕСУРСЫ ОБЪЯВЛЕНИЙ). ПОЧИТАЙТЕ ОТЗЫВЫ НА РАЗНЫХ САЙТАХ О ПРОДАВЦЕ.

ЧАСТО В СЕТИ ВСТРЕЧАЮТСЯ САЙТЫ-КЛОНЫ ДОБРОСОВЕСТНЫХ ПРОДАВЦОВ. МОШЕННИКИ КОПИРУЮТ ИНТЕРФЕЙС ТОРГОВОЙ ПЛОЩАДКИ С ОТЛИЧНОЙ РЕПУТАЦИЕЙ И ОБМАНЫВАЮТ ПОТРЕБИТЕЛЕЙ. ЧТОБЫ ЭТОГО НЕ ПРОИЗОШЛО С ВАМИ, НУЖНО ВНИМАТЕЛЬНО ПРОВЕРИТЬ ДОМЕННОЕ ИМЯ САЙТА.

ЕСЛИ ПРОДАВЕЦ ПРЕДЛАГАЕТ КУПИТЬ ТОВАР ПО ЦЕНЕ, СУЩЕСТВЕННО НИЖЕ СРЕДНЕРЫНОЧНОЙ, ЛИБО ДЕЛАЕТ СЛИШКОМ БОЛЬШИЕ СКИДКИ, ТО ПРЕЖДЕ, ЧЕМ ДЕЛАТЬ ПОКУПКУ:

- ПРОВЕРЬТЕ ДАТУ РЕГИСТРАЦИИ САЙТА ЧЕРЕЗ СПЕЦИАЛЬНЫЕ ИНТЕРНЕТ-СЕРВИСЫ. ЕСЛИ ПРОДАВЕЦ РАБОТАЕТ НЕДАВНО, ЛУЧШЕ НАЙТИ АЛЬТЕРНАТИВУ.
- ЗАЙДИТЕ В РАЗДЕЛ САЙТА, ГДЕ РАЗМЕЩЕНЫ КОНТАКТНЫЕ ДАННЫЕ ПРОДАВЦА. ЕСЛИ УКАЗАН ЛИШЬ АДРЕС ЭЛ. ПОЧТЫ И НОМЕРА МОБИЛЬНЫХ ОПЕРАТОРОВ, ОЗДЕРЖИТЕСЬ ОТ ПОКУПКИ.

СТАРАЙТЕСЬ НЕ СОВЕРШАТЬ ПОКУПКИ В СЕТИ ИНТЕРНЕТ, ЕСЛИ ТРЕБУЕТСЯ СТОПРОЦЕНТНАЯ ПРЕДОПЛАТА. ОБЫЧНО ДОБРОСОВЕСТНЫЕ ПРОДАВЦЫ ПРЕДЛАГАЮТ ВОЗМОЖНОСТЬ ОТПРАВКИ ТОВАРА НАЛОЖЕННЫМ ПЛАТЕЖОМ.

ПРИ ПОЛУЧЕНИИ ТОВАРА ОТ КУРЬЕРА ВСКРЫВАТЕ ПОСЫЛКУ ПРИ НЁМ И НЕ ОТДАВАЙТЕ ДЕНЬГИ ПРЕЖДЕ, ЧЕМ УБЕДИТЕСЬ В ТОМ, ЧТО ПОЛУЧИЛИ ТО, ЧТО ЗАКАЗЫВАЛИ. ПРИ ВСКРЫТИИ ПОСЫЛКИ ЖЕЛАТЕЛЬНО ПРОИЗВОДИТЬ ВИДЕО ИЛИ ФОТОСЪЁМКУ ЭТОГО ПРОЦЕССА.

Мобильное мошенничество

Типичные ситуации:

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь делать перевод
- Перезвоните родным и узнайте, все ли у них в порядке
- Уточните, где находится близкие, подключите услугу «Маячок»

Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка

Ваш аккаунт в социальных сетях заблокирован. Для разблокировки вас просят отправить SMS на «короткий» номер

- Не торопитесь следовать инструкциям
- Обратитесь с запросом к администрации социальной сети и мобильному оператору
- Не доверяйте сомнительным источникам
- Не размещайте в социальных сетях конфиденциальную информацию

Вам прислали «Открытку» (MMS) с неизвестного номера

- Не открывайте вложенные файлы и не переходите по ссылкам
- Удалите сообщение с ссылкой
- Защитите свой телефон, подключите **БЕСПЛАТНУЮ** услугу «Стоп-контент»
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков

Как защитить себя и близких от мобильных мошенников:

Будьте бдительны
Узнавайте подробную информацию об актуальных схемах мошенничества в новостном разделе на портале stopfraud.megafon.ru или в средствах массовой информации.

Избегайте или сводите к минимуму передачу любой конфиденциальной информации
В последнее время участились случаи использования этой информации в мошеннических целях.

Не спешите действовать по инструкциям неизвестных людей
Убедитесь в достоверности информации, полученной с незнакомых номеров, через уполномоченные организации, родственников или знакомых.

Не переводите деньги на незнакомые номера

При использовании «коротких» номеров уточняйте у оператора стоимость предоставляемой услуги
Внимательно читайте условия предоставления услуг. Для проверки стоимости SMS воспользуйтесь БЕСПЛАТНЫМ сервисом «Мобильный прайс»: отправьте $ на «короткий» номер услуги. В ответном сообщении будет указана стоимость отправки SMS на данный номер и название контент-провайдера.

Не отдавайте телефон в руки незнакомцев
Предложите самостоятельно набрать нужный номер и передать информацию.

Помните, что «бесплатный сыр бывает только в мышеловке»
Не доверяйте неизвестным людям, которые обещают вам легкие выигрыши, быстрые исцеления и баснословные заработки.

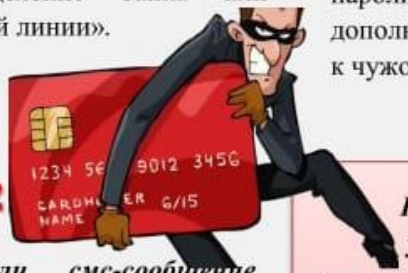
ОСТОРОЖНО, МОШЕННИКИ!

В результате телефонных и интернет-мошенничеств с банковских карт граждан совершаются хищения денежных средств, чтобы не стать жертвами данных мошенников, необходимо запомнить основные способы их действий:

Ситуация №1

Вам пришло смс-сообщение или поступил звонок якобы от работников банка о том, что банковская карта заблокирована, произошло списание денежных средств, или необходимо подключить какую-либо услугу?

Не выполняйте никаких операций с картами по полученным от неизвестных лиц инструкциям по телефону, сразу же обратитесь в отделение банка или по телефону «горячей линии».



Ситуация №2

Вам отправили смс-сообщение или позвонили якобы ваши близкие, или от имени сотрудников полиции и сообщили, что родственник попал в беду и требуют деньги для решения проблем?

Сохраняйте спокойствие, прекратите разговор, перезвоните своим близким и убедитесь, что всё в порядке.

Ситуация №3

Вам позвонили по объявлению, размещенному вами на сайтах «Авито», «Дром» и др., и просят для перечисления денежных средств подойти к банкомату и выполнить какие-либо операции покарте?

Помните, что для перечисления денежных средств на вашу карту достаточно знать только ее номер, не сообщайте никому другой дополнительной информации (реквизиты, пароли, коды доступа) и не подключайте дополнительную услугу «Мобильный банк» к чужому номеру.

Кроме того, в последнее время участились хищения с карт через услугу «Мобильный банк» при помощи вирусной программы.

Чтобы обезопасить свои счета, в таком случае необходимо обеспечить безопасный выход в интернет через мобильный телефон, подключенный к данной услуге, установить антивирусную программу или вообще исключить доступ в интернет с мобильного телефона.

Ситуация №4

Вам от друзей поступило обращение на интернет-сайтах («Одноклассники», «ВКонтакте» и др.) с просьбой занять деньги или назвать реквизиты своей карты?

В данному случае от имени друзей могут действовать мошенники, цель которых одна - завладеть вашими деньгами.

Обратите внимание!

В сети Интернет действует большое количество мошеннических сайтов, предлагающих свои товары и услуги. Доверяйте только проверенным сайтам или производите оплату только при получении товара.

Если Вы стали жертвой мошенничества, незамедлительно обратитесь по телефонам: 02, 102!

ОСТОРОЖНО - МОШЕННИКИ!

Полиция всегда готова прийти на помощь пострадавшим от действий преступников, но самый лучший способ борьбы с правонарушениями - Ваша правовая грамотность и бдительность!

С каждым годом мошенники придумывают все более изощренные схемы отъема денег. Вот простые рекомендации, соблюдение которых поможет Вам сохранить деньги и ценности:

Вы получили СМС-сообщение о неожиданном выигрыше.

Задумайтесь! Настоящий розыгрыш призов не должен подразумевать денежные выплаты с Вашей Стороны! Не торопитесь расставаться со своими деньгами!

Вы получили СМС-сообщение о том, что Ваша банковская карта заблокирована или Вашей банковской карте необходима «двойная» защита от мошенников.

Знайте, что основная часть мошенничеств совершается именно данным способом, когда граждане теряя бдительность сообщают мошенникам номера и пароли (пин-код) от своей банковской карты или перечисляют деньги на указанные мошенниками счета.

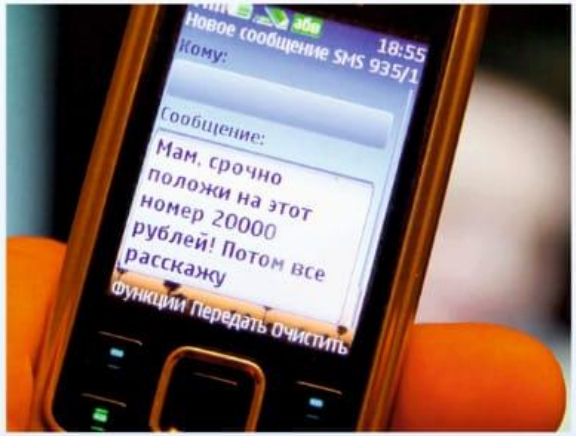
Вам звонят с незнакомого номера и тревожным голосом сообщают, что Ваши близкие попали в беду. А для того, чтобы решить проблему, нужна крупная сумма денег.

По такой схеме работают мошенники! Позвоните родственникам, чтобы проверить данную информацию. И знайте, что дача взятки является также преступлением.

ТАКТИКА ТЕЛЕФОННЫХ МОШЕННИКОВ

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок.

SMS - это мошенничество «вслепую»: такие сообщения рассылаются в большом объеме - в надежде на доверчивого получателя.



Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

Цель мошенников - заставить Вас передать свои денежные средства «добровольно». Для этого используются различные схемы мошенничества.

Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

❶ передать деньги из рук в руки или оставить в условленном месте;

❷ приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;

❸ перевести деньги на свой счёт и ввести специальный код;

❹ перевести деньги на указанный счёт;

❺ позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства.

КАК ПРАВИЛЬНО РЕАГИРОВАТЬ НА ПОПЫТКУ ВОВЛЕЧЕНИЯ В МОШЕННИЧЕСТВО

Мошенники очень хорошо знают психологию людей. Они используют следующие мотивы:

❶ Беспокойство за близких и знакомых.

❸ Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.

❸ Желание выиграть крупный приз.

❹ Любопытство - желание получить доступ к SMS и звонкам других людей.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от Вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

Телефонные мошенники рассчитывают на доверчивых, податливых людей, которые соглашаются с тем, что им говорят, и выполняют чужие указания. Спокойные, уверенные вопросы отпугнут злоумышленников.

ЧТО НАДО ЗНАТЬ, ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Если Вы сомневаетесь, что звонивший действительно Ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Помните, что никто не имеет права требовать коды с карт экспресс-оплаты!

Оформление выигрыша никогда не происходит только по телефону или Интернету. Если Вас не просят приехать в офис организатора акции с документами - это мошенничество.

Не ленитесь перезванивать своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования якобы заблокированного номера.

Для возврата средств при якобы ошибочном переводе существует чек. Не возвращайте деньги - их вернет оператор.

Услуга «узнайте SMS и телефонные переговоры» может оказываться исключительно операторами сотовой связи и в установленном законом порядке.

ЕСТЬ НЕСКОЛЬКО ПРОСТЫХ ПРАВИЛ:

❶ отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;

❷ не реагировать на SMS без подписи с незнакомых номеров;

❸ внимательно относиться к звонкам с незнакомых номеров.