Внимание! Мошенники!

04.02.2021 20:21

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. УМВД России по Мурманской области рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН КОД КАРТЫ
2. ВЫУЧИТЬ ПИН КОД ЛИБО ХРАНИТЬ ЕГО ОТДЕЛЬНО ОТ КАРТЫ И НЕ В БУМАЖНИКЕ
3. НЕ ПЕРЕДАВАТЬ КАРТУ ДРУГИМ ЛИЦАМ ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ
4. ПОЛЬЗОВАТЬСЯ ТОЛЬКО БАНКОМАТАМИ НЕ ОБОРУДОВАННЫМИ ДОПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ
5. ПО ВСЕМ ВОПРОСАМ СОВЕТОВАТЬСЯ С БАНКОМ, ВЫДАВШИМ КАРТУ

Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

ПИН-КОД — КЛЮЧ К ВАШИМ ДЕНЬГАМ

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду, как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ВАША КАРТА – ТОЛЬКО ВАША

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

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.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

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.

Использование банкоматов без видеонаблюдения опасно вероятностью нападения злоумышленников.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

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 нём телефону.

БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – отнажитесь от его использования. Велика вероятность того, что он перепрограммирован мошенниками.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком – он обязан предоставить консультацию по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе 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.

ИНТЕРНЕТ – ЭТО БЕЗГРАНИЧНЫЙ МИР ИНФОРМАЦИИ. ЗДЕСЬ ТЫ НАЙДЁШЬ МНОГО ИНТЕРЕСНОГО И ПОЛЕЗНОГО ДЛЯ УЧЁБЫ. В ИНТЕРНЕТЕ МОЖНО ОБЩАТЬСЯ СО ЗНАКОМЫМИ И ДАЖЕ ЗАВОДИТЬ ДРУЗЕЙ.

НО КРОМЕ ХОРОШЕГО, В ВИРТУАЛЬНОМ МИРЕ ЕСТЬ И ПЛОХОЕ. НЕПРАВИЛЬНОЕ ПОВЕДЕНИЕ В ИНТЕРНЕТЕ МОЖЕТ ПРИНЕСТИ ВРЕД НЕ ТОЛЬКО ТЕБЕ, НО ТАКЖЕ ТВОИМ РОДНЫМ И БЛИЗКИМ.

ЧТОБЫ ОБЕЗОПАСИТЬ СЕБЯ В ИНТЕРНЕТЕ, ДОСТАТОЧНО СОБЛЮДАТЬ ПРАВИЛА, КОТОРЫЕ СОДЕРЖАТСЯ В ЭТОЙ ПАМЯТКЕ. В ЭТИХ ПРАВИЛАХ НЕТ НИЧЕГО ТРУДНОГО. ОТНЕСИСЬ К НИМ ВНИМАТЕЛЬНО – И РАССКАЖИ О НИХ СВОИМ ДРУЗЬЯМ!

ТЕСТ НА ЗНАНИЕ ПРАВИЛ ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.
   А Попрошу его фото, и потом отправлю своё.
   В Посоветуюсь с родителями.
2) В чате тебя обозвали очень грубыми словами.
   А Скажу в ответ: «Сам дурак».
   В Прекращу разговор с этим человеком.
3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.
   А Потребую доказательств, что она плохая.
   В Сразу откажусь.
4) Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.
   А Вышлю только пароль: они сами должны знать логин.
   В Отмечу письмо как спам.

ПОСЧИТАЙ, СКОЛЬКО ПОЛУЧИЛОСЬ ОТВЕТОВ «А» И СКОЛЬКО «В».

4 «А»
Тебе ещё многому надо научиться.

3 «А» и 1 «В»
Внимательно прочитай эту памятку.

2 «А» и 2 «В»
Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В»
Ты почти справился, но есть слабые места.

4 «В»
Молодец! К Интернету готов!

Внимание! Мошенники!

04.02.2021 20:21

Внимание! Мошенники!

04.02.2021 20:21

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS: "ваша карта временно заблокирована, перезвоните по номеру" Вам ответит мошенник и попытается узнать персональные данные вашей карты.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер-«грабитель»:платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом.

В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

УМВД России по Мурманской области напоминает, что чаще всего в сети телефонных мошенников попадаются пожилые люди или доверчивые подростки. При этом **каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.**

Телефонные мошенники используют мобильные телефоны для обмана и изъятия денежных средств граждан.

- **Основные схемы**
- **Тактика мошенников**
- **Как реагировать**

ТАКТИКА ТЕЛЕФОННЫХ МОШЕННИКОВ

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

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – 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:

1. **передать деньги из рук в руки или оставить в условленном месте;**
2. **приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;**
3. **перевести деньги на свой счёт и ввести специальный код;**
4. **перевести деньги на указанный счёт;**
5. **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:

а. Беспокойство за близких и знакомых.
б. Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
в. Желание выиграть крупный приз.
г. 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 отключён, 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.

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.
При поступлении на мобильный телефон смс-сообщения о блокировке банковской карты не следует звонить по указанному в сообщении номеру, нужно самостоятельно проверить работоспособность карты, либо позвонить по официальному номеру клиентской службы обслуживающего карту банка.
Также следует помнить, что банковские работники никогда не совершают никаких операций по счету карты в телефонном режиме, никогда не требуют от клиентов разглашения конфиденциальных сведений.

Ни в коем случае не следует выполнять требований и просьб, поступающих с неизвестных номеров мобильных или стационарных телефонов, от неизвестных лиц, совершать любые платежные операции по данным просьбам.

Если есть подозрения, что в отношении Вас или Ваших близких совершены мошеннические действия, следует незамедлительно сообщить об этом в полицию.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

SMS: "ваша карта временно заблокирована, перезвоните по номеру" Вам ответит мошенник и попытается узнать персональные данные вашей карты.

Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом.

В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

ТАКТИКА ТЕЛЕФОННЫХ МОШЕННИКОВ

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

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – 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:

1. **передать деньги из рук в руки или оставить в условленном месте;**
2. **приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;**
3. **перевести деньги на свой счёт и ввести специальный код;**
4. **перевести деньги на указанный счёт;**
5. **позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства;**

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 отключён, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

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

При поступлении на мобильный телефон смс-сообщения о блокировке банковской карты не следует звонить по указанному в сообщении номеру, нужно самостоятельно проверить работоспособность карты, либо позвонить по официальному номеру клиентской службы обслуживающего карту банка.
Также следует помнить, что банковские работники никогда не совершают никаких операций по счету карты в телефонном режиме, никогда не требуют от клиентов разглашения конфиденциальных сведений.

Ни в коем случае не следует выполнять требований и просьб, поступающих с неизвестных номеров мобильных или стационарных телефонов, от неизвестных лиц, совершать любые платежные операции по данным просьбам.

КАК ПРАВИЛЬНО РЕАГИРОВАТЬ НА ПОПЫТКУ ВОВЛЕЧЕНИЯ В МОШЕННИЧЕСТВО

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

а. Беспокойство за близких и знакомых.
б. Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
в. Желание выиграть крупный приз.
г. 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.

ЕСТЬ НЕСКОЛЬКО ПРОСТЫХ ПРАВИЛ:

- отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- не реагировать на SMS без подписи с незнакомых номеров;
- внимательно относиться к звонкам с незнакомых номеров.