

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ 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 Управления «К» 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 сэкономят Ваши средства.



Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ

**Будьте
осторожны
и внимательны!**

Мошенничества
с пластиковыми картами



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 кошелек, 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 – откажитесь 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.

САЙТ-ДУБЛЁР –

это сайт, который внешне на 99% повторяет настоящий сайт благотворительной организации или активиста, собирающего средства на доброе дело.

Отличия сайта-дублёра от оригинального минимальны: одна или две буквы в доменном имени сайта (имени, которое указано в адресной строке браузера) и другой номер счёта, куда перечисляют средства.

Изготовить такой сайт-дублёр очень просто: он может появиться в самое кратчайшее время после публикации настоящего – оригинального сайта. Поэтому мошенники всё чаще прибегают к этой схеме обмана.



На сегодняшний день Интернет является очень эффективным инструментом для использования его в благотворительных целях.

Развитие электронных кошельков и расширение возможностей по перечислению денежных средств, упрощает участие в благотворительной деятельности для каждого пользователя Интернета.

Одновременно злоумышленники приспособились использовать сбор средств на благотворительных сайтах в своих мошеннических схемах.



Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

**ПОЛЬЗОВАТЕЛЯМ
ИНТЕРНЕТА**

**Будьте
осторожны!**

МОШЕННИЧЕСКОЕ
ДУБЛИРОВАНИЕ
БЛАГОТВОРИТЕЛЬНЫХ
САЙТОВ



КАК ОРГАНИЗОВАНО МОШЕННИЧЕСТВО:

Вы узнаете о трагической ситуации, в которой требуется помощь.

Достаточно зайти на некий сайт и перевести деньги на указанные реквизиты.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Злоумышленники отслеживают социальную ситуацию и активно используют темы, которые являются заведомо выигрышными с точки зрения возможных откликов граждан.

Тематика благотворительных сайтов может быть самой разной:

- ▶ помощь больным детям – сбор средств на операцию;
- ▶ помощь жертвам терактов;
- ▶ помощь пострадавшим во время стихийных бедствий – землетрясений, цунами, сходов лавин и оползней;
- ▶ восстановление храмов;
- ▶ помощь приютам, заботящимся о брошенных животных.

Для осуществления своих противоправных замыслов мошенники создают сайты-дублиеры, которые являются точной копией официальных сайтов с той лишь разницей, что на них указаны другие расчетные счета, по которым гражданам предлагается направлять денежные средства.

Учащаются случаи создания полностью выдуманных историй, созданных на основе правдивых.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не поленитесь перепроверить информацию в Интернете.

Ей можно будет доверять только в том случае, если на нескольких сайтах будет указан один и тот же расчетный счет и номер телефона.

Если вы планируете постоянно участвовать в благотворительной деятельности, используйте сайт, принадлежащий благотворительной организации или группе активистов. Помогайте тем, кто даёт информацию «из первых рук» и известен своей надёжной репутацией.

Посмотрите, указан ли на сайте номер телефона для связи.

Если да, то следует позвонить по нему и уточнить все детали. Например, если необходимы деньги на операцию ребенку, спросите о диагнозе, узнайте имя лечащего врача, номер больницы, в которой наблюдается ребенок и т.д.

Задавайте как можно больше уточняющих вопросов: если на другом конце провода вам не смогут ответить на поставленные вопросы, либо ответы будут уклончивыми и неуверенными, или ответы вообще не будут совпадать с тем, что указано на сайте, то, скорее всего, вы общаетесь с мошенниками.

Зачастую мошенники вообще не указывают никаких телефонных номеров, чтобы их было сложнее вычислить.

