



Рекомендации гражданам по защите от мошенников использующих высокотехнологичные устройства



В нашей повседневной жизни мы используем мобильные телефоны, компьютеры и банковские (пластиковые) карты, которые постоянно усовершенствуются новыми программами и сервисами. Достаточно наличия в мобильном телефоне сервиса «Мобильный банк» чтобы, не выходя из дома произвести различные платежные операции (оплата коммунальных услуг, покупок, перевод денег и др.). Но все чаще граждане попадают на уловки мошенников имеющих в своем арсенале десятки способов присвоения денежных средств с пластиковых карт или счета мобильного телефона.

Не поддаваться на уловки мошенников можно соблюдая следующие рекомендации:

ТЕЛЕФОННЫЕ ВИРУСЫ

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения перейдите 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



Официальный сайт

Следственное управление Следственного комитета Российской Федерации по Чеченской Республике

используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт 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.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

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.

Чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

Как поступать в такой ситуации:

Ни один банк и ни одна организация 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.

Как защититься от мошенников владельцам пластиковых банковских карт:

1. Никогда и никому не сообщайте ПИН-код Вашей карты, это ключ к вашим деньгам. Лучше всего запомнить ПИН-код. Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счет, заблокировав карту после кражи или утери.
2. Не позволяйте никому использовать Вашу пластиковую карту – это все равно, что отдать свой кошелек, не пересчитывая сумму в нем.
3. 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 предложениями, не спешите ее 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.

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

5. Пользуйтесь защищенными 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.

Лица, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

6. Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей.

Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

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.

7. 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.

8. 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.

9. Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.



Официальный сайт

Следственное управление
Следственного комитета Российской Федерации
по Чеченской Республике

10. 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.

Будьте бдительны!

29 Августа 2017

Адрес страницы: <https://chr.sledcom.ru/news/item/1159578>