ПРОКУРАТУРА
КЕМЕРОВСКОЙ ОБЛАСТИ –
КУЗБАССА

КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРМОШЕННИКОВ, СОВЕРШАЯ ПОКУПКИ В ИНТЕРНЕТ-МАГАЗИНАХ

PROKURATURA42

Накануне «майских» праздников возможен рост дистанционных мошенничеств. Опасность представляют письма якобы из интернет-магазинов, в которых предлагаются подарки, скидки, выгодные акции или используются другие уловки. Они, как правило, содержат ссылки или вложенные файлы. Загрузка небезопасного файла или переход по сомнительной ссылке могут повлечь автоматическую установку на компьютер или мобильный телефон вредоносных программ или перенаправить на мошеннический сайт.

Цель преступников - получить данные банковской карты (номер, CVV-код на обратной стороне) или пароль подтверждения операции из СМС. В итоге можно лишиться всех денег на банковской карте.

Прокуратура Кемеровской области – Кузбасса предупреждает: совершайте покупки только на проверенных ресурсах, которым вы доверяете. Адрес поддельного сайта может отличаться от настоящего одной-двумя буквами, но, введя на нем данные своей карты, вы даете преступникам ключ к своим деньгам.

Для интернет-покупок можно завести отдельную карту и держать на ней только ту сумму, которую собираетесь потратить.

Если вас пытаются увести из чата безопасной площадки - сервиса объявлений или доставки товаров - в один из мессенджеров, чтобы обсудить сделку и просят назвать данные вашей банковской карты - откажитесь. Никогда и ни под каким предлогом не сообщайте посторонним данные своей карты.

Если вы пострадали от действий мошенников, незамедлительно обратитесь в органы полиции **(02, 112).**

За хищение денежных средств с банковского счета, а равно электронных денежных средств, в том числе путем обмана или злоупотребления доверием, предусмотрена уголовная ответственность (**п. «г» ч. 3 ст. 158 и ст. 159** Уголовного кодекса Российской Федерации).

ПРОКУРАТУРА
КЕМЕРОВСКОЙ ОБЛАСТИ –
КУЗБАССА

предупреждает:

НИКОМУ НЕ СООБЩАЙТЕ СЕКРЕТНЫЕ КОДЫ БАНКОВСКИХ КАРТ

PROKURATURA42

1. Никогда и никому не сообщайте ПИН-код банковской карты, трехзначный код на обороте карты, коды из СМС, пароли от интернет-банка.

2. Сотрудники банка никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он свершается якобы с официального номера банка, – дело рук мошенников!

3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните все ли в порядке с вашими деньгами.

4. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером.

5 Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.

6 Знакомый в соцсетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7 Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните: попытка дать взятку – преступление!

8 Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.

9 **Пользуйтесь только проверенными интернет-магазинами!**

10 **Используйте лицензионное антивирусное программное обеспечение.**

11 **Никогда и ни при каких обстоятельствах нельзя под диктовку неизвестных лиц выполнять какие-либо операции со своими банковскими счетами и картами. Компенсации за якобы некачественные услуги или ущерб от деятельности финансовой пирамиды – это стандартные уловки мошенников.**

За мошенничество с использованием электронных средств платежа, кражу с банковского счета, а равно в отношении электронных денежных средств предусмотрена уголовная ответственность

В ЛЮБОЙ СИТУАЦИИ СОХРАНЯЙТЕ БДИТЕЛЬНОСТЬ, НЕ ПОЗВОЛЯЙТЕ МОШЕННИКАМ ОБМАНЫВАТЬ ВАС !

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАЙТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ

02, 112

ПРОКУРАТУРА КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССА

предупреждает:

НИКОМУ НЕ СООБЩАЙТЕ СЕКРЕТНЫЕ КОДЫ БАНКОВСКИХ КАРТ!

1. Никогда и никому не сообщайте ПИН-код банковской карты, пароль от мобильного и Интернет-банка, трехзначный код на обороте карты, коды из СМС.
2. Сотрудники банка никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он свершается якобы с официального номера банка, - дело рук мошенников!
3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните все ли в порядке с вашими деньгами.
4. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером.
5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.
6. Знакомый в соцсетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!
7. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните: попытка дать взятку – преступление!
8. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.
9. Пользуйтесь только проверенными интернет-магазинами!
10. Используйте лицензионное антивирусное программное обеспечение.
11. Никогда и ни при каких обстоятельствах нельзя под диктовку неизвестных лиц выполнять какие-либо операции со своими банковскими счетами и картами. Компенсации за якобы некачественные услуги или ущерб от деятельности финансовой пирамиды – это стандартные уловки мошенников.

За мошенничество с использованием электронных средств платежа, кражу с банковского счета, а равно в отношении электронных денежных средств предусмотрена уголовная ответственность

В ЛЮБОЙ СИТУАЦИИ СОХРАНЯЙТЕ БДИТЕЛЬНОСТЬ, НЕ ПОЗВОЛЯЙТЕ МОШЕННИКАМ ОБМАНЫВАТЬ ВАС!

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАЙТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ 02, 112

- использовать банковскую карту в торговых точках, не вызывающих подозрений
- в случае некорректной работы банкомата если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – рекомендуется отказаться от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Если вам пришло СМС от банка о блокировке карты или звонят из банка и спрашивают номер карты, пароль и код доступа, необходимо проверить эту информацию и перезвонить в клиентскую службу поддержки банка.

Одним из видов мошенничества с платежными картами является так называемый «скимминг» - считывание данных карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру. Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты. Поэтому перед тем как вставить карту в картоприемник следует внимательно осмотреть банкомат на предмет наличия подозрительных устройств.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

Если вы стали жертвой мошенничества, незамедлительно обратитесь в органы полиции по телефонам 02 и 112, либо путем подачи заявления о совершении преступления непосредственно в отделении полиции.

ПРОКУРАТУРА
КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССА
650992, Кемеровская область,
г.Кемерово, ул. Кирова, д. 24,
kem-pilat@kemprok.ru,

Кемерово, 2021

ПРОКУРАТУРА КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССА

О МЕРАХ ПО ПРЕДУПРЕЖДЕНИЮ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ КАРТ

Росту преступлений, связанных с хищением денежных средств с банковских карт, как показывает практика, способствует недостаточная осведомленность граждан в области информационных технологий и несоблюдение элементарных правил безопасности.

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из следующего.

СОТРУДНИКИ БАНКА НИКОГДА ПО ТЕЛЕФОНУ ИЛИ В ЭЛЕКТРОННОМ ПИСЬМЕ НЕ ЗАПРАШИВАЮТ:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты)
- реквизиты и срок действия карты
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены
- логин, ПИН-код, или CVV-код банковских карт

СОТРУДНИКИ БАНКА ТАКЖЕ НЕ ПРЕДЛАГАЮТ:

- установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства)
- перейти по ссылке из СМС-сообщения
- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк
- под их руководством перевести для сохранности денежные средства на «защищенный счет»
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма

Банк может инициировать общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии и т.д.

НЕОБХОДИМО УЧИТЫВАТЬ, ЧТО ДЕРЖАТЕЛЬ КАРТЫ ОБЯЗАН САМОСТОЯТЕЛЬНО ОБЕСПЕЧИВАТЬ КОНФИДЕНЦИАЛЬНОСТЬ ЕЕ РЕКВИЗИТОВ И В ЭТОЙ СВЯЗИ ИЗБЕГАТЬ:

- подключения к общедоступным сетям Wi-Fi
- использования ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону, сообщения их третьим лицам

При использовании банкоматов убедитесь, что все операции, совершаемые предыдущим клиентом, завершены, что на клавиатуре и в месте для приема карт нет дополнительных устройств.

Совершая операции, не прислушивайтесь к советам незнакомых людей и не принимайте их помощь.

ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ТЕЛЕФОНА СОБЛЮДАЙТЕ СЛЕДУЮЩИЕ ПРАВИЛА:

- при установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»
- отключите в настройках возможность голосового управления при заблокированном экране

Применяя сервисы СМС-банка, сверяйте реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.

При оплате услуг картой в сети «Интернет» требуется всегда учитывать высокую вероятность перехода на поддельный сайт. Поэтому необходимо использовать только проведенные сайты, внимательно читать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операций.

КРОМЕ ТОГО, НЕОБХОДИМО ПРИДЕРЖИВАТЬСЯ СЛЕДУЮЩИХ ПРАВИЛ:

- в торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты. В противном случае мошенники могут получить ее реквизиты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки
- в случае потери банковской карты немедленно позвонить в банк для блокировки - это поможет сохранить денежные средства
- подключить услугу смс-информирование это обеспечит контроль за проведением любых операции по карте. При получении смс о несанкционированном списании средств со счета, заблокировать карту
- установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удалённо - в интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте
- при вводе пин-кода прикрывать клавиатуру. Вводить пин-код быстрыми отработанными движениями - это поможет в случае, установки скрытых видеокамер мошенников
- выбирать для пользования терминалы и банкоматы, которые расположены непосредственно в отделениях банка или других охраняемых учреждениях