

Обращайте внимание на картоприемник и клавиатуру банкомата. Если вы видите, что картоприемник банкомата имеет видимые повреждения (трещины, надломы, лопнувший корпус), клавиатура банкомата неестественно приподнята, при нажатии кнопок шатается, то от использования данного банкомата лучше воздержаться.

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования.

Возможно он перепрограммирован мошенниками.

7. 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.

8. По возможности используйте одни и те же банкоматы. У Вас будет возможность заметить что-нибудь необычное и новое на знакомом аппарате.

9. При вводе ПИН-кода, прикройте второй рукой, перчаткой или еще чем-нибудь процесс ввода ПИН-кода.

Делайте это всегда, даже в том случае, если на банкомате установлены специальные стенки защиты клавиатуры.

10. Регулярно меняйте ПИН-код Вашей карты. Особенно после заграничных поездок или снятия денег в подозрительных местах.

Помните Ваша бдительность и внимательность поможет Вам не стать жертвой преступления!



Информация подготовлена
Кунгурской городской прокуратурой
Пермский край, г. Кунгур,
ул. Октябрьская, д. 30,
Тел. (34271) 23069, 23388

Кунгурская городская прокуратура



ВНИМАНИЕ!

мошенничество

с кредитными картами



Кунгур
2019

Банковские пластиковые карты – способ совершения преступления

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.

Способы защиты пользователей банковский карт от скимминга

Что такое Скимминг — это кража денег с Вашей банковской карты, при котором используется скиммер — инструмент для считывания магнитной дорожки платёжной карты, а также миниатюрная видекамера или ложная накладка на блок для ввода ПИН-кода.

При осуществлении «скимминга» используется два основных устройства: прибор для считывания магнитной дорожки, миниатюрная видекамера или накладка на клавиатуру для определения вводимого ПИН-кода.

Скимминг-мошенничество может произойти в любом месте, где совершается финансовая операция без участия сотрудника банка или продавца магазина.

Все устройства имеют автономное питание, поэтому, если Вы не видите лишних проводов, это не значит, что скимминг-устройства отсутствуют. Данные с этих устройств могут сохраняться на внутренних картах памяти или автоматические передаваться по каналам мобильного интернета.

Миниатюрная камера, или камеры, могут быть размещены под козырьком банкомата, в накладных панелях, на рекламных боксах с брошюрами и т.п.

Даже если разместить камеру на стене помещения, можно определить вводимый ПИН-кода по движению пальцев руки.

Вместо камеры мошенниками может быть использована ложная клавиатура, которая запоминает все вводимые данные. Такие клавиатуры выдают себя плохим креплением.



Основные правила безопасности для владельцев пластиковых карт

1. Никому и никогда не сообщаете ПИН-код карты.

2. 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 её выполнять.

3. Выучите ПИН-код.

4. Не храните ПИН-код рядом с картой и тем более записывать ПИН-код на неё.

5. Не передавать карту другим лицам — все операции с картой должны проводиться на Ваших глазах.

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.

6. Пользуйтесь только банкоматами Банка либо банкоматами, находящимися в государственных учреждениях, торговых центрах и т.д.

Банкомат должен быть полностью исправным.

