Акционерный банк “Пивденный”

Советы по предотвращению мошенничества с использованием платежных карт

Уважаемые клиенты, держатели платежных карт Акционерного банка “Пивденный”!
В связи с участившимися случаями мошенничества с использованием платежных карт, просим Вас ознакомиться с правилами и мерами безопасности, направленными на предупреждение мошеннических действий с картой.

1. Общие рекомендации:

- Никогда не передавайте карту и ПИН-код другим лицам, в т.ч. родственникам, коллегам, сотрудникам банка;
- Не пишите ПИН-код на карте и не храните записанный ПИН-код вместе с платежной картой;
- Никому не сообщайте ваш ПИН-код и реквизиты карты;
- В случае утери или кражи карты, выявления подозрительных операций немедленно сообщите об этом в круглосуточную службу поддержки Акционерного банка "Пивденный" по телефону **0-800-30-70-30** или **+38-0482-30-70-30**;
- Устанавливайте суточные лимиты на операции по платежной карте для минимизации несанкционированного использования денежных средств;
- Подключите услугу SMS-информирования для оперативного получения данных об операциях по карте и своевременного выявления подозрительных операций;
- Не используйте для оплаты в сети интернет карты, на которых находятся крупные суммы денег.

2. Банкоматное мошенничество. Примеры установки скиммингговых устройств.

Скимминг – вид мошенничества с банковскими картами, который предусматривает считывание данных с карты (информацию с магнитной полосы карты и вводимый ПИН-код) посредством установки на банкомат специального оборудования с дальнейшим изготовлением дубликатов платежных карт (“белого пластика”) и последующим снятием средств с дубликатов карт.

Как обнаружить скиммингговое устройство:

Накладка на картоприемник банкомата представляет собой устройство, которое приклеивается поверх щели картоприемника и с помощью магнитной головки производит запись информации с магнитной полосы. Данные устройства могут иметь как грубое «кустарное» исполнение и быть хорошо заметны, так и практически точно имитировать детали банкомата. Тем не менее, есть признаки, которые выдают ее работу и могут быть обнаружены обычным пользователем. Накладка банкомата выдает себя хорошо заметной считывающей магнитной головкой прямо за щелью картоприемника. В обычном картоприемнике головка расположена внутри и не видна снаружи. Ниже приведены несколько фото банкомата с установленной накладкой разных моделей. Красным кружком выделена магнитная головка накладки:


не забрали деньги или
рованы в банкомате
3
6
9
000
0


МАГНИТНАЯ ПОЛОСА
ВНИЗУ СПР ВА!


МАГНИТНАЯ ПОЛОСА

Меры безопасности при использовании банкоматов:

- При наборе ПИН-кода прикрывайте клавиатуру руками, а также следите за тем, чтобы вводимый ПИН-код не заметили окружающие;
- Наиболее защищенными являются банкоматы, расположенные на территории банка, а также в хорошо освещенных местах, где есть охрана и видеонаблюдение;
- Не пользуйтесь банкоматом, на котором отсутствует наименование банка и логотипы карт, которые обслуживаются в данном устройстве;
- Внимательно осматривайте картоприемник банкомата до проведения операции. При обнаружении подозрительных устройств, немедленно обратитесь в круглосуточную службу поддержки;
- При проведении операций в банкомате не обращайтесь за помощью к посторонним людям;
- В случае изъятия платежной карты чужим банкоматом немедленно обратитесь в круглосуточную службу поддержки для блокировки карты;
- Выпустите чиповую карту! Этот тип карт на сегодняшний день наиболее защищен от скимминга, т.к. данные с чипа невозможно скопировать!

3. Мошенничество в сети интернет.

Данный тип мошенничества представляет собой сбор конфиденциальных данных платежной карты (номер карты, срок действия, защитный CVV2 / CVC2 код) с последующим проведением операций в интернете от имени держателя платежной карты. Для проведения операций в интернете ПИН-код не требуется, поэтому мошенникам необходимо знать только номер карты, срок ее действия и защитный код, который используется при проведении интернет-расчетов.

Основными способами получения конфиденциальной информации являются:

Фишинг – вид интернет-мошенничества, целью которого является получение реквизитов платежной карты. Данный вид мошенничества реализуется посредством:

1) Поддельного сайта - создание поддельных, временных мошеннических сайтов, на которых держатель карты оставляет реквизиты платежной карты;
2) Телефонного фишинга – мошенник в телефонном режиме предлагает держателю карты сообщить реквизиты карты, якобы для проверки информации о заказе, оформления акции, получения денежного бонуса и.т.д.

3) Отправки писем, электронной почты, SMS-сообщений с просьбой предоставить номер карты, срок ее действия и защитный CVV2 / CVC код, который используется при проведении интернет-расчетов. Держатель карты получает письмо на различную тематику(акции, розыгрыши, выигрыш денежных средств, блокировка карты), при этом получателю предлагают перейти по указанной ссылке, в которой ввести реквизиты карты, либо отправить данные карты ответным письмом.

Кража данных с помощью вирусов и троянских программ – вид интернет-мошенничества, который реализуется с помощью внедрения на персональные компьютеры или мобильные устройства пользователей вредоносного программного обеспечения (трояны, вирусы и.т.п.), которые перехватывают реквизиты карты, вводимые держателем при интернет-расчете.

Хаккерский взлом баз данных интернет-сайтов с целью получения реквизитов платежных карт.

Меры безопасности при проведении интернет-расчетов:

- Не используйте для оплаты в сети интернет карты, на которых находятся крупные суммы;
- Используйте для осуществления покупок только защищенные сайты, которые начинаются с https:// и отмечены изображением закрытого замочка возле адресной строки сайта;
- Поддерживайте в рабочем состоянии антивирусную базу вашего компьютера, смартфона, с помощью которых вы осуществляете операции, регулярно обновляйте антивирусную базу и проверяйте устройства на наличие вредоносного программного обеспечения;
- Не переходите по нехарактерным для сайта ссылкам, не открывайте прикрепленные к ним файлы, не отвечайте на подозрительные электронные письма, SMS-сообщения и т.д.;
- Никогда не вводите ПИН-код при совершении расчетов в сети интернет. Для данного типа операций ввод ПИН-кода не требуется.

- В том случае, если Вы планируете на постоянной основе проводить операции в сети интернет, рекомендуем открыть платежную карту Visa Virtuon, которая предназначена только для операций в интернете. Пользуясь надежно защищенным ресурсом дистанционного управления счетами Интернет-банкинг Акционерного банка “Пивденный”, Вы можете перечислить на данную карту сумму, необходимую для совершения онлайн-покупки, что исключит возможность мошеннического хищения средств с вашего счета;
- Подключите вашу карту к услуге 3-D Secure! Данная технология была разработана платежными системами для обеспечения дополнительной безопасности при проведении интернет-платежей. После подключения данной услуги в процессе оплаты, кроме реквизитов карты, вводимых держателем на сайте, добавляется запрос на подтверждение владения картой – одноразовый код, который отправляется банком в SMS-сообщении, на заранее привязанный к карте номер телефона. Данная услуга позволяет минимизировать мошенничество в сети интернет. Подключить услугу 3D Secure вы можете в любом банкомате Акционерного банка «Пивденный».

4. Мошенничество в торгово-сервисной сети.

Мошенничество в торгово-сервисной сети в основном представляет собой переписывание реквизитов платежной карты или намеренное списание со счета большей суммы, чем та, которая подлежит оплате. Встречаются также случаи считывания данных с магнитной полосы, с помощью установки скиммингового устройства на платежном терминале, - данный тип мошенничества не распространен в Украине, однако за границей иногда встречается.

Меры безопасности при проведении расчетов в торгово-сервисной сети:

При проведении операций контролируйте манипуляции работников торгово-сервисного предприятия, не позволяйте переписывать карточные реквизиты под любым предлогом или уносить карту вне зоны видимости.

Перед тем как подписать чек, внимательно проверьте сумму операции, валюту, номер карты, указанный в чеке. В случае указания неверной суммы требуйте от кассира провести отмену операции и получите чек отмены (кредитовый слип).

Если Вы планируете поездку за границу с вероятным использованием карты в торгово-сервисной сети страны следования, пожалуйста сообщите об этом в круглосуточную службу поддержки Акционерного банка “Пивденный” по номеру телефона 0800-30-70-30.

Акционерный банк “Пивденный”

СПАСИБО ЗА ВНИМАНИЕ!