



02.01.2015

Предотвращение мошенничества и обеспечение безопасности

Риск мошенничества является реальным при использовании банковских продуктов. Тем не менее, следуя нескольким простым правилам безопасного банкинга, вы можете избежать возможной ситуации мошенничества.

Имея счёт в банке и став жертвой мошенничества, вы сможете обратиться, чтобы получить свои деньги обратно, если вы следовали положениям и условиям вашего банка. Эти условия определяются практикой банковской безопасности и включают сообщения о потере или краже карты, и/или сообщение о мошеннической деятельности, как только вы это осознали.

Безопасное использование платёжных карт



Когда вы получите карту банка, сразу подпишитесь на её обороте в месте подписания.

Держите записи реквизитов карты в надёжном месте. Не давайте свою карту для использования другим лицам, в том числе членам семьи. Храните карту в условиях, исключающих повреждение, потерю, кражу или хищение данных, содержащихся на ней. Внимательно прочитайте правила и условия / контракт, которые сопровождают дебетовую карту, и соблюдайте их. Никогда и никому не сообщайте ваш PIN-код, CVV2 или другие пароли, в том числе сотрудникам банка. Если вы записываете свой личный идентификационный код (PIN-код), не держите его вместе с платёжной картой. Убедитесь, что у вас есть контактный телефон вашего банка, чтобы иметь возможность немедленно известить его в случае если ваша карта будет утеряна или похищена.

Банк имеет круглосуточный центр поддержки, для того, чтобы клиент имел возможность сообщить о потере или краже карты, как только он осознает это. Банк немедленно заблокирует вашу карту, и вы избежите таким образом последующие потери с вашего счета.

Вы можете в вашем банке установить на своём счёте максимальный суточный лимит по снятию средств, который поможет уменьшить потери на вашем счёте в случае, если карта и PIN будут похищены.

Сверяйте выписки с банкоматов и квитанции на покупку полученные в магазинах с выпиской по счёту. Если вы подозреваете наличие какой-либо мошеннической деятельности, связанной с использованием вашего счёта, обратитесь в свой банк немедленно.

Суммарный перечень советов по безопасному использованию платёжной карты:

- Берегите вашу платёжную карту. Всегда знайте, где она находится; если вы её потеряли, сообщите в банк об этом как можно скорее.
- Рекомендуется чтобы PIN-код вашей платёжной карты, отличался от вашего адреса,
- номера телефона, номера социального страхования или даты рождения. Это затруднит похитителю использование вашей карты. Некоторые банки предоставляют возможность самостоятельной смены владельцем карты своего PIN-кода посредством банкоматов.
- Сохраняйте и проверяйте квитанции для всех видов операций с вашими выписками со счёта, для того

чтобы вы смогли обнаружить ошибки или несанкционированные переводы и сообщать о них.

- Убедитесь, что вы знаете и доверяете продавцу или компании, прежде чем поделиться какой-либо информацией о банковском счёте или дать предварительное согласие на списание средств с вашего счета.
- Каждый месяц безотлагательно и внимательно изучите выписку по своему счету. При обнаружении несанкционированных операций или ошибок немедленно свяжитесь с банком или другим соответствующим финансовым учреждением.

Безопасное использование банкоматов



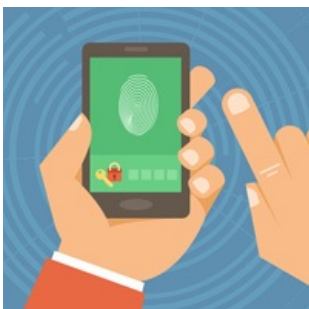
Убедитесь, что никто не может увидеть PIN-код, который вы вводите. Проверьте, если на банкомате не установлены какие-то необычные устройства/оборудование. Если что-то окажется не так, следует немедленно связаться с банком. Если во время транзакции, ваша карта застряла в банкомате, не отдаляйтесь от банкомата и позвоните в банк. Если вы находитесь у банкомата в нерабочее время, позвоните в службу 24-часовой поддержки вашего банка по поводу потерянных или украденных карт. Банк немедленно заблокирует все операции по вашей карте, чтобы избежать потери средств вследствие потенциального мошенничества. Не позволяйте себе отвлекаться или принимать «помощь» посторонних. Эти люди могут попытаться завладеть вашей картой и PIN-кодом.

Безопасные платежи банковскими картами в магазинах, ресторанах и других пунктах розничных продаж

При вводе своего PIN-кода не позволяйте никому видеть цифры, которые вы набираете. Несмотря на то, что новые технологии значительно уменьшили возможность копировать информацию с вашей карты (известную, как скимминг), соблюдайте следующие меры предосторожности, чтобы предотвратить любую возможность дублирования вашей карты:

- Держите вашу карту всегда в поле зрения. Например, если официант хочет унести вашу карту, чтобы инициировать транзакцию в другом месте, сопроводите официанта к этому месту.
- Не позволяйте проводить вашей картой более чем по одному считывающему устройству в одной точке продажи. Если устройство не работает, появится сообщение и/или распечатка, что операция или соединение не удалось.
- При покупках в интернет-магазинах, проверьте наличие защитных символов 3Dsecure, обычно размещённые на нижней части веб-сайта продавца. При покупках по интернету не требуется вводить PIN-код вашей платёжной карты, поэтому не вводите свой PIN-код на каких-либо веб-сайтах.

Безопасное использование интернет-банкинга.



С большой долей вероятности компьютерные системы вашего банка будут достаточно безопасными, но вы должны защитить себя и свой банковский счёт от внешних воздействий при проведении операций посредством интернет-банкинга. Избегайте использования общественных терминалов (например, в библиотеках или интернет-кафе) для электронного банкинга. Если все-таки вам приходится использовать

общественный терминал, убедитесь, что никто не может видеть, как вы вводите своё имя пользователя и пароль при входе в систему, и убедитесь, что вы правильно вышли из системы в конце вашей сессии. Рекомендуем менять свой пароль после пользования интернет-банкингом с помощью общественного терминала.

Проводите свои электронные банковские операции, используя беспроводной доступ, только если вы уверены в неприкосновенности соединения, так как есть высокий риск перехвата во время беспроводной связи.

Убедитесь, что у вас есть современные антивирусные и антишпионские программы для защиты от мошенников. Этот тип программного обеспечения защитит вас от вирусов, а также от риска дистанционного хищения ваших паролей или личной информации во время интернет-банкинга.

Перед входом в интернет-банк закройте другие веб-сайты.

Заходите сразу на сайт вашего банка, а не через ссылку, например, поисковой системы или электронной почты. Введите адрес в адресной строке браузера, или сохраните ссылку на веб-сайт банка в избранном. Никогда не переходите по ссылке на сайт, который запрашивает изменение вашего пароля или предоставление информации о вашем банковском счёте. Вероятнее всего, это мошенничество. Вашему банку не требуется подтверждения ваших данных.

Все сайты, которые предлагают электронные средства оплаты, такие как банки и интернет-магазины, имеют веб-ресурсы, которые начинаются с <https://>. Присутствие «s» в <https://> информирует вас о безопасности веб-сайта. Убедитесь, что ваш веб-браузер отмечен значком закрытого замка, который также указывает на безопасность веб-сайта. Вы можете кликнуть на этот значок для подтверждения владельца сайта.

Выберите надёжный пароль, который нельзя угадать легко. Постарайтесь, чтобы в пароле присутствовало, как минимум, восемь знаков, в том числе буквы, цифры и символы, такие как восклицательный знак или решетка. Регулярно меняйте свой пароль.

Никогда и никому не передавайте ваш пароль доступа интернет-банкинга, в том числе банковским работникам. По окончании операций через интернет-банкинг, выйдите из системы и закройте окно браузера. Если вы заметили какое-либо мошенничество или другую подозрительную активность, сообщите об этом в свой банк.

Метки

[риск](#) ^[1]

[мошенничество](#) ^[2]

[Предотвращение мошенничества](#) ^[3]

[советы](#) ^[4]

[Советы использование банковских карточек](#) ^[5]

[Безопасное использование интернет-банкинга](#) ^[6]

[Безопасное использование платёжных карт](#) ^[7]

[кампания по продвижению безналичных расчётов](#) ^[8]

[безналичные расчёты](#) ^[9]

[кампания](#) ^[10]

Источник УРЛ:

<http://bnm.md/ru/content/predotvrashchenie-moshennichestva-i-obespechenie-bezopasnosti>

Ссылки по теме:

[1] [http://bnm.md/ru/search?hashtags\[0\]=риск](http://bnm.md/ru/search?hashtags[0]=риск) [2] [http://bnm.md/ru/search?hashtags\[0\]=мошенничество](http://bnm.md/ru/search?hashtags[0]=мошенничество) [3]

[http://bnm.md/ru/search?hashtags\[0\]=Предотвращение мошенничества](http://bnm.md/ru/search?hashtags[0]=Предотвращение мошенничества) [4] <http://bnm.md/ru/search?>

[hashtags\[0\]=советы](http://bnm.md/ru/search?hashtags[0]=советы) [5] [http://bnm.md/ru/search?hashtags\[0\]=Советы использование банковских карточек](http://bnm.md/ru/search?hashtags[0]=Советы использование банковских карточек) [6]

[http://bnm.md/ru/search?hashtags\[0\]=Безопасное использование интернет-банкинга](http://bnm.md/ru/search?hashtags[0]=Безопасное использование интернет-банкинга) [7] <http://bnm.md/ru/search?>

[hashtags\[0\]=Безопасное использование платёжных карт](http://bnm.md/ru/search?hashtags[0]=Безопасное использование платёжных карт) [8] [http://bnm.md/ru/search?hashtags\[0\]=кампания по](http://bnm.md/ru/search?hashtags[0]=кампания по)

продвижению безналичных расчётов [9] [http://bnm.md/ru/search?hashtags\[0\]=безналичные расчёты](http://bnm.md/ru/search?hashtags[0]=безналичные%20расчёты) [10]
[http://bnm.md/ru/search?hashtags\[0\]=кампания](http://bnm.md/ru/search?hashtags[0]=кампания)