

Памятка

«О рекомендациях по безопасному использованию пластиковых карт и мобильного приложения банка»

Общие рекомендации

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.
4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
6. Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
7. С целью предотвращения неправомерных действий по снятию денежных средств с банковского счета целесообразно использовать электронную услугу оповещения посредством SMS-сообщений или push-уведомлений.
8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
10. В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в кредитной организации - эмитенте банковской карты.
11. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

Рекомендации при совершении операций с банковской картой в банкомате

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.
3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.
5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.
8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата банковской карты.
9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.
10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
4. В случае если при попытке оплаты банковской картой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
 2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.
 3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.
 4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
 5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
 6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или) информации о банковской(ом) карте (счете).
- В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

Рекомендации при использовании мобильного приложения банка

1. Не сообщайте другим лицам Ваш логин, пароль доступа к мобильному приложению, а также коды подтверждения, полученные в SMS.
- Необходимо запомнить Ваш логин, пароль доступа к мобильному приложению или в случае, если это является затруднительным, хранить их в неявном виде (чтобы нельзя было понять, что это данные от входа в мобильное приложение банка) и недоступном для третьих лиц, в том числе родственников, месте.
2. Скачивайте мобильное приложение банка только из официальных источников, таких как GooglePlay, AppStore, для входа в официальный магазин GooglePlay, AppStore не используйте внешние ссылки с других ресурсов, вход осуществляйте только через иконку магазина в мобильном телефоне.
 3. Избегайте на своем мобильном устройстве настроек типа root и jailbreak, использование данных настроек сделает Ваш телефон более уязвимым к заражению вирусными программами.
 4. Не посещайте с мобильного телефона интернет-сайты сомнительного содержания. Не открывайте с мобильного телефона неизвестные файлы, присланные на e-mail или через социальные сети, а также не открывайте сомнительные ссылки. Мошенники могут заразить Ваш телефон вирусом и украсть Ваши данные.
 5. Проверяйте реквизиты, которые указаны в СМС, получаемых от Банка при совершении переводов и платежей.
 6. При установке приложений на телефон обращайте внимание на полномочия, которые они запрашивают. Будьте осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к интернету — оно может быть опасным, лучше не устанавливайте его.
 7. Не устанавливайте на мобильное устройство какие-либо программы по просьбе 3-х лиц. Не давайте прав удаленного доступа к мобильному устройству.
 8. Регулярно обновляйте установленное программное обеспечение.

Основные признаки телефонного мошенничества

Мошеннических схем много и регулярно появляются новые. Чтобы не стать жертвой обмана, полезнее знать не столько сами схемы, сколько ключевые признаки того, что Вы столкнулись с мошенником. В таком случае меньше шансов остаться без денег.

По статистике в четырех из пяти случаев мошенничества клиенты банков теряют свои деньги не из-за хакерской атаки, а из-за того, что сами их отдают или сообщают мошенникам реквизиты карт. Обычно мошенники выуживают номер и срок действия карты, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций. То есть киберпреступники – это по большей части не столько хакеры, сколько психологи, которые «взламывают» не компьютер (ноутбук, телефон, планшет и другое), а сознание своей жертвы.

По каким же признакам можно распознать мошенников?

1. На Вас выходят сами

Кто-то сам Вам звонит (пишет письмо, присылает ссылку и так далее). Вне зависимости от того, кем он представляется, – сотрудником банка, полиции, магазина, богатым родственником – и чего он хочет, надо быть осторожным. Помните: если кто-то незнакомый звонит вам, значит ему что-то нужно. Вопрос: что?

2. Разговор касается денег или Вашей банковской карты

Важно помнить, что у мошенников единственная цель – Ваши деньги. Ключ к ним – банковская карта. Мошенники либо вынуждают человека самого отдать деньги, либо выуживают у него информацию (например, данные карты), которая позволит эти деньги украсть. Если Вас просят перевести деньги на некий счет, вернуть ошибочно/случайно перечисленные Вам средства, заплатить налог, брешь, штраф, внести залог, аванс или совершить другие действия, связанные с денежным переводом или раскрытием данных карты, – будьте бдительны, возможно, это мошенники.

3. Делают супервыгодное предложение или пугают

Вам делают супервыгодное предложение: щедрые выплаты, призы, невероятно привлекательные условия по кредитам и депозитам, инвестиционные продукты, обещающие огромную доходность. При этом Вас убеждают, что нельзя упускать шанс получить сразу много денег, надо обязательно использовать уникальную возможность. Противоположная схема – Вас пытаются запугать: деньги вот-вот украдут, спишут со счета, Вы лишитесь потенциального дохода.

Имейте в виду, что у мошенников всегда заготовлены ответы на возможные вопросы. Поэтому даже не пытайтесь вступать с ними в беседу, ведь чем дольше Вы беседуете, тем крепче Вас «подсаживают на крючок».

Помните, если Вам обещают многое, требуя взамен малое, то Вы лишитесь либо малого, либо всего, что есть на карте, но так и не получите ничего взамен.

4. Морально давят, требуют принять решение немедленно

Мошенники работают с большим количеством людей. Им некогда долго возиться с каждым в отдельности. Кроме того, их задача – не дать жертве опомниться. Поэтому они всегда требуют от человека быстрого принятия решений, действуют уверенно и агрессивно. Если Вы чувствуете, что на Вас давят, угрожают, ставят условие сделать покупку, совершить транзакцию «либо сейчас, либо никогда» – прерывайте общение. Это точно мошенники.

5. Запрашивают информацию о банковской карте

Банки обязаны отслеживать подозрительные операции со счетами своих клиентов. Если у банка возникает подозрение, что совершается несанкционированная операция, его представитель может связаться с владельцем счета и уточнить, действительно ли он совершает эту операцию. Владелец счета должен только подтвердить или не подтвердить операцию – на этом общение заканчивается. Мошенники же начинают выуживать разные данные: коды из СМС, номер карты, трехзначный код на ее обратной стороне, ПИН-код и так далее. Важно помнить, что настоящий сотрудник банка никогда и ни при каких обстоятельствах не будет запрашивать у человека данные его карты. Если кто-то пытается это сделать, прервите разговор – Вы общаетесь с мошенником.

Если Вы будете всегда помнить об этих признаках, то вне зависимости от хитрости и новизны мошеннической схемы, не попадете в расставленные сети. Важно понимать, что каждый из этих признаков в отдельности не является однозначным доказательством того, что с Вами говорят мошенники (кроме случаев, когда у Вас запрашивают трехзначный код на обратной стороне банковской карты, ПИН-код или код из СМС). Но чем больше таких признаков, тем больше вероятность того, что Вас пытаются обмануть.

Если после разговора с незнакомцем у Вас возникли какие-то сомнения или вопросы, перезвоните в свой банк по номеру телефона, указанному на его сайте или банковской карте, и уточните интересующую Вас информацию.