Приложение

Методические материалы для обучающихся общеобразовательных школ по вопросам безопасности при обороте банковских карт

Уважаемые педагоги! Сегодня можно с уверенностью сказать, что банковские карты наконец-то вошли в нашу жизнь. Причем пользуются ими не только взрослые, но и, зачастую, дети. Поэтому необходимо ознакомить учащихся с основными правилами безопасности при пользовании различными банковскими картами.

Соблюдение несложных правил безопасности, содержащихся в Методических рекомендациях, позволит обеспечить максимальную сохранность банковской карты, её реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации

1. 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. Начнем мы, пожалуй, с того, что нужно делать сразу после получения карты. Итак, вы пришли домой и вскрыли конверт, выданный вам в банке. Что дальше? Первым делом необходимо запомнить секретный PIN-код. Именно запомнить, а не записать его на бумажку или на карту! Впрочем, если вы не надеетесь на свою память, то можете просто спрятать содержимое конверта куда-нибудь подальше. В этом случае, если вы забудете пароль, то сможете просто достать его и посмотреть нужную информацию. Следующий шаг - записать номер своей карты и экстренный телефон банка или платежной системы на отдельный листочек, после чего уберите его в какое-либо место (например, положите вместе с документами). Это пригодится в том случае, если карта будет украдена. Ведь чем быстрее вы сможете позвонить в банк и заблокировать свой счет, тем меньше шансов у злоумышленника воспользоваться ворованным. Именно поэтому нужно знать номер телефона, которым можно воспользоваться в экстренных случаях

2. При получении банковской карты распишитесь на её оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае её утраты. Далеко не все карты предполагают нанесение на них подписи владельца. Обычно это верно только в отношении карт международных платежных систем. Для чего это вообще нужно? Да для защиты ваших денег. Давайте предположим, что карта была украдена и злоумышленник пришел с ней в магазин за покупками. Увидев подпись на карте, кассир может потребовать от мошенника роспись, чтобы убедиться в его праве распоряжаться деньгами. Правда, у нас это делают редко. Исключением являются организации, кассы которых не оборудованы POS-терминалами. В этом случае покупатель должен расписаться на слипах (чеках), а кассир обязан сравнить эту подпись с образцом на карте.

3. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.

Нельзя носить с собой листочек с записанным PIN-кодом и не наносить эти данные на обратную сторону карты. Подумайте сами, чем грозит невыполнение этого простого условия. PIN-код - это пароль доступа к вашим деньгам. Зная его и имея карту, можно снять с нее все деньги, спокойно расплачиваться с ее помощью за покупки в магазинах и т.д. А теперь давайте представим, что карманник вытащил у вас кошелек. Найдя в нем банковскую карту и не зная пароля для доступа

к операциям с ней, он просто-напросто выкинет ее в ближайшую урну. Естественно, в этом случае вам придется заплатить в банк за изготовление новой карты, однако деньги на счету будут целы. Ну а что будет, если карманник вместе с картой обнаружит и листочек с PIN-кодом? Естественно, он тут же пройдет к ближайшему банкомату и... В общем, понятно, что сделает злоумышленник и чего лишится владелец карты.

Во многих случаях это правило распространяется и на номера банковских карт. Возьмем для примера любую международную платежную систему. Зная только номер карты и срок окончания ее действия, можно оплачивать покупки в интернет-магазинах или заказывать любые услуги через Глобальную сеть. Таким образом, листок с номером карты (который мы записали для незамедлительных действий в экстренных случаях) лучше не носить с собой, а хранить в надежном месте.

4. 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.

На первый взгляд это совершенно очевидно. И действительно, никто не будет отдавать карту малознакомым лицам или людям, которым человек не доверяет. Однако мало кто учитывает, что это правило стоит распространять на всех, в том числе и на членов своей семьи. И дело здесь не в том, что последние попытаются обмануть владельца карты. Просто родственники могут оказаться менее сведущими в области безопасности и стать жертвами мошенников. Кроме того, в случае возникновения непредвиденных ситуаций они не смогут доказать свое право пользования картой. Ведь даже в магазине кассир может попросить подтвердить личность владельца документами или подписью. И это не говоря уже о ситуациях, когда карта по тем или иным причинам оказалась задержанной банкоматом. В этих случаях получить ее назад может только владелец.

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.

Одним из излюбленных приемов мошенников является вытягивание из жертвы номера его карты и PIN-кода к нему по телефону. Делается это следующим образом. Сначала злоумышленник узнает телефонный номер и полные фамилию, имя и отчество жертвы, а также название банка-эмитента, выпустившего его карту. Затем он звонит ему и представляется сотрудником этой организации. Знание имени и отчества человека, а также упоминание его банка обычно притупляет осторожность жертвы. Ну а дальше мошенник просит собеседника немедленно сообщить ему номер его карты и PIN-код для доступа к ней. При этом звучат такие причины, как "компьютерный сбой банковской системы и необходимость восстановления базы данных", "победа в лотерее, проводимой нашим банком", и т.п. Некоторые идут еще дальше. Они представляются сотрудниками служб безопасности и утверждают, что картой человека воспользовался злоумышленник, которого только что поймали. И чтобы возместить убытки, понесенные владельцем, необходим PIN-код. О том, что происходит после того, как человек сообщит мошенникам секретные данные о своей карте, наверное, рассказывать не стоит.

Поэтому достаточно запомнить одну вещь. Никто и ни при каких обстоятельствах не может требовать от вас номер карты или PIN-код для доступа к ней. Это правило распространяется абсолютно на всех: на работников банка, на сотрудников правоохранительных органов, на обслуживающий персонал банкоматов и т. д. Некоторые источники утверждают, что владелец карты может сообщить PIN-код милиционерам или работникам прокуратуры по решению суда. Однако на самом деле это не так. Сотрудники правоохранительных органов, имея на руках постановление суда, обратятся прямо в банк, откуда смогут проследить все операции с данной картой, а также заблокировать нужный счет. А поэтому помните, что из третьего правила

безопасности не существует абсолютно никаких исключений.

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 всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

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.). Первое и самое главное, что необходимо учитывать тогда, когда вы хотите снять деньги со своей карты, - это выбор банкомата и времени транзакции. Точнее, даже не самого банкомата, а его расположения. Дело в том, что желательно избегать безлюдных или, наоборот, слишком шумных мест. В первом случае вас легко могут

подкараулить самые обычные грабители. А еще вид человека, вынимающего купюры из банкомата на пустынной улице, может оказаться слишком большим соблазном, например, для компании подвыпившей молодежи. Такой опасностью нельзя пренебрегать. Ну а если банкомат расположен в слишком людном месте, то владельцы карты подвергаются другой угрозе. Ведь в этом случае человек не может быть уверен в том, что никто не смог подсмотреть PIN-код, который он ввел

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. Соблюдайте правило - никому не доверяйте около банкомата. Часто бывает, что люди, мало работавшие до этого момента с банковской картой, путаются. И тут же может найтись "доброжелатель", который все объяснит, поможет выполнить нужное действие. А при этом еще и запомнит PIN-код, который вводил владелец. Вроде бы, все хорошо и прекрасно. Однако через некоторое время человек обнаруживает, что его карта пропала. Ну а в банк обращаться уже поздно - злоумышленник, зная пароль, может очень быстро снять все деньги со счета владельца. Конечно же, нельзя утверждать, что каждый человек, предлагающий свою помощь, - преступник. Тем не менее вероятность наткнуться на мошенника вполне реальна, и ей лучше не пренебрегать.

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 её 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.

13. Закончив работу, необходимо проверить, все ли вы забрали из банкомата. Обычно на руках у человека должны остаться три вещи: сама карта, выписка о проведенной операции и снятые со счета деньги. Причем последние две вещи не обязательны. Обычно клиент сам может отказаться от выписки, а проведенная операция не обязательно должна быть связана со снятием наличности. Ну а если чего-то из приведенного списка не хватает, то банкомат покажет на экране соответствующее сообщение, например, о задержке карты по определенной причине. Если же этого не произошло, то нужно немедленно обращаться в банк (лучше всего позвонить, не отходя от банкомата). Ведь в этом случае вы рискуете стать жертвой мошенников.

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 её 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.