Банк России

ЗНАНИЕ – СИЛА: ЗАЩИТИ СЕБЯ И БЛИЗКИХ ОТ МОШЕННИЧЕСТВА НА ФИНАНСОВЫХ РЫНКАХ

Мошенничество в разных сферах нашей жизни присутствовало всегда, и сегодня оно приобретает новые формы, что во многом обусловлено появлением и развитием финансовых технологий. Как защититься от угроз современного финансового рынка, как распознать их и что они из себя представляют — вот основные вопросы, которые предлагается рассмотреть ниже.

Взяв за принцип известное латинское изречение «Praemonitus, praemunitus» («Предупрежден, значит, вооружен»), вооружимся знаниями по финансовой грамотности и таким образом не только оставим мошенников ни с чем, но и научим, как не попасться к ним на удочку, своих родных, друзей и знакомых.

Чаще всего мошенники обнаруживают себя в момент нашего взаимодействия с банкоматом, при совершении покупок, оплаты услуг в интернете, при получении фишинговых рассылок или в более сложных ситуациях — когда происходит утечка конфиденциальной информации, например из-за незащищенного соединения в сети.

Рассмотрим наиболее распространенные мошеннические схемы и выявим правила безопасного финансового поведения.

БАНКОМАТ: ПРАВИЛА ОСТОРОЖНОГО ИСПОЛЬЗОВАНИЯ

Банкоматы бывают адаптированными (доступными) и неадаптированными. Адаптированный (доступный) банкомат — это устройство для обслуживания людей с инвалидностью или ограничениями по здоровью. Такие банкоматы могут отличаться размерами, наличием особого программного обеспечения или, например, специальным аудиоразъемом, в момент использования которого банкомат переходит в специальный режим для работы с незрячими держателями карт.

Однако такие банкоматы расположены не везде. С одной стороны, адаптированный банкомат — это необходимость, и попытки найти его для совершения операций понятны и оправданы. С другой стороны, нельзя забывать о безопасности, ведь расположение банкомата имеет очень важное значение. Например, для незрячего клиента выбор между доступным банкоматом, находящимся на улице, и неадаптированным в офисе банка — неоднозначен. Нельзя забывать, что использовать банкомат на улице более рискованно, чем в офисе банка. Если банкомат не адаптирован — попросите помочь вам сотрудника банка, полицейского, другое должностное лицо или знакомого, которому вы доверяете.

При использовании банкомата не забывайте и о других правилах безопасности. Помните, что ПИН-код необходимо держать в тайне, его никогда нельзя сообщать третьим лицам, и поэтому безопаснее использовать те банкоматы, расположение которых не позволяет посторонним людям находиться рядом с вами. При вводе ПИН-кода всегда прикрывайте клавиатуру рукой. Клавиатура банкомата оснащена тактильными метками, что позволяет незрячим пользователям вводить ПИН-код без посторонней помощи. Такие метки чаще всего представляют собой выступы на кнопках, соответствующих цифре 5, клавишам ввода, коррекции и отмены. В некоторых случаях на клавиатуру банкомата наносится шрифт Брайля.

Транзакции, подтвержденные ПИН-кодом, оспорить очень трудно, поскольку по условиям договора, заключаемого с банком при получении платежной карты, ПИН-код не должен знать никто, кроме владельца карты. Если вам нужно снять наличные, но вы испытываете затруднения, не передавайте свою карту и ПИН-код к ней третьим лицам, лучше переведите нужную сумму на карту тому, кому вы доверяете и кто готов вам помочь, попросив этого человека снять для вас наличные. При обращении за помощью соблюдайте осторожность, не прибегайте к услугам, если вам предложили их без вашей просьбы непосредственно у банкомата. Возможно это обычные неравнодушные граждане, но для обеспечения собственной безопасности лучше от такой помощи отказаться.

Будьте внимательны при завершении операций с банкоматом — по окончании операции можно услышать характерный щелчок, свидетельствующий о том, что банкомат вернул вам карту, — заберите карту сразу же, как услышите его, иначе через 30-40 секунд банкомат в целях безопасности захватит карту обратно. Деньги, выдаваемые банкоматом через презентер (отверстие для выдачи наличных), тоже будут доступны в среднем около 30 секунд, по истечении которых банкомат заберет банкноты обратно в так называемую реджект-кассету, которую вынимают из банкомата только при инкассации. Процесс возврата денег может растянуться на несколько дней. В случае, если вы попали в такую ситуацию, немедленно позвоните или лично обратитесь в банк, изложите суть своей проблемы и следуйте инструкциям оператора. Скорее всего, вас попросят написать заявление: от руки или в системе мобильного/интернетбанка. Не переживайте: карту вам если и не вернут, то перевыпустят, а деньги зачислят на счет вскоре после инкассации и пересчета наличных в банкомате.

Случается, что банкомат, издав характерные звуки, не выдет наличных. Обычно так бывает, если в банкомате закончились деньги вообще или купюры необходимого достоинства. В этом случае деньги не списываются со счета. Если же вы получили СМС-сообщение о списании средств, то, как правило, через несколько секунд вам придет сообщение об отмене операции и деньги вернутся на ваш счет.

Однако существует и другая причина, и связана она с мошенническими операциями. В этом случае злоумышленники блокируют окно выдачи денег (диспенсер) с помощью скотча или различных вилок/рогатин. Банкомат может решить, что деньги вам уже выданы и списать их со счета. Такая ситуация встречается редко, но если вы с ней столкнулись — немедленно звоните в банк и следуйте советам оператора.

ОПЛАТА ТОВАРОВ И УСЛУГ ЧЕРЕЗ ИНТЕРНЕТ ИЛИ ДРУГИЕ ДИСТАНЦИОННЫЕ КАНАЛЫ

Если при использовании банкомата или оплате покупок в торговых точках необходима карта или иное бесконтактное устройство платежа (брелок, браслет, телефон), то при дистанционном проведении операций используются данные платежной карты или другого бесконтактного устройства, в связи с чем возникают определенные риски, которых можно избежать или существенно снизить, если следовать правилам безопасности.

Для того чтобы лучше разобраться в них, ответим на вопрос: какие данные платежных карт используются при дистанционной оплате?

Прежде всего это номер карты — от 16 до 19 цифр, срок окончания действия карты и проверочный код (CVC или CVV) — три цифры на обратной стороне карты, расположенные справа от поля для подписи. Как правило, этот код необходим для подтверждения платежа и именно поэтому мошенники пытаются всеми способами узнать его у вас. Причем если номер карты может сохраняться у продавца, то данный код — нет. Помните, что CVV или CVC-код никогда нельзя передавать/называть третьим лицам, никто не имеет права потребовать от вас назвать его, отправить письмом или сообщением. Если же это произошло, значит, вы имеете дело с мошенниками.

Кроме обозначенных реквизитов, многие интернет-магазины запрашивают имя держателя. Эта информация используется исключительно на стороне магазина и по каналам платежной системы от продавца к эмитенту карты не передается. Компания-продавец запрашивает ее в целях собственной безопасности на случай претензий со стороны покупателя. Если система запрашивает ввод имени держателя для оплаты покупки — напишите его, вам это ничем не грозит.

Рост мошенничества в виртуальной области вынудил платежные системы добавить еще одну степень защиты в процесс совершения платежей через интернет, а именно одноразовый пароль (так называемая технология 3DSecure). Такой пароль может быть получен различными способами:

- с помощью скретч-карты — специальной карты со счищаемым слоем;
- с помощью кода, рассчитанного специальным устройством;

- а в подавляющем большинстве случаев с помощью СМС или PUSH-сообщений — одноразовых паролей, направляемых вам банком-эмитентом карты.

Такой пароль необходимо ввести в специальном окне при покупке или совершении платежа через интернет. Так же как ПИН-код, CVV или CVC-код, его нельзя никому и никогда сообщать, поскольку при нормальной процедуре платежа он требуется только для проведения платежа через интернет. Никакие сотрудники банка, Банка России, полиции, любых других организаций и тем более частные лица не имеют права требовать от вас информацию об одноразовых кодах и паролях для подтверждения платежа.

Иногда совершенная вами транзакция может вызвать вопросы у сотрудников службы безопасности банка. В этом случае вам могут позвонить и попросить уточнить информацию о последних проведенных вами операциях по карте. Однако никогда и ни при каких обстоятельствах они не должны просить вас предоставить такую информацию, как номер карты, срок ее действия или тем более CVV или CVC-код и/или одноразовый пароль. Если кто-то под видом сотрудника банка пытается узнать у вас эти сведения, немедленно завершите разговор — вы имеете дело с мошенником.

Важно соблюдать главный принцип: все, что пришло по СМС, предназначено только для вас, и никакие люди по телефону не могут интересоваться этими цифрами. Если кто-то просит вас назвать код или другую секретную информацию, высылаемую вам банком в СМС-сообщении, такие люди — однозначно мошенники.

ФИШИНГ

Фишинг (англ. phishing, от сходного по звучанию английского слова fishing — рыбалка) — один из видов интернет-мошенничества, своеобразная «ловля на живца» с помощью массовых рассылок СМС-сообщений и сообщений по электронной почте якобы от имени популярных компаний или организаций, банков, Банка России и так далее, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих. Целью данного вида мошенничества является получение ваших конфиденциальных данных: логинов, паролей, данных лицевых счетов и банковских карт, ваших документов, одноразовых паролей, получаемых по СМС, ПИН-кодов к картам, CVV или CVC-кодов и другой информации, относящейся к вам и вашим финансам.

Обычно фишинговые рассылки маскируются под сообщения от имени вашего банка, популярных организаций или известных компаний. В текстах таких писем обычно содержится информация о блокировке карты, переводе или зачислении средств, выигрыше в лотерею, а также просьбы обновить или подтвердить верность персональных данных из-за каких-либо проблем

с ними. При письменном или устном общении злоумышленники запрашивают определенные данные либо предлагают пройти по ссылке на страницу фальшивого сайта, внешне неотличимого от настоящего, где просят жертву ввести необходимые им персональные данные. Получение подобной информации злоумышленниками может привести к краже персональных данных или списанию средств с карты.

Для того чтобы не стать жертвой фишинговой атаки, необходимо следовать принципам безопасного поведения в интернете:

- не переходить по ссылкам, присланным в подозрительных или непонятных СМС-сообщениях, сообщениях электронной почты, социальных сетей;
- не загружать вложенные файлы из сообщений, которых вы не ожидали;
- обеспечить надежной защитой свои пароли и никому их не передавать;
- не сообщать никому свои персональные данные — ни по телефону, ни лично, ни в каких-либо сообщениях;
- внимательно проанализировать адрес сайта (URL), на который осуществляется переадресация. Несмотря на то что сайт мошенников часто выглядит очень похожим на настоящий, его URL-адрес в большинстве случаев отличается от оригинального (например, заканчиваться на .com вместо .ru);
- не звонить по телефонам, указанным в подозрительном сообщении. Если у вас есть сомнения — перезвоните в свой банк по телефонам, которые приведены на вашей карте или на сайте банка;
- поддерживайте свой браузер обновленным и своевременно устанавливайте обновления безопасности и антивирусные программы.

ФИНАНСОВАЯ ПИРАМИДА

Финансовая или инвестиционная пирамида — это система обеспечения дохода более ранним инвесторам путем постоянного привлечения денежных средств новых участников. Основатели финансовой пирамиды обещают инвесторам сверхвысокую доходность, однако поддерживать такой уровень доходности длительное время невозможно, особенно при том, что реальной хозяйственно-инвестиционной деятельности пирамида, как правило, не ведет. Это означает, что погашение обязательств перед всеми участниками пирамиды заведомо невыполнимо.

Принципиальным отличием финансовой пирамиды от реального бизнес-проекта является источник выплаты дохода. Если сумма выплат дохода стабильно превышает размер добавленной стоимости, которую обеспечивает данный бизнес, то можно смело говорить о том, что проект является финансовой пирамидой.

Зачастую финансовые пирамиды регистрируются как некие организации, привлекающие средства для финансирования какого-нибудь проекта. В случае если его реальная доходность оказывается ниже обещанных инвесторам доходов или отсутствует вообще, то часть средств, поступивших от новых инвесторов, направляется на выплату дохода. Закономерным итогом такой ситуации является банкротство проекта и убытки последних инвесторов. Собранные средства направляются не на покупку ликвидных высокодоходных активов или развитие бизнеса, а сразу используются для выплат предыдущим участникам, оплату рекламы и дохода организаторов. Чем дольше функционирует пирамида, тем меньше процент возможного возврата средств при ее ликвидации.

МОШЕННИКИ НА ТОРГОВЫХ ОНЛАЙН-ПЛОЩАДКАХ

Сегодня все большей популярностью пользуются различные торговые онлайн-площадки, на которых в том числе и частные лица могут продать или купить как новые, так и бывшие в употреблении товары, а также различные услуги. Такие площадки представляют особый интерес для мошенников. Популярность мошенничества в этой системе объясняется большим количеством пользователей, которые размещают свои объявления.

На этих площадках мошенники работают в основном по нескольким схемам, среди которых можно выделить следующие:

- **Пересылка товара с предоплатой.** Зачастую процесс купли-продажи на сайте проходит между лицами из разных городов. Перед отправкой товара покупатель и продавец договариваются об условиях пересылки необходимого товара. Мошенники же действуют следующим образом: продавец отказывается встречаться с покупателем на удобной территории и требует предоплату за пересылку товара или говорит, что у него есть несколько покупателей и он отдаст товар в случае немедленной предоплаты в размере, например, 10% от суммы на его карту. Покупатель переводит необходимую сумму и остается ни с чем, так как мошенник пропадает и перестает выходить на связь. Поэтому если продавец начинает требовать заплатить ему частичную или полную стоимость товара, игнорируйте это требование, а при настойчивом вымогательстве прекращайте любые контакты. Подобные ситуации легко узнаваемы и, к сожалению, возникают часто. Старайтесь в них не попадать, так как те, кто все же совершит предоплату и не получит обещанный товар, потеряет деньги навсегда.
- **Требование ответить по СМС.** Очень часто мошенники отправляют с неизвестного номера СМС-сообщения различного содержания.

Например, о блокировке объявления за нарушение правил, о наличии откликов на размещенное объявление, просьбы прислать СМС с кодом для отмены блокировки и другие. Таким образом, злоумышленники вынуждают отправить СМС, за которое с вас могут списать крупную сумму. Для уверенности в правомерности подобных требований необходимо обратиться в службу поддержки используемого сайта. Обратите внимание, что некоторые мобильные операторы предоставляют услугу открытия отдельного счета для оплаты различных сервисов, подключение которых снижает риск потерь.

- **Работа с предоплатой.** Одним из распространенных случаев мошенничества является просьба о предоплате за услуги по устройству на работу. Мошенники просят внести определенный взнос за заключение договора, оформление документации, пропуск на территорию, обучающие материалы и так далее. Получив деньги, злоумышленники, естественно, исчезают. Помните! Ни одна организация не берет денег у будущих работников ни до их устройства на работу, ни после. Если вы столкнулись с такими просьбами — скорее всего, вы имеете дело с мошенниками.
- **Передача персональных данных.** Недобросовестные продавцы/покупатели под различными предлогами могут пытаться узнать у вас личные данные, например номер банковской карты и ее ПИН-код, CVV или CVC-код, даже одноразовый СМС-пароль для подтверждения оплаты. Разглашение данной информации третьим лицам может угрожать вашей личной и финансовой безопасности. Если вы хотите быть уверены в защите личных данных и денежных средств, держите сведения о них при себе.

«НИГЕРИЙСКИЕ» ПИСЬМА

«Нигерийские» письма — особый вид высокоорганизованного мошенничества, появившийся почти 40 лет назад и получивший наибольшее распространение с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что широкое распространение данный вид мошенничества получил в Нигерии, причем еще до появления интернета — в то время мошенники действовали с помощью обычной почты. Сегодня «нигерийские» письма можно получить и из других африканских стран, а также из Англии, Голландии, Испании, ОАЭ, США и даже России. Мошенники, как правило, просят у получателя письма помощи в совершении многомиллионных денежных операций, обещая за нее солидные проценты. Это могут быть, например, различные дела по получению адресатом наследства, или просьбы помочь с банковским переводом за границу, или предложения о получении денег с банковского счета умершего клиента, который

по какому-то чудесному совпадению является однофамильцем адресата. Если получатель письма соглашается помочь, у него постепенно выманиваются крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, а потом и штрафы.

Проблема состоит в том, что в данном случае у мошенников все продумано до мелочей: у них есть офисы, работающий факс, собственные сайты, связи с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде.

Несмотря на то что на протяжении многих лет в средствах массовой информации подробно рассказывается о данном виде мошенничества, массовость рассылки приводит к тому, что злоумышленники находят все новые и новые жертвы, которые отдают им крупные суммы денег.

В целом можно выделить общие особенности «нигерийских» писем и любого мошенничества, связанного с выманиванием денег. Во-первых, почти в каждом случае есть ощущение, что все надо делать «срочнейшим образом». Упоминаются форс-мажорные обстоятельства, а в теме письма пишут «срочно, очень срочно». Во-вторых, в большинстве случаев корреспонденция отправляется по факсу или через электронную почту. В-третьих, злоумышленники используют различные ссылки на разного рода документы, печатные издания, законодательные акты, призванные вызвать доверие жертвы. В-четвертых, всячески подчеркивается элитарность, эксклюзивность предлагаемой схемы. Предложение исходит якобы от высокопоставленных чиновников, вдов политических лидеров, различных наследников и так далее. Говорится, что вас как человека очень надежного и честного рекомендовал один ваш знакомый, пожелавший остаться неизвестным. В письмах практически всегда фигурируют большие суммы денег: от 10 до 80 млн $ США. Получателю предлагается сотрудничать за крупный процент (до 30% от общей суммы). Наконец, мошенники акцентируют внимание жертвы на конфиденциальном характере сделки, не скрывая ее нелегитимности. Все это нужно для того, чтобы после успешной аферы пострадавший не побежал жаловаться в полицию из-за страха быть уличенным в незаконных операциях.

Лучший способ избежать неприятностей, связанных с последствиями общения и взаимодействия с подобными мошенниками, — игнорировать их письма, немедленно удаляя без ответа.

ПСЕВДОБРОКЕРЫ И ПСЕВДОДИЛЕРЫ

Мошенники регулярно предлагают клиентам брокерские или дилерские услуги, с помощью которых якобы можно приумножить свой капитал и осуществить высокодоходные инвестиции, не имея при этом никакого отноше-

ния к реальным брокерам и дилерам, а также лицензии на осуществление такой деятельности. Их цель — вынудить клиента перевести им денежные средства.

К основным приемам мошенников можно отнести:

- **Вывод денег через повышение торгового статуса**. Например, клиент зарегистрировался на сайте торговой площадки по бинарным опционам, пополнил свой баланс и получил уведомление о получении «бонусных доходов». Однако для вывода этих денег к нему предъявляют требование о повышении своего торгового статуса, а именно просят внести дополнительную сумму. В итоге клиент вносит все больше и больше средств, но так и не получает возможности вывести свои деньги. Из реальной же брокерской или дилерской компании клиент всегда может вывести свои свободные денежные средства без каких-либо дополнительных вложений.
- **Просьба перевести деньги на карту (или электронный кошелек) третьему лицу.** Запомните, что реальные брокерские или дилерские компании не просят перевести средства на карту третьего лица. Если вы выполните такой перевод, отозвать средства будет уже невозможно.
- **Договор участия в лотерее или договор-пари.** Клиент невнимательно читает договор, который подписывает с якобы брокерской компанией, и когда он пытается получить свои деньги, компания отказывается их вернуть, ссылаясь на договор, где указано, что клиент участвовал в лотерее или пари, причем чаще всего эта информация прописывается мелким шрифтом. Получается, что клиенту «просто не повезло» и он проиграл свои деньги. Для того чтобы избежать такой ситуации, внимательно читайте договоры, которые вы подписываете. При любых сомнениях берите время на более детальное изучение документов и по возможности знакомьтесь с ними в спокойной домашней обстановке, прибегая при необходимости к консультации юриста.

Помните, если деньги переведены в компанию, зарегистрированную на территории другого государства, то споры придется решать в его правовом поле, то есть в другой стране, так как российские законы на эти компании не распространяются. Если случалось так, что вы все-таки перевели деньги на счет компании злоумышленников, банк сможет вернуть их только в случае согласия компании, на что рассчитывать не приходится.

Для того чтобы избежать встречи с мошенниками подобного типа, убедитесь, что у выбранной вами компании есть лицензия на осуществление брокерской или дилерской деятельности. Перечень российских компаний, у которых есть соответствующая лицензия, представлен в Справочнике участников финансового рынка на сайте Банка России. Кроме того, постарайтесь найти отзывы на профильных сайтах/форумах о нужной вам компании и разузнать о реальном опыте взаимодействия с ней.

ОПРОСЫ, КОНКУРСЫ, РАСПРОДАЖИ

Довольно часто в СМС-сообщениях, электронных письмах можно получить предложения пройти опрос/анкетирование с обещанием получить за это гарантированный приз. При ответе на такое сообщение или даже звонок мошенники долго рассказывают о компании, опросе, награде, а потом предлагают клиенту подтвердить свою личность, гражданство, место жительства, предоставив для получения приза определенную личную информацию: чаще всего данные банковской карты. Подвох состоит в том, что злоумышленники под разными предлогами настаивают на списании с карты небольшой денежной суммы, похищая при этом все имеющиеся на ней средства. В другом варианте мошенники просят перевести денежные средства на другую карту в целях подтверждения ее наличия у жертвы или осуществить гарантированный платеж для резервирования товара.

Для того чтобы не стать жертвами таких псевдорозыгрышей, необходимо помнить о том, что настоящие компании, проводящие опросы, не просят перевести им предварительно денежные средства. Любой платеж незнакомой компании или человеку должен быть обоснован.

РАБОТА В СЕТИ И МОШЕННИЧЕСТВО С ДОСТАВКОЙ НА ДОМ

В интернете, а также в различных рассылках можно получить предложения удаленной работы с возможностью высокого заработка. Как правило, в описании вакансии особо подчеркивается, что соискателю не требуются специфические знания, он должен будет пройти обучение, для чего ему надо приобрести специальные материалы либо получить базу данных клиентов. Для этого необходимо немного заплатить за почтовые расходы, подготовку базы данных, обучение или что-то еще и только после этого приступать к работе. Естественно, что после перевода денежных средств мошенники исчезают.

Другой распространенный вариант такого мошенничества можно встретить офлайн. Например, известная фирма расширяет свою сеть и нанимает сотрудников (можно с инвалидностью) для работы на домашнем телефоне. К кандидату приезжает «представитель фирмы» и проводит экзамен, который проходят абсолютно все кандидаты. Перед отъездом он оставляет у соискателя какие-либо вещи: набор образцов продукции, инструкции для общения с клиентами, телефонные справочники и получает за них залог — обычно порядка 1000-5000 рублей. После чего исчезает навсегда.

Настоящие работодатели перед трудоустройством не требуют пройти платное обучение, купить их продукцию, оплатить трудоустройство.

Прежде чем начинать общение с любым работодателем, зайдите на сайт его компании, ознакомьтесь с отзывами о ней, соберите информацию о реальном опыте взаимодействия с этой компанией, используя профильные сайты и/или форумы.

Случается, что злоумышленники маскируются под социальных работников и, приходя под их видом в дом, начинают рассказывать о новом лекарстве для пенсионеров по льготной цене или приборе, улучшающем, скажем, работу сердца. Конечно, его можно приобрести в районном центре социальной защиты, но тогда придется долго ждать, а вам повезло, и вы сейчас же его получите со скидкой 90%, говорят они. Как правило, предлагаемый мошенниками товар не сто́ит запрашиваемых за него денег, зачастую человека склоняют к заключению кредитного договора или даже обворовывают.

Для того чтобы не стать жертвой подобных мошеннических схем, необходимо помнить, что быстрый заработок, легкие большие деньги, ставки по вкладам в 10 раз больше, чем у любого банка, работа без образования и навыков, опросы, лотереи, дешевые лекарства и товары, оказавшиеся внезапно на пороге вашего дома, — очень часто становятся приманками для доверчивых граждан. Не теряйте бдительности и не спешите расставаться с деньгами!

ЗАКЛЮЧЕНИЕ

В заключение, еще раз обратим внимание на правила финансовой безопасности, которые помогут вам защититься от действий мошенников на финансовом рынке.

При совершении любой операции с картой или денежными средствами продумывайте свои действия и учитывайте возможные действия мошенников. Не оставляйте карту без присмотра, не передавайте ее никому и тем более не сообщайте ПИН-код, одноразовые пароли и другую информацию, получаемую вами от банка по телефону, в СМС-сообщениях или по электронной почте, даже своим близким родственникам, не говоря уже о друзьях, знакомых и прочих третьих лицах. Помните, что сотрудник банка не имеет права спрашивать ни номер вашей карты, ни тем более ПИН-код или пароли, пришедшие в СМС-сообщениях. При любых проблемах с картой, сомнениях или подозрениях в ее компрометации срочно связывайтесь с банком-эмитентом по телефонам, указанным на обороте карты или на сайте нужной кредитной организации. Используйте банкоматы, установленные в безопасных местах. Не пренебрегайте компьютерной безопасностью: установите антивирус, не открывайте файлы, ссылки из незнакомых источников.

Осмотрительно используйте публичный Wi-Fi. Не передавайте конфиденциальную информацию (пароли, банковские данные и так далее), по возможности используйте виртуальные частные сети (VPN), подключайтесь только

к тем сайтам, которые используют безопасный протокол (это можно увидеть по наличию https в начале названия сайта в адресной строке браузера).

Обращайте внимание на сообщения браузера о безопасности. Скачивайте только необходимые приложения из известных источников. Официальные интернет-магазины принимают определенные меры для предотвращения распространения вредоносных программ (хотя и не всегда успешно), и вы можете проверить отзывы других пользователей, прежде чем решите установить приложение или если заметите что-то подозрительное. Если вы скачиваете приложение с неофициального сайта и устанавливаете его на свое устройство, вероятность того, что приложение может содержать вредоносные программы, значительно возрастает.

С осторожностью подходите к любым финансовым сервисам, требующим ввода данных вашей карты, счета, персональных данных, адресов, телефонов, особенно если это связано с каким-то выигрышем, промоакциями и прочим.

По вопросам финансовой грамотности:

fingramota@cbr.ru

Сайт Банка России по финансовой грамотности:

fincult.info

Контактный центр Банка России:

8 800 300-30-00

(для бесплатных звонков из регионов России)

Интернет-приемная Банка России:

cbr.ru/reception