Университет старшего поколения

КУРС

Финансовая и правовая грамотность

Пенсионная социальная карта МИР

Как обезопасить себя от действий мошенников с пластиковыми картами

№ 8

Электронные сервисы сегодня активно развиваются. Многие пожилые люди уже регулярно пользуются пластиковыми банковскими картами для оплаты товаров и услуг.

Россия — последняя страна в мире, где сохранились сберегательные книжки и где пенсию приносят на дом. Во всех странах пенсию перечисляют только на карту. Так что впереди у российских пенсионеров только электронные переводы и оплата картами, и к ним надо привыкать.

Карта — это выгодно, удобно и современно. А при необходимых знаниях и небольшой осторожности это еще и безопасно.

В России выпускается своя карта МИР. Это первая российская карта. МИР предназначена для начисления зарплат, а также есть пенсионная карта МИР. Она выдается на 5 лет и начисляется в рублях.

МИР

Карта бесплатна. За годовое обслуживание не берутся деньги.

На карте сохранили ту же процентную ставку, что на сберегательной книжке. Сбербанк предлагает пенсионерам с помощью программы «Спасибо от Сбербанка» зарабатывать бонусы. Даже не имея накоплений на карте, вы сможете зарабатывать себе деньги этой картой. Все операции нужно оплачивать картой — в аптеках, в кафе, в магазинах.

С каждой вашей покупки 0,5 % возвращается вам в виде бонусов.

Один бонус равен одному рублю. Но нужно открыть счет «Спасибо Сбербанку». На этот счет и будут возвращаться эти бонусы-рубли. Этими бонусами-рублями вы можете расплатиться в «Пятерочке» и в некоторых других местах.

Количество накопленных бонусов можно посмотреть самостоятельно в банкомате Сбербанка. Там есть специальная кнопка «Бонусная программа». Вы вставляете карту в терминал, нажимаете эту кнопку, и вам на экране показывают, сколько бонусов вы накопили.

Бонусы также можно посмотреть в приложении «Сбербанк онлайн». Либо со своего телефона вы можете послать сообщение по программе «Спасибо от Сбербанка», и вам сообщат, сколько у вас бонусов.

С картой МИР вы можете путешествовать по стране и снимать деньги в других городах без комиссии.

Пластиковая карта экономит время.

Сбербанк имеет широкую сеть банкоматов — и в магазинах, и в аптеках, и даже на остановках. Там вы можете круглосуточно снять нужную сумму. Не нужно стоять в очереди или куда-то далеко идти на почту.

Карта позволяет клиентам не возить с собой наличность.

Кошельки воруют, и деньги в кошельке пропадают навсегда. Но украденная карта — уже проблема для преступников. Им нужно подобрать пин-код, а это сложно. К тому же вы сразу можете заблокировать карту, и все деньги там будут сохранены до выпуска новой карты для вас.

Во все отделениях сбербанка дежурят консультанты. Они помогают сориентироваться в новых технологиях.

С пластиковой карты удобно платить коммунальные платежи.

Не нужно искать размен или переплачивать по счету. Вы можете подключить автоплатежи. Это поручение сбербанку вовремя оплачивать коммунальные платежки. Нужно принести квитанцию в сбербанк и указать дату. Накануне автоплатежа вам придет смс «Завтра с вашего счета спишется такая-то сумма за газ». Если вы несогласны, вы можете отменить платеж. Если согласны, то банк сам спишет деньги.

За 30 рублей в месяц можно подключить услугу смс оповещения о хождении денежных средств по вашему счету. Идет контроль за вашими денежными средствами. Если какая-то сумма списана без вашего ведома, вы сразу звоните на 900 и блокируете операцию.

С развитием технологий возрастают и риски, в том числе и риски, связанные с использованием банковских карт

Безусловно, часть механизмов защиты от рисков находятся под контролем банка. Все операции по банковским картам контролируются.

Но абсолютная безопасность возможна только, если клиенты банка тоже будут контролировать свои действия и предпринимать необходимые меры по защите своих финансов. Для этого необходима определенная финансовая грамотность. Клиенты должны знать о потенциальных угрозах при использовании банковских карт, а также о том, какие действия необходимо предпринимать для своей защиты.

Неграмотный пользователь — самая лакомая добыча для мошенников. Грамотный пользователь защищен, поскольку знает, на какие трюки способны пойти мошенники и как не попасть в их ловушку.

Раньше мошенники в основном атаковали банковские сервисы. В настоящее время основные финансовые преступления совершаются против клиентов банка. Доверчивость людей и их низкая финансовая грамотность позволяют мошенникам легко обогащаться.

На что стоит обращать внимание в первую очередь?

Мошенники часто в качестве первого хода используют стрессовое сообщение, то есть пытаются ввести вас в состоянии паники и неспособности думать рационально.

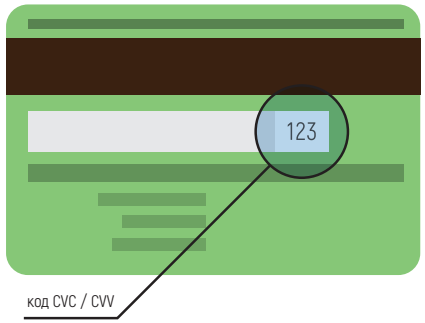
Раздается телефонный звонок или приходит уведомление «от банка» с информацией, что «вашим деньгам грозит опасность!», «ваша карта заблокирована» или «с вашего счета совершен перевод на такую-то сумму».

Это всё относится к методам психологического воздействия. Обычно информация сопровождается уточнением, что времени осталось мало. Вас в состоянии паники загоняют в еще большую панику — у вас мало времени на обдумывание, вам грозит цейтнот, вы должны мгновенно совершать какие-то действия и поступки. В результате пользователь либо сам переводит деньги на счет преступников, либо предоставляет им какую-то важную информацию, в результате которой мошенники могут уже сами снимать деньги с ваших счетов.

При телефонном звонке мошенники могут представляться сотрудниками — службы безопасности, сотрудниками кол-центра, сотрудниками технической службы банка. При этом для большей убедительности они могут обращаться к вам по имени-отчеству, то есть иметь доступ к вашим личным данным. Они могут указать в разговоре ваш адрес или последние цифры вашей карты.

Основная цель мошенников — или заставить вас совершать какие-то действия по карте, или сообщить данные своей карты.

У вас на карте расположена следующая информация: номер карты, имя владельца, срок действия карты и трехзначный CVC-код (три цифры на белом фоне на оборотной стороне карты). При наличии доступа ко всей этой информации в интернете можно совершать платежи с помощью этой карты. Никому из реальных сотрудников банка CVC-код потребоваться не может. НИКОГДА! Этот код нужен только вам и мошенникам.



Как определить, звонит ли вам банк или мошенники? В первую очередь обратите внимание на номер телефона. Сбербанк, к примеру, всегда звонит с номера 900. В редких случаях это может быть номер 8-800-707-00-70. Это очень редкий случай.

Если вы все-таки взяли трубку и с вами, по вашему мнению, говорит сотрудник безопасности, помните, что номер карты и трехзначный код на обороте — это ваша личная информация. И сотрудник банка не может ее спрашивать.

Код, который вам приходит в СМС-сообщениях с номера 900, тоже исключительно ваша личная информация. Ее нельзя сообщать никому!

Этот СМС-пароль означает ваше разрешение на проведение операции с деньгами. Иногда мошенники говорят, что это пароль на отмену операции. Паролей на отмену не бывает! Как только вы сообщили пароль из СМС-кому-то, вы в этот момент разрешили ему переводить деньги с вашего счета. Настоящая служба безопасности может отменить операцию без пароля, им эта информация не нужна. Для блокировки карты тоже не нужны пароли. Служба безопасности банка блокирует карты простым нажатием кнопки. Если у вас по телефону просят пароль из СМС для отмены операции, или блокировки карты, или для чего угодно другого — это мошенники!

Данные карты

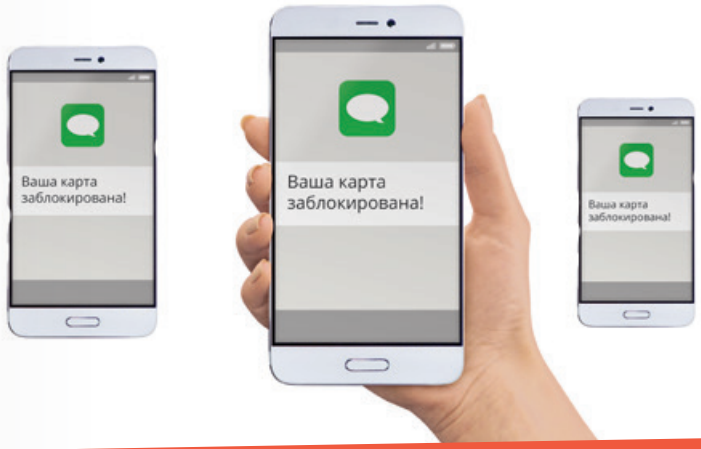
Еще вариант, с которым вы можете столкнуться, — перевести ваши средства на какой-то резервный счет. Мошенники вам предложат якобы «для сохранности денег» перевести деньги временно на какую-то карту или счет в этом или в другом банке. Банки не используют резервные счета! Банк блокирует средства непосредственно на карте.

Любая просьба о переводе на резервный счет — мошенничество!

Просьба об установке на ваш телефон каких-либо приложений — тоже мошенничество. Единственное приложение от банка — это мобильный сбербанк. Если вам звонят и предлагают приложения по улучшенной защите ваших денег, для удаленного управления счетами или для проверки чего-либо от банка — не устанавливайте. Это определенно мошенничество.

Проверяйте номер, с которого вам приходят СМС-сообщения. Сбербанк присылает СМС только с номера 900 и в редких случаях с номера 9000 (когда проверяют качество обслуживания). Никогда СМС от банка не приходят со сторонних номеров.

Мошенники рассылают СМС-сообщения веерно, многим пользователям одновременно, в надежде, что хотя бы часть из получателей поверит и отреагирует. Чаще всего мошенники не владеют информацией, в каком банке вы обслуживаетесь, какой номер вашей карты и пр. Они пишут «Ваша карта VISA заблокирована».



Если у вас есть VISA, вы можете заволноваться и поверить. Мошенники могут рассылать и более конкретные веерные сообщения, например «Ваш счет в ВТБ-банке заблокирован. Срочно перезвоните по номеру XXX-XXX-XX-XX». Да, многие получатели удивятся, глядя на СМС, потому что у них нет счетов в ВТБ-банке. Но те получатели, у которых есть счет в ВТБ, могут попасть в ловушку мошенников. Получатель же не знает, что он один из тысячи получателей СМС. Он уверен, что пишут именно ему.

Сбербанк, когда посылает СМС, обращается адресно. То есть, если вы получили СМС без обращения, это уже серьезный повод насторожиться и считать СМС попыткой вымогательства. Банк всегда указывает последние цифры карты. Мошенники чаще всего не владеют этой информацией. Их задача — выведать всё это в процессе телефонного разговора.

Храните свою карту в недоступном для окружающих месте. Не передавайте свою карту третьему лицу. Вы можете дать свою карту кассиру в магазине, но операция по списанию денег с карты должна проходить при вас. Карта не должна уходить из вашего поля зрения.

Если вы расплачиваетесь картой в магазине и уже собираетесь ввести пин-код, проверьте сумму, которая высветилась на терминале. Если операция по терминалу не прошла (такое случается время от времени), сохраните чек по непройдённой операции. Случается, что неудачная операция через некоторое время все-таки пройдет, и деньги с вашего счета спишутся. Чек вам понадобится для того, чтобы впоследствии обратиться в банк и вернуть себе денежные средства. Иначе у вас может быть двойное списание за один товар или услугу.

Пин-код храните отдельно от банковской карты. Ни в коем случае не пишите пин-код на карте или на листочке, который вы храните рядом с банковской картой. Сейчас можно выбрать пин-код самостоятельно, т.е. подобрать именно те цифры, которые вам проще всего запомнить.

При пользовании банкоматами помните, что наиболее защищенные банкоматы — это те, которые расположены в помещениях банков.

Одиноко стоящие банкоматы и особенно плохо освещенные банкоматы — это угроза. Такие банкоматы привлекают внимание мошенников и могут нести в себе какие-то ловушки.

При пользовании банкоматом всегда прикрывайте рукой пин-код. Сейчас на всех банкоматах Сбербанка появились черные коробочки. Это считыватели бесконтактных карт. Вам не нужно вставлять карту в банкомат, ее достаточно приложить к этому считывателю. Она считывается, вы вводите пин-код и проводите операцию.

Точно так же многие магазины сейчас обзавелись терминалами со считывателем. Вы просто прикладываете карту к терминалу, и нужная сумма списывается с вашего счета. До тысячи рублей пин-код вводить не требуется.

Не пользуйтесь советами третьих лиц при проведении каких-либо операций с банковской картой. Если вам требуется помощь, обратитесь к сотруднику банка или воспользуйтесь номером на обратной стороне карты Сбербанка.

В случае утраты или кражи карты необходимо незамедлительно обратиться в филиал банка либо по номеру 900 и сообщить об утрате или краже карты. Сделать это нужно как можно быстрее. Если вы потеряли карту, а пришли в банк с заявлением только через неделю, то за все операции по карте, проведенные в течение этой недели, вы несете ответственность. Чем быстрее вы заблокируете карту, тем лучше.

Начальник 5-го отдела
УУР ГУМВД России
по Нижегородской области
Артем ФРОЛОВ

На территории Нижегородской области продолжаются мошенничества и кражи. Часто жертвами становятся пенсионеры и люди преклонного возраста. Нередко мошенничество совершается в адрес покупателей товаров через интернет.

1. Если вы захотели что-то купить в интернет-магазине, почитайте отзывы об этом магазине. Часто такие магазины бывают однодневными. Они собирают деньги за какой-то товар и исчезают. Если отзывы плохие или отзывов вообще нет, стоит задуматься, не пытаются ли вас заманить в ловушку.
2. Если нужный вам товар продается по очень заниженной цене — это повод задуматься. Если цена сильно ниже, чем у других интернет-магазинов, и ниже, чем в розничной торговле, стоит насторожиться.
3. Старайтесь избегать случаев предоплаты. Если вы вначале расстаетесь с деньгами, а потом кто-то должен вам привезти товар, это очередной повод насторожиться. Лучше пользоваться магазинами, у которых есть пункты выдачи, куда вы приходите и оплачиваете товар на месте. Бывает даже, что товар вам все-таки приходит по предоплате. Но он может оказаться ненадлежащего качества. Что возвращает нас к пункту № 1 — читайте отзывы об этом магазине, прежде чем решите заплатить им деньги.

Брошюра по материалам лекций

Лекция курса «Финансовая и правовая грамотность».
Тема: «Всё о пластиковых картах (как завести, как использовать и как обезопасить от действия мошенников), выгодные кредиты, оплата услуг через платёжные терминалы»

Дашкова Надежда, Куракина Ксения, *специалисты Сбербанка*

Лекция курса «Финансовая и правовая грамотность».
Тема: «Пластиковые карты.
Как обезопасить себя от действий мошенников с ними»

Артем Петрович Фролов, *подполковник полиции, начальник 5-го отдела Управления уголовного розыска ГУ МВД России по Нижегородской области*

Павлов Евгений Александрович, *гл. специалист отдела экономической безопасности управления безопасности Волго-Вятского банка ПАО Сбербанк*

Брошюра
«Пенсионная социальная карта МИР.
Как обезопасить себя от действий мошенников
с пластиковыми картами»
входит в цикл просветительских материалов, выпускаемых социальным проектом «Университет старшего поколения».

Видеоурок можно посмотреть на сайте проекта
старшеепоколение.рф

Университет старшего поколения

Занятия Университета старшего поколения популярны у нижегородцев. Но не у всех есть возможность посещать очные занятия, поэтому мы решили открыть и дистанционное обучение. Лекторы Университета подготовили материалы по курсам «Компьютерная грамотность», «Правовая и экономическая грамотность», «Психология» и многие другие. Информация подается в формате брошюр и видеоуроков, которые размещены на сайте **старшеепоколение.рф.**

Мы надеемся, что дистанционное обучение поможет сделать полезные занятия более доступными для нижегородцев пожилого возраста.

СТРАТЕГИЯ
НИЖНИЙ
ФОНД

С уважением, руководитель проекта «Университет старшего поколения»
Оксана ДЕКТЕРЕВА

запись по телефону
(831) 233-20-83

информация на сайте
старшеепоколение.рф