Цифровая безопасность личных финансов

Слайд 1. Приветствие

Дорогие друзья!

Цифровая реальность, в которой мы все сегодня живем, уже давно распространила свое действие и на денежные отношения. Технический прогресс облегчает нашу жизнь, упрощает рутинные действия, предлагая нам больше свободного времени для полезных и приятных дел. В настоящее время к нашим услугам – разнообразные банковские и платежные сервисы, которыми мы можем воспользоваться в рамках онлайн-услуг, в интернет-магазинах и т.д. Чтобы пользоваться этим многообразием предложений и функций, человеку надо ориентироваться в них. Кроме того, как и в любой сфере, здесь есть свои правила безопасности, которые совсем несложно соблюдать. Они минимизируют риски быть обманутыми мошенниками, которые пытаются добраться до чужих денег с помощью цифровых технологий.

Что надо делать, чтобы наши деньги в цифровом мире были в сохранности, а жулики остались ни с чем? Чтобы ответить на этот вопрос, надо иметь знания о цифровых услугах, предоставляемых на финансовом рынке, уметь ими пользоваться и обеспечить при этом себе цифровую безопасность. Далее в нашей презентации именно с учетом этих моментов мы рассмотрим самые распространенные финансовые инструменты, которыми большинство из нас пользуется сегодня практически каждый день.

Слайд 2. Банковская платежная карточка

В наше время банковские платежные карточки получили широкое распространение во всем мире. В Беларуси большинство граждан – от ребенка до пенсионера – пользуется этим современным банковским продуктом.

Взрослым людям банки открывают счета для перечисления зарплат, пособий, пенсий и выдают к ним платежные карточки. Дети с 6 до 14 лет могут пользоваться только дополнительными карточками, которые родители выпускают к своему банковскому счету. Открыть свой собственный счет в банке и завести личную карточку можно после 14 лет.

Слайд 3. Возможности и преимущества карточки

Банковская платежная карточка – это универсальный инструмент для совершения широкого спектра финансовых операций. Она позволяет ее держателю производить оплату товаров и услуг в организациях торговли и сервиса, в сети интернет, совершать множество операций посредством каналов дистанционного банковского обслуживания, получать наличные денежные средства в пунктах выдачи наличных и банкоматах. Ее основные функции – это замена наличных при расчетах и средство для хранения денег и обеспечения доступа к их получению.

Так как денежные средства находятся не на самой карточке, а хранятся на счете человека в банке, то банковская платежная карточка как бы удостоверяет право собственности этого человека и является своеобразным ключом к деньгам. Держателю карточки доступны все удобства и преимущества использования этого банковского продукта, к которым можно отнести следующее:

Удобство.

Имея карточку, можно не носить с собой большие суммы наличности, но в то же время всегда иметь возможность совершить необходимую покупку. Банковская платежная карточка весьма компактна и занимает мало места в кошельке. И она предоставляет возможность осуществлять широкий диапазон финансовых операций дистанционно и совершать покупки в интернет-магазинах.

Безопасность.

Банковская карточка – более безопасный способ пользования денежными средствами, но только при правильном ее использовании (мы сейчас будем говорить об этом подробнее). В случае утраты (кражи, утери, физического уничтожения) наличных денег – их скорее всего вернуть не удастся. Деньги, находящиеся на счете, к которому выпущена банковская карточка, можно сохранить если своевременно ее заблокировать.

Широкая география платежей.

Карточки международных платежных систем действуют не только в стране, в которой находится выпустивший их банк, но и за рубежом, что позволяет оплачивать товары и услуги в большинстве стран мира. Кроме того, ввоз и вывоз наличных денежных средств законодательно ограничивается и пристально контролируется в большинстве стран мира.

Беспроблемное пополнение счета в случае необходимости.

Если возникла непредвиденная трудная финансовая ситуация, держатель банковской платежной карточки, даже находясь в другом городе или вообще стране, может попросить помощи у своих родственников или друзей, которые смогут быстро пополнить его счет на нужную сумму.

Финансовый контроль.

Приучив себя совершать покупки преимущественно по карточке вы получаете возможность анализировать свои расходы, используя ежемесячные банковские выписки. А анализ совершаемых покупок позволяет определить ключевые статьи расходов и при необходимости осознанно их ограничить.

Гигиена.

Что касается гигиены, карточка, в отличие от наличных денег, более ”приватна“ и ее чистоту проще контролировать.

А вот после соприкосновения с наличными деньгами медицинские работники советуют каждый раз мыть руки с мылом, так как банкноты и монеты в процессе обращения могут побывать в руках у множества совершенно разных людей. Однако мы все знаем, что в реальных жизненных ситуациях не всегда есть возможность следовать этой рекомендации.

Бонусы.

При оплате карточкой иногда дают разные приятные бонусы. Например, можно копить баллы за покупки и потом обменивать их на подарок. Или получать в конце месяца обратно часть потраченных денег – это называется манибэк. Узнать о бонусных программах можно на официальных сайтах банка.

Возможности банковских платежных карточек увеличиваются с каждым годом, однако при неаккуратном их использовании именно банковская платежная карточка может ”открыть двери“ злоумышленникам к нашим деньгам.

Слайд 4. Реквизиты банковской платежной карточки

Каждая банковская платежная карточка имеет уникальный набор реквизитов. Реквизиты карточки – это информация, которую можно увидеть на самом ”пластике“, на его лицевой и оборотной стороне. Давайте внимательно рассмотрим, каждый элемент банковской платежной карточки и узнаем о его предназначении.

На лицевой стороне:

номер банковской карточки (это не номер счета, к одному счету можно выпустить несколько карточек). Обычно он состоит из 16 цифр, в номере зашифрованы название платежной системы, идентификационный номер вашего банка и другая важная служебная информация;

имя держателя карточки. Могут быть указаны имя и фамилия, однако карточка может быть и неименной;

окончание срока действия карточки – в формате месяц/год (две последние цифры). Срок действия карточки, как правило, от года до пяти лет;

наименование банка, выпустившего карточку. Вообще-то платежная карточка – это собственность банка, а клиент банка являются владельцем счета и держателем карточки;

логотип платежной системы. Карточки могут быть кобрендинговые (то есть совместные карточки банка с одной или несколькими компаниями-партнерами) или кобейджинговые (совместные карточки двух платежных систем). На таких карточках логотипов будет больше;

чип – это встроенный микропроцессор, который содержит информацию о карточке и ее держателе.

На оборотной стороне:

магнитная полоса – как и чип содержит информацию о карточке и ее держателе и нужна для идентификации клиента. С магнитной полосой надо быть осторожными: такую карточку нельзя нагревать или оставлять рядом с электромагнитными приборами, она может размагнититься.

специальная полоса для образца подписи держателя. Получив карточку, надо обязательно расписаться в этом поле, без подписи карточка будет недействительной;

код безопасности – этот код как правило состоит из трех цифр и является одним из защитных элементов и необходим при покупках через интернет. Код безопасности позволяет подтвердить подлинность банковской карточки и то, что именно собственник карточки пользуется ей при оплате через интернет. Каждая платежная система имеет свои отличительные коды безопасности – CVC2 (CVV2, CID).

данные банка – как правило, на карточке указаны номер телефона банка, выдавшего карточку, и его адрес.

Слайд 5. Кто и как охотится за данными банковских платежных карточек

Украсть деньги с банковской карточки сложнее, чем вытащить из кошелька. Тем не менее с развитием цифровых технологий во всем мире с каждым годом становится все больше преступлений в сфере банковских карт. Сегодня для любого человека, использующего банковские платежные карточки, существует риск утраты своих денег вследствии мошеннических действий со стороны злоумышленников.

Мошенничество с платежными карточками, кардинг (от английского carding) – вид мошенничества, при котором производится операция с использованием платежной карточки или ее реквизитов, не инициированная или не подтвержденная ее держателем. Преступников, которые специализируются на банковских карточках, называют кардерами. С развитием информационных технологий, повсеместным распространением дистанционных платежных услуг и доступностью в сети интернет различных информационных ресурсов кардеры уже давно перестали быть редкостью в том числе и для нашей страны.

Для осуществления операций злоумышленникам не требуется иметь доступ к самой карточке. Им нужна информация. Давайте посмотрим, что можно, а что нельзя говорить третьим лицам.

Какие данные банковской платежной карточки можно говорить посторонним?

Номер банковской платежной карточки. Единственная операция, которую можно провести, зная только номер банковской платежной карточки – перевести денежные средства на ваш счет. Поэтому на вопрос можно ли давать номер банковской платежной карточки в целом можно ответить утвердительно. Без дополнительных данных эти цифры не дают доступа к денежным средствам.

Имя и фамилию держателя. Безопасность передачи этой информации неоднозначна. Само по себе ФИО собственника не дает доступа к счету, однако зная дополнительно номер карточки и срок ее действия можно зарегистрироваться в некоторых интернет-магазинах, которые работают без дополнительной системы защиты переводов. Так злоумышленник может делать покупки от вашего имени. Поэтому, если кто-то запрашивает комплекс данных по банковской платежной карточке, это должно вас насторожить.

Какие данные банковской платежной карточки нельзя сообщать?

Комплекс реквизитов. Как мы уже сказали, нельзя передавать совокупность данных, например номер банковской платежной карточки, срок ее действия и имя владельца. Знание этого набора данных открывает возможности для мошенничества.

Код безопасности. Каждая банковская платежная карточка оснащена дополнительным кодом безопасности CVC2 (CVV2, CID). Сообщать кому-либо этот трехзначный код нельзя. При желании его можно даже заклеить кусочком бумажного скотча, чтобы скрыть от посторонних глаз.

Коды из смс подтверждений. Их также никому нельзя сообщать. Это могут быть сеансовые пароли (секретные коды, которые приходят к вам в смс-сообщениях при входе в системы банка) или пароль 3-D Secure (секретный код, который приходит вам в смс-сообщениях на телефон при проведении какого-либо платежа).

ПИН-код. При оформлении банковской платежной карточки сотрудники банка обращают особое внимание на то, что ПИН-код нельзя озвучивать никому, в том числе близким родственникам, друзьям, знакомым, третьим лицам, которые запрашивают ваш ПИН-код для перевода средств, оплаты покупки, усиления безопасности, переоформления или с другой целью. Кроме этого, не рекомендуется носить код вместе с банковской платежной карточкой, например, на отдельной бумажке в кошельке или писать его на самой банковской платежной карточке.

Наше государство обеспечивает защиту интересов и имущественных прав держателей банковских платежных карточек: для них в Беларуси на законодательном уровне установлен принцип ”нулевой ответственности“. Это значит, что если у вас с карточки украли деньги, то вы можете в течение 30 дней обратиться в банк, и деньги вам должны вернуть за 45 дней (в случае, если это произошло в Беларуси), а если операция по списанию денег произошла за пределами нашей страны, то срок возврата удлиняется до 90 дней. Однако следует помнить, что ”нулевая ответственность“ действует только при условии, если были соблюдены все правила безопасного использования банковских платежных карточек. Конечно же, и сами банки постоянно совершенствуют свои системы по минимизации рисков и противодействию махинациям с банковскими карточками, так как такие мошеннические действия приводят к финансовым издержкам и наносят ущерб деловой репутации банков.

Для того, чтобы уберечь свои личные финансы от посягательства мошенников, давайте ознакомимся с самыми распространенными способами, с помощью которых злоумышленники могут попытаться воспользоваться чужими деньгами.

Слайд 6. Вишинг

Знаете, что такое ”вишинг“? Это когда злоумышленники, используя телефонную связь, под разными предлогами выманивают у хозяина платежной карточки конфиденциальную информацию.

Вишинг-мошенники могут представляться сотрудниками банка, работниками госучреждений, или, например, покупателями, которые звонят по объявлению о продаже, размещенному на виртуальных торговых площадках или в социальных сетях. Самое главное – выведать у будущей жертвы необходимые им данные.

Для этого используются различные схемы: сообщение о якобы оформленном кредите, отмена ”ошибочно“ выполненного перевода на карточку жертвы, возможность устранить проблему с неожиданно списанными деньгами, история о преступниках, которые пытаются незаконно использовать карточку, угроза ”блокировки“ карты и др. И, конечно же, по их словам, избежать всех этих неприятностей можно только сообщив ”сотруднику банка“ ваши персональные данные – реквизиты платежных карт, коды авторизации, пароли.

Для убедительности и правдоподобия мошенники пользуются профессиональной терминологией, при разговоре слышен офисный шум, например, разговор другого ”специалиста“ с ”клиентом“. С помощью специальных программ изменяют номер, с которого звонят, чтобы он отличался от телефона реального банка только одной цифрой.

На самом деле сотрудник банка при звонке клиенту заранее должен знать все необходимые ему данные. Поэтому сообщать кому-то информацию о своей банковской платежной карточке, пароли и коды доступа, паспортные данные ни в коем случае нельзя.

Также при вишинге мошенник может предложить ”выгодную“ покупку с огромной скидкой или сообщить вам о выигрыше в какой-либо ”крутой“ акции.

Однако в таких случаях не нужно терять голову от удачной покупки или выгодной акции, необходимо перепроверить информацию, позвонив в контакт-центр организации, которую якобы представляет собеседник. После этого сразу будет понятно, по какому поводу радоваться: реальному неожиданному счастью или тому, что удалось не стать жертвой вишинга.

Слайд 7. Скимминг

Еще одним хитроумным способом получения мошенниками вашей конфиденциальной информации является ”скимминг“ – это установка специального оборудования на банкомат с целью считывания и записи данных банковской карточки для дальнейшего изготовления ее копии.

Скиммер представляет собой устройство, которое крепится к банкомату и с помощью которого мошенники воруют данные банковских карт: реквизиты и пин-код. Это может быть пластиковая накладка, прикрепляемая к картоприемнику, миниатюрная видеокамера рядом с банкоматом, а также специальная накладка на клавиатуру, которая запоминает порядок набора пин-кода. К банкоматам скиммеры крепятся с помощью обычного двустороннего скотча.

Существуют также портативные скиммеры, позволяющие делать копию карты, когда она оказалась в руках злоумышленника, если он, например, работает официантом в ресторане или продавцом в магазине, где клиенты часто расплачиваются банковскими платежными карточками.

При пользовании банкоматами следует проявлять разумную осмотрительность и внимательность, чтобы заметить следы их мошеннической ”модернизации“. Например, если изначально клавиатура была вогнутой, то специальная накладка сделает панель более плоской. Также скимминговое устройство может изменить сами клавиши: они будут либо утоплены в панель клавиатуры, либо, наоборот, слишком сильно выпирать.

Обнаружить скиммер на банкомате для неподготовленного человека непросто, поэтому рекомендуется при выборе банкомата избегать плохо освещенных и безлюдных мест и отдавать предпочтение тем из них, которые установлены в отделениях банков, торговых центрах, на охраняемой территории.

Обнаружив следующие признаки, лучше выбрать другой банкомат:

механические повреждения на корпусе банкомата, такие как трещины, царапины и сколы;

неровный картоприемник или наличие выступов на нем;

посторонние детали, прикрепленные к банкомату, например, магнит;

несовпадение контуров деталей, даже самых небольших. А также явное отличие в цвете или материале.

Слайд 8. Основные правила безопасного использования карточки

Таким образом, банковская платежная карточка предоставляет ее владельцу неоценимые удобства и широкие возможности по управлению личными денежными средствами. При этом всегда найдутся недобросовестные люди, которые пытаются незаконно завладеть чужими деньгами, используя для этого хитроумные приемы и приспособления.

Для противодействия «цифровым» преступникам следует неукоснительно соблюдать простые правила безопасности.

1. Никому нельзя говорить реквизиты карточки и другую информацию, связанную с ней.
2. Хранить карточку следует в надежном месте. Это нужно, чтобы избежать незаконного ее использования или копирования реквизитов.
3. Если вы все-таки потеряли карточку или оставили ее в банкомате, необходимо немедленно ее заблокировать через интернет- или мобильный банкинг или позвонив в банк.
4. Чтобы обезопасить свои денежные средства, также возможно установление лимитов, что убережет ваши деньги хотя бы от потери всей суммы – пока вы не заблокируете свою платежную карточку. Полезно также подключить услугу смс-оповещения, которая позволит получать уведомления о совершенных по карточке операциям и отслеживать движение денежных средств, что предоставляет держателю карточки возможность мгновенно узнать о неправомерных действиях с ней, а значит, и своевременно отреагировать на угрозу.
5. Также разумно обезопасить свои деньги путем использования нескольких карточек – разных для разных целей (для повседневных расчетов, для оплаты в интернете, для зарубежных поездок).
6. Для защиты от скимминга рекомендуется не выпускать карточку из вида при оплате в кафе или ресторане, и пользоваться банкоматами, расположенными на охраняемой территории.

Соблюдение этих элементарных правил поможет вам не стать жертвой мошенников и в полной мере наслаждаться удобствами и преимуществами, связанными с использованием банковской платежной карточки.

Слайд 9.

А ведь еще не так давно, чтобы оплатить счет за коммунальные услуги, надо было идти с бумажной квитанцией в банк или на почту и ожидать в очереди, а, чтобы купить билет на поезд, надо было ехать на вокзал, где, отстояв очередь, можно было узнать, что билетов на нужную дату уже нет. Теперь ситуация кардинально поменялась. Сегодня с помощью систем дистанционного банковского обслуживания мы можем управлять своими деньгами, не выходя из дома.

Слайд 10. Банк без очереди

Интернет- и мобильный банкинг – это технологии, позволяющие клиенту получить доступ к своим счетам и совершать операции с ними в любое время с любого устройства, имеющего доступ в интернет (в случае интернет-банкинга для выполнения операций используется специальный интернет-сайт, в случае мобильного банкинга – мобильное приложение для смартфонов и планшетов). Не снимая тапочек, можно оформить кредит и открыть вклад, оплатить коммунальные услуги, перевести деньги, купить товары в интернет-магазинах и многое другое.

Сегодня, если человек посетит один из банков и пройдет в нем процедуру идентификации, он может получать банковское обслуживание с помощью цифровых каналов в любом банке Беларуси.

Межбанковская система идентификации – это специальная база данных, используемая для удаленной идентификации клиентов и предоставления им услуг с помощью цифровых каналов обслуживания.

В настоящее время банки при обслуживании своих клиентов активно используют современные тенденции автоматизации и роботизации различных процессов, что позволяет исключить рутинный и однообразный труд, обрабатывать и передавать информацию быстрее, сделать работу более эффективной. Например, тенденциями роботизации мобут быть:

- чат-боты – применение голосовых автоответчиков (когда, позвонив в банк, вам отвечает, например, робот, Алиса);
- роботы – операционисты;
- автоматические запросы на выставление оценок за обслуживание и др.

Развитие цифровых технологий способствует:

1. Сокращению временных и финансовых издержек по предоставлению финансовых услуг;
2. Повышению качества предоставляемых услуг;
3. Снижению стоимости услуг для конечного пользователя;
4. Повышению прозрачности финансов и многое другое.

Цифровые технологии дают больше возможностей в жизни и свободного времени на любимые дела. Пользоваться ими удобно и приятно.

Но и тут тоже надо быть бдительными и не забывать о безопасности, потому что преступники не дремлют, и очень желают улучшить свое финансовое положение. Давай посмотрим, где нас могут обмануть?

Слайд 11. Поддельный сайт (фишинг)

Например, на фишинговом (поддельном) сайте. Злоумышленники могут создать подделку сайта, очень-очень похожую внешне на официальный сайт, а его URL-адрес (символы, которые вводятся в адресную строку браузера) будет отличаться всего на одну букву или цифру. Мошенники надеются, что человек, ничего не подозревая, введет свои данные на таком сайте, а они получат их. Недаром ”фишинг“ в переводе с английского значит ”рыбалка“. Так рыбаки-мошенники ловят на свою удочку невнимательных и доверчивых пользователей.

Человек может изначально попасть на фишинговый сайт, являющийся копией оригинала. Но может быть и так, что преступник встраивает ссылку на свою страницу в подлинный сайт, и, кликая мышью на какой-то раздел (чаще всего платежный), человек оказывается на имитаторе этой страницы. При этом все остальные ссылки – настоящие. В обоих случаях пользователь оставляет на сайте свои данные и они становятся доступны мошенникам.

Для того чтобы заманить на поддельный сайт, мошенники используют социальные сети, смс или электронную почту. Зачастую фишинговые сайты оказываются в первых строках поисковой выдачи в интернете. Мошенники применяют инструменты веб-маркетинга, чтобы эффективно продвигать фишинговые сайты.

Зная, как определить мошеннический сайт, вы сможете без опаски совершать денежные переводы и платежи в интернете. Итак, обращаем внимание на следующие моменты.

Внимательно посмотрите на веб-адрес сайта.

Вы можете узнать, является ли сайт фишинговым, проверив домен в адресной строке и сравнив его с изначальным адресом домена. Как мы говорили, фишинговые сайты очень часто используют похожие домены для обмана пользователей. Например, ваш домен выглядит так: yourbank.by. Домен фишингового сайта может выглядеть так your.bank.by. или так yourbanc.by.

Проверьте, имеет ли сайт безопасное соединение.

Адрес сайта, через который вы хотите провести оплату, должен начинаться с ”https://“ и иметь пиктограмму в виде закрытого замка зеленого цвета. Этот замочек означает, что информация, которую вы вводите, передается через безопасный канал связи или через защищенное соединение. Не делай покупок в интернет-магазинах, которые не имеют этого замочка рядом с веб-адресом.

Проверьте, когда и на кого зарегистрирован сайт.

Фишинговые сайты обычно существуют недолго, их быстро вычисляют специалисты по борьбе с киберпреступностью. Но и за свое недолгое существование они могут нанести большой вред множеству людей. Поэтому стоит проверить, когда зарегистрирован сайт. Быстро получить всю информацию о домене, например, дату регистрации, контакты для связи с организацией, можно с помощью специальных программ в интернете.

Сайт содержит грамматические или орфографические ошибки.

Крупные компании имеют в штате или привлекают профессиональных дизайнеров, копирайтеров, редакторов и корректоров, которые строго следят за соблюдением правил оформления сайта. Насторожить должны неправильное название организации, обилие опечаток и ошибок, ”поехавшая“ верстка и др.

В любом случае надо быть очень осторожными, если запрашивается ваша личная информация, даже если вам приходят сообщения с адресов, которые могут показаться официальными.

Слайд 12. Надежный пароль

Пароль – залог безопасности, он защищает наши финансы в цифровой среде от различных угроз, не дает злоумышленникам узнать конфиденциальную информацию и использовать ее в своих целях. И поэтому к паролям – отдельные требования.

Для разных аккаунтов должны быть разные пароли.

Некоторые люди используют один и тот же пароль для всех сайтов. На самом деле, если использовать только один пароль для всех своих аккаунтов, то хакерам или ворам намного проще причинить вам вред. Преступнику нужно взломать только один пароль, чтобы получить доступ сразу к нескольким аккаунтам.

Пароли надо периодически менять.

Оптимальная частота смены пароля составляет в среднем раз в полгода для важных для вас сервисов, вроде почты, электронных кошельков, мобильного и интернет банкинга и тому подобного.

Пароль для входа в платежные сервисы должен быть сложным.

Нельзя использовать в качестве пароля личные данные, которые есть в любой социальной сети: например, свое имя и фамилию, дату своего рождения, клички животных и др. Если ваш пароль ”Мурзик“, а в соцсетях фотография, которая подписана ”Я с любимым котом

Мурзиком на диване“, то всякая конфиденциальность отсутствует, и мошеннику проще простого подобрать такой пароль.

Для того чтобы придумать сложный пароль, надо сделать его длинным – как минимум 8 знаков, даже если сайт не требует этого. Кроме длины сложный пароль должен состоять из заглавных и прописных букв, чисел и символов. При такой комбинации знаков мошенникам будет сложнее подобрать пароль. Не очень хорошая идея – создавать пароль путем набора русских слов при включенной английской раскладке. Хакеры уже давно создали специальный словарь, позволяющий перебирать такие пароли.

Пароль надо держать в голове.

Вот лайфхак, как запомнить сложный пароль. Это можно сделать с помощью фразы, короткой поговорки, части песни или детской считалки. Например, можно использовать строчку из песни или только первые буквы ее каждого слова. Также можно использовать специальные символы, заглавные буквы и числа в разных частях пароля, не только в начале или в конце. Например, ”нТгП!уВрМ!1“ (наша Таня громко плачет, уронила в речку мячик) будет надежным паролем, который одновременно легко запомнить. Пароль должен быть таким, чтобы тебе было легко его запомнить, а другим сложно угадать.

Слайд 13. Опасности в интернете

Интернет – целый мир, где есть много полезной информации, разнообразных сервисов и развлечений. Но здесь есть и преступники, мошенники, воры, другие злоумышленники, которые тоже оценили возможности интернета, который позволяет им действовать анонимно. Поэтому, пользуясь интернетом, надо быть осторожными и соблюдать правила безопасности.

Обязательная установка антивирусных программ.

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить наши действия и украсть деньги со счета. Программы ”Трояны“, ”Шпионы“, ”Черви“, – их множество разновидностей, а суть одна – все это вредные вирусы. Для защиты компьютера на нем надо установить специальные защитные программы и фильтры. Использовать лучше лицензионное антівірусное программное обеспечение с актуальными обновлениями.

Не пользуйтесь интернет- и мобильным банкингом, платежными сервисами через общественный wi-fi.

Скорее всего, ваши девайсы автоматически подключаются к wi-fi дома. Естественно, так намного легче, быстрее и удобнее. Также это удобный способ сохранять просмотренные данные. Бесплатный wi-fi кажется очень привлекательным, когда вы находитесь в кафе, или за городом. Однако если вы пользуетесь критически важными сайтами, например, интернет банкингом или другими сайтами, где вы вводите персональные данные, то важно использовать только те сети wi-fi, владельцу которых вы доверяете. Многие кафе и рестораны предлагают бесплатный доступ к открытым (незащищенным) сетям для своих клиентов. Но если злоумышленники подключатся к этой открытой сети, они легко смогут получить доступ к информации, которая отправляется на ваш девайс и с него и воспользоваться ей. Поэтому следует быть очень осторожным по отношению к wi-fi сети и незащищенному каналу, к которым вы подключаетесь.

Не выкладывайте всю информацию о себе в интернете.

Наши персональные данные – это ключ ко многим нашим тайнам. И их защите уделяется большое внимание даже на законодательном уровне. Но зачастую при помощи социальных сетей, а также блогов люди сообщают о себе всю конфиденциальную информацию и весьма легко составить полную анкету человека – узнать о дате рождения, где он живет, кто проживает вместе с ним (и даже когда его не бывает дома), где он учится и как предпочитает проводить свободное время.

Всю эту информацию надо держать в тайне. Что касается работы с платежными сервисами, тут надо быть осторожными вдвойне и никому не сообщать логин, пароль, сеансовые ключи, личные данные. Не стоит также позволять браузерам сохранять данные карточки для упрощения совершения платежей в будущем.

Виртуальный собеседник может выдавать себя за другого.

Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. Знайте, что виртуальные знакомые могут быть не теми, за кого себя выдают. Нельзя слишком доверять знакомцам в сети.

Слайд 14. Мошенники на досках объявлений

Такой огромный виртуальный рынок, как площадка с объявлениями о продаже и покупке разных вещей и оказании услуг, конечно же, тоже привлекает мошенников. Ведь здесь можно поживиться чужими деньгами.

Самая распространенная мошенническая схема со стороны продавца выглядит так: вы находите привлекательное по цене или другим признакам объявление. Вас просят отправить аванс или

предоплату до того как вы встретитесь с продавцом, чтобы подтвердить свои намерения или ”отложить“ востребованный товар. Для получения предоплаты продавец предлагает перевод на карточку, оплату на счет мобильного телефона или денежный перевод частному лицу. После получения предоплаты мошенник перестанет отвечать на ваши звонки, а доказать факт мошенничества не получится, так как вы добровольно перевели деньги частному лицу.

Но не только продавцы бывают мошенниками. Некоторых покупателей тоже стоит опасаться. Представьте, вы разместили объявление и спустя некоторое время с вами связывается ”покупатель“, который готов перечислить вам предоплату или полностью оплатить товар, но только переводом на банковскую карточку. Приехать лично он не может, но обещает прислать курьера или своего родственника на следующий день. А деньги готов перечислить прямо сейчас и для этого просит у вас реквизиты карты. Если вы поверили и дали номер своей карты, через некоторое время будет повторный звонок, и ”покупатель“ попросит продиктовать ему код из смс-сообщения, полученный вами от банка. Если сделать это, ваша карточка будет привязана к чужому виртуальному счету и с нее можно будет снять все доступные деньги.

Пусть вас насторожат следующие факты:

Товар продается исключительно по предоплате. Никогда не переводите предоплату, пока не получите товар/услугу: утром деньги – вечером стулья.

Слишком низкая цена. Не кидайтесь на дешевый товар. Вспомните, где бывает бесплатный сыр?

Обманщики соглашаются купить выставленный товар не глядя. У них, как правило, особенные жизненные обстоятельства, они торопятся, и не готовы встречаться лично.

Просят личную информацию, выписки банковских счетов. Не давайте никому никакую персональную информацию, данные карты, коды, которые приходят в смс.

Слайд 15. Правила безопасности в интернете

Итак, давайте подытожим важные моменты для того, чтобы наши деньги оставались в безопасности, когда мы пользуемся интернетом:

1. Обязательно установить на гаджетах антивирусное обеспечение.
2. Надо убедиться, что перед вами не подделка сайта, где вы будете вводить свои данные.

3. Нельзя никому сообщать или передавать логин, пароль, сеансовый ключ, другие личные данные для входа в интернет- и мобильный банкинг.

4. Пароль для входа в интернет- и мобильный банкинг должен быть надежным, его лучше всего запоминать (не записывать) и периодически менять.

5. Не рекомендуется заходить на персональную страницу интернет- и мобильного банкинга с чужих электронных устройств и передавать свои гаджеты для использования другому человеку. Но если это все-таки необходимо, то надо проверять не сохранились ли ваши персональные данные на чужом устройстве.

6. Помните, что ваш виртуальный друг может быть не тот, за кого себя выдает.

Слайд 16. Безопасный мобильный

Не так давно мобильные телефоны умели только звонить и отправлять смс-сообщения. Сегодня мобильные устройства превратились в портативные мультимедийные центры, фотоаппараты и рабочие мини-компьютеры, они позволяют совершать широкий спектр платежных и других операций (оплачивать товары и услуги, переводить денежные средства, пополнять вкладные счета, осуществлять покупки через интернет и многое-многое другое). Все это расширяет возможности пользователей мобильных устройств. Но это также делает мобильный телефон очень привлекательным для мошенников.

В этом разделе мы поговорим о возможностях и безопасности наших мобильных, а также рассмотрим основные разновидности мобильного мошенничества.

Слайд 17. Возможности мобильного

Современные способы оплаты товаров и услуг, которые ориентируются на внедрение новейших технологий, развиваются семимильными шагами.

Бесконтактная оплата мобильным телефоном.

Сегодня мобильный телефон способен выполнять роль банковской бесконтактной карточки. Для пользователя единственное отличие заключается в том, что к терминалу в магазине он приложит не карточку, а телефон. Чтобы пользоваться таким способом оплаты, необходимо один раз ввести реквизиты карточки в платежное приложение, находящееся в смартфоне. После этого можно производить оплату, используя смартфон вместо карточки.

Оплата с помощью QR-кода.

Внешне QR-код (с англ. – quick response переводится как быстрый ответ) – это квадратный штрих-код, состоящий из черных точек и пробелов. Многие компании используют эти коды для хранения и распространения самой различной информации. Это может быть, например, обычный текст, адрес в сети интернет, контактные данные человека или платежные реквизиты.

Воспользоваться таким способом оплаты несложно. Если магазин, в котором вы собираетесь совершить покупку или ресторан, в котором вы ужинаете подключены к сервису оплаты посредством QR-кода, то выбрав товар ли заказав услугу, вам достаточно отсканировать QR-код, который соответствует данному товару или услуге и оплатить. Отсканировать QR-код можно специальным приложением на смартфоне или, используя приложение мобильного банкинга либо приложение вашего сотового оператора с поддержкой QR-кодов. Функцию оплаты посредством QR-кодов активно внедряют в свои мобильные приложения банки Республики Беларусь.

18. Ограничение доступа к гаджету

Если ваш телефон попадет в руки к злоумышленникам, те воспользуются возможностями вашего мобильного телефона для своих целей. Поэтому обязательно надо установить себе на телефон функцию автоматической блокировки экрана, и желательно с паролем или другим способом аутентификации (сегодня это может быть графический ключ, отпечаток пальца или даже сканирование вашего лица).

Создавать надежные графические ключи на девайсах также важно, как сложные пароли с разными цифрами, буквами и символами. К сожалению, многие люди не устанавливают хорошие графические ключи. У половины пользователей мобильных телефонов, у кого есть такой графический ключ, он начинаются в левом верхнем углу, а еще у половины – ключи представляют собой форму первой буквы фамилии или имени человека. Надежный графический ключ состоит из пересекающихся друг с другом линий. Также важно отключить опцию ”сделать видимым“, чтобы никто не смог увидеть пароль (ключ), когда вы его вводите.

С помощью вредоносных программ также можно легко получить все, что нужно для доступа к платежным сервисам. Самый распространенный вариант, установка на ваш телефон программы-вируса, который передает все данные злоумышленнику. Под предлогом

позвонить, злоумышленники просят смартфон, и незаметно устанавливают на нем программное обеспечение, после чего, имеют возможность от имени владельца осуществлять различные действия. Далее с помощью таких программ мошенник получает ваши данные и может с легкость перевести ваши деньги себе на счет. Не передавайте ваши гаджеты в чужие руки.

Пользуйтесь антивирусным программным обеспечением и обновляйте его!

Слайд 19. Мобильные ”разводки“

СМС-рассылки о выигрышах и бонусах.

Получали ли вы когда-нибудь сообщение о том, что вы вдруг стали богатым наследником, и чтобы получить деньги, вам только надо заплатить комиссию за банковский перевод или что-то подобное. Также вы можете получить смс-сообщение, в котором вы якобы являетесь победителем в лотерее или выиграли ценный подарок. Такие письма могут приходить и по электронной почте. Лучше всего такие письма не открывать и сразу отправлять в папку ”спам“.

Нужно помнить, что обогатиться подобным образом просто невозможно. Это опять-таки уловки мошенников, которые пытаются играть на наших слабостях и эмоциях. Такие письма также опасны тем, что в них может быть заложен вирус, который поможет ворам добраться к вашим персональным данным, а в последствии к деньгам.

СМС-рассылки с просьбами о помощи.

Или такая ситуация. Мошенники делают рассылку следующего содержания: ”Маша, это Вася. У меня проблемы. Помоги мне, надо срочно 100 рублей! “. Или абонент сотовой связи получает смс: ”Сынок, я попала в беду, положи мне на такой-то номер 50 рублей. Потом все объясню“.

Простейшие схемы ”мобильной разводки“ работают ”наудачу“. Разумеется, текст смс может быть каким угодно: это может быть отсутствие денег на поезд в другом городе, ”украденный кошелек“ и др. Обычно мошенники просят перевести им деньги, хотя некоторые могут попросить и данные вашей банковской карты.

Смысл ”разводки“ в том, что жертва верит в то, что смс действительно от знакомого ей человека и тут же переводит ему запрошенную сумму.

Также часто бывают ситуации, когда мошенники взламывают ваши социальные сети, и пишут от имени ваших знакомых или родных. Если адресат просит выручить или одолжить ему деньги, вам в первую очередь надо насторожиться, и не поверить. Далее – позвоните тому,

кто просит у вас деньги, или найдите другой способ убедиться, что вы общаетесь именно со своим родственником или другом, прежде чем дать какую-либо информацию или перевести деньги. Скорее всего, у него все в порядке, и он даже не подозревает о том, что от его имени отправлено сообщение.

Слайд 20. Платные опции и контент

Существует много сервисов, где можно скачать и установить на свой мобильный телефон обновленные и новые программы, которые расширяют возможности наших гаджетов. Как правило, мы стараемся пользоваться бесплатными или ”условно бесплатными“ (предполагающими возможность бесплатной установки программы при условии просмотра рекламы) программами. Но и тут могут подстерегать мошенники.

Например, они могут спрятать вирус внутрь архива скачиваемого файла, или, например, при попытке найти и скачать программку пользователи периодически натыкаются на сайты, предлагающие ввести номер мобильного телефона. Выглядит это примерно так: ”Напишите номер своего мобильного, вам придет смс с кодом (или ссылкой), подтвердите ее получение ответной смс (или нажмите на ссылку). При отправке смс с ”секретным“ кодом доступа вполне возможно, что вас подпишут на платную рассылку или спишут деньги со счета телефона, а нужного файла вы так и не увидите. Не отправляйте ответных смс и не активируйте пришедшие ссылки.

Также вы можете приобретать различные мобильные сервисы – приложения, игры, музыку и т.д. на платной основе. Оплата при этом происходит либо через специальный аккаунт путем списания денег с подключенной к нему банковской карты (обычно при этом не требуется дополнительного ввода данных вашей карты, а только лишь подтверждение оплаты путем введения пароля, либо с банковской карты напрямую. И тут также необходимо быть очень осторожным.

Не пользуйтесь малоизвестными сервисами, предоставляющими доступ к контенту. Крупный и серьезный сервис уважает свою репутацию – там легче понять, какую сумму и за какую услугу конкретно вы платите. К тому же, меньше вероятность того, что вместо желанного доступа к новому фильму вы попадете на сайт к мошенникам.

Слайд 21. Правила мобильной безопасности

1. Не передавайте ваши гаджеты в чужие руки.

2. Установите пароль или другой способ аутентификации на своем смартфоне.

3. Пользуйтесь антивирусным программным обеспечением и обновляйте его.

4. Будьте осторожны! Не доверяйте слепо смс сообщениям.

5. Внимательно читайте все условия, на которых предоставляется услуга по установке дополнительных опций на ваш смартфон.

6. Пользуйтесь известными сервисами для покупки опций и контента для вашего смартфона.

Слайд 22. Заключение

Этот урок был подготовлен, чтобы помочь вам, дорогие ребята, безопасно ориентироваться в цифровом мире денег. Сегодня мы говорили про базовые вещи, которые должен знать каждый современный человек, чтобы уберечь свои деньги от злоумышленников.

Но мошенники изобретательны и постоянно придумывают все новые и новые схемы обмана. Поэтому в заключение хочется дать вам одно напутствие – всегда руководствуйтесь здравым смыслом! Если вы видите необычную ссылку или сайт, которые кажутся вам небезопасными, лучше проигнорируйте их. Если предложение кажется вам слишком хорошим, чтобы быть правдой – это, скорее всего, действительно, обман.

Пусть у вас все получится. Спасибо за внимание!