Слайд 1. Береги себя и свои деньги!

Дорогие друзья!

Международная неделя финансовой грамотности (Global Money Week) – это ежегодная общемировая компания повышения осведомленности детей и молодежи о финансах. Начало Global Money Week было положено в 2012 году, и с тех пор ее участниками стали более 170 стран и территорий по всему миру. Республика Беларусь с 2013 года присоединилась к числу партнеров этого международного движения и каждый год участвует в важной образовательной инициативе.

В этом году слоган международной недели финансовой грамотности – ”Береги себя и свои деньги“. Такую важную и интересную тему для проведения мероприятий в рамках недели предложила Организация экономического сотрудничества и развития, которая является ее глобальным координатором.

Почему эта тема так актуальна сегодня? Передовые цифровые технологии уверенно входят в нашу жизнь и делают ее более комфортной. Наши дома и окружающие нас вещи становятся более ”умными“, предоставляют нам удобства и позволяют экономить время. Кроме того, пандемия коронавируса многократно подтолкнула всех нас перестроить свой образ жизни, поменять наши привычки – теперь мы учимся и работаем онлайн, ”ходим“ в гости, музеи и театры по интернету. Инновационные программно-технические решения все активнее применяются и в финансовой сфере. Наше взаимодействие с финансовыми организациями происходит посредством новейших технологий и постепенно перемещается из сферы офлайн-коммуникаций в виртуальную онлайн-среду. Традиционные пункты финансового обслуживания уходят на второй план, а дистанционные каналы доступа к финансовым услугам все больше распространяются.

Для того, чтобы быть полноправным участником цифрового финансового рынка и пользоваться всеми предоставляемыми им возможностями и преимуществами от нас с вами требуется значительно больше знаний, умений и навыков, чем несколько лет назад. К тому же эти процессы сопровождаются возникновением новых финансовых рисков и обостряют вопросы финансовой безопасности. Человеку надо знать и соблюдать основные правила безопасности, которые позволяют минимизировать риски быть обманутыми мошенниками, пытающимися украсть деньги с помощью цифровых технологий.

Поэтому сегодня мы поговорим с вами о стремительно развивающихся цифровых финансовых продуктах и сервисах (которые помогут нам сберечь себя, в частности, в условиях пандемии) и

остановимся на основных моментах цифровой финансовой безопасности (которые помогут сберечь свои деньги).

Слайд 2. Дистанционное банковское обслуживание

Дистанционное банковское обслуживание – это возможность пользоваться банковскими услугами без посещения банка. Самыми распространенными технологиями дистанционного банковского обслуживания клиентов сегодня являются *интернет- и мобильный банкинг*.

Интернет- и мобильный банкинг – это технологии, позволяющие клиенту получить доступ к своим счетам в банке 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 (вэб приложение), в случае с мобильным банкингом – мобильное приложение для смартфонов и планшетов).

Преимущества использования интернет- и мобильного банкинга очевидны.

- Вам не нужно добираться в банк, стоять в очереди, тратить время на обратную дорогу. В любой удобный момент вы можете получить доступ к своим счетам и совершить любую операцию не выходя из дома.
- Благодаря этим сервисам банки экономят на расходах на аренду помещений, зарплату сотрудников, технику, канцелярию. Логично, что банки заинтересованы в распространении дистанционного банковского обслуживания – и поэтому они предлагают ”самостоятельным“ клиентам всевозможные бонусы. Если, к примеру, в отделении банка клиент должен заплатить комиссию за какой-либо платеж, то, возможно, в интернет-банкинге такой комиссии не будет, либо она будет заметно ниже. Если вы открываете депозит онлайн – то более привлекательной будет доходность. Если самостоятельно оформляется заявка на выпуск новой карточки – это тоже обойдется дешевле, чем при личном посещении отделения банка. И так по многим другим банковским услугам.
- Наличие у клиента доступа ко всем своим счетам и операциям в режиме 24/7. Понадобилось заплатить за телефон в новогоднюю ночь? Без проблем. Интернет- и мобильный банкинг работают без праздников и выходных.

Сегодня через интернет- или мобильный банкинг можно с легкостью совершить большинство банковских операций. Например:

- получение информации о счетах, а также выписок по ним;

- совершение любых платежей – от коммунальных услуг до налогов и взносов;
- переводы между карточками, в том числе между карточками, выпущенными в разных банках, а иногда – и в разных странах;
- открытие и пополнение депозитов и электронных кошельков;
- погашение кредитов;
- оформление заявок на кредиты, платежные карточки и другие продукты;
- управление лимитами по карточке;
- быстрая блокировка карточки в случае форс-мажора (например, утери);
- могут быть доступны и другие услуги.

Кроме того, здесь всегда можно ознакомиться с актуальными курсами валют, последними новостями вашего банка и получить множество другой полезной информации.

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

Слайд 3. Межбанковская система идентификации

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

Межбанковская система идентификации (МСИ) – это информационная система, в которую поступают персональные данные клиентов банков, храняться в ней и используются для дистанционного предоставления услуг. Благодаря МСИ любые банки страны могут дистанционно идентифицировать обратившегося к ним клиента и получить все необходимые данные о нем, даже если этот человек ранее никогда не обращался в данный банк.

Владельцем МСИ, который обеспечивает ее функционирование, является ОАО ”Небанковская кредитно-финансовая организация ”ЕРИП“. Чтобы клиенту пользоваться возможностями МСИ, нужно пройти регистрацию на сайте ЕРИП. После этого можно войти в личный кабинет по логину и паролю. Процедура регистрации в МСИ бесплатная.

Благодаря межбанковской системе идентификации можно:

- стать клиентом любого банка Беларуси, не выходя из дома;
- пользоваться услугами банков и оформлять банковские продукты в режиме 24/7, не подстраиваясь под режим работы банка;

- оформлять банковские продукты в режиме онлайн – например, текущие счета, депозиты, кредиты – и управлять ими;
- получить и изучить свою кредитную историю.

Слайд 4. Биометрия в сфере финансов

Усы, лапы и хвост когда-то были документами кота Матроскина, а сегодня подобным ”удостоверением личности“ может обзавестись любой и называются они биометрические данные.

Биометрические данные – это уникальные сведения, которые характеризуют физиологические и поведенческие особенности человека и, на основе которых можно с достоверно установить его личность. Наиболее популярны пять типов биометрических данных: отпечаток пальца, изображение лица, голос, радужная оболочка глаза, рисунок вен ладони и пальца.

Работа любой биометрической технологии проходит в четыре основных этапа:

- снимок биометрического образца – например, запись вашего голоса или фиксация отпечатка пальца;
- преобразование полученного образца в математический код и создание шаблона (оцифровка);
- сравнение биометрических данных, предоставляемых в момент попытки осуществления операции, с шаблоном – например, вы прикладываете отпечаток пальца к сканеру в момент прохождения паспортного контроля в зоне шенгена, и система сравнивает его с отпечатком, который вы сдавали при оформлении визы;
- результат – система ”понимает“, совпали образцы или нет.

Биометрические технологии используются в таких сферах нашей жизни, как госуслуги, туризм, здравоохранение. Не осталась в стороне и сфера финансов.

По данным международных экспертов около 80% утечек информации связано с некорректным использованием учетных данных, украденными или слабыми паролями (пароль ”123456“ остается самым популярным в мире паролем). Поэтому очевидно, что одних паролей для защиты данных недостаточно.

Сегодня биометрию используют банки, например, при осуществлении платежей, денежных переводов; оформлении вкладов и кредитов в режиме онлайн, при входе в онлайн-банкинг, при доступе к банковским ячейкам пр. При этом биометрия может использоваться как дополнительный фактор подтверждения личности человека вместе с уникальными кодами и паролями, стандартными документами. Такая комбинация факторов позволяет максимально защитить клиентов банков от злоумышленников. Например, при звонке в колл-центр банк

использует биометрию, чтобы распознать вас по голосу, но дополнительно попросит озвучить некоторые личные данные. При посещении хранилища с банковскими ячейками может потребоваться отпечаток пальца и, к примеру, паспорт или специальная карта доступа.

Биометрическая идентификация удобна для пользователей. Биометрические данные всегда при вас, их нельзя забыть, как это часто бывает с паролем, или потерять, как это случается, например, с банковской платежной карточкой.

Также плюс применения биометрических технологий для человека – это простота и скорость: приложил палец и платеж прошел.

Таким образом, внедрение и использование биометрических технологий в финансовой сфере удобно, оно упрощает финансовые операции, а также защищает наши деньги от мошенников.

Слайд 5. Современные платежные гаджеты

Благодаря развитию бесконтактных технологий в последние годы вместо карточек все чаще используются всевозможные гаджеты – смартфоны, часы, специальные кольца, браслеты и так далее. Многие эксперты полагают, что в будущем мы совсем перестанем пользоваться карточками в их классической форме и перейдем на альтернативные платежные инструменты.

Смартфоны

Для того чтобы использовать смартфон вместо карточки, он должен быть оснащен специальным NFC-модулем. Такой модуль имеют все современные устройства, однако из-за особенностей развития систем NFC-платежей не каждый смартфон с NFC будет полноценно работать на белорусском рынке. В нашей стране оценить удобство платежей смартфоном могут владельцы гаджетов от Apple, Samsung, HUAWEI и HONOR. Все необходимые настройки легко осуществляются в специальном мобильном приложении. После того как ваша карточка будет привязана к телефону, вы сможете легко оплачивать им покупки как обычной бесконтактной карточкой, поднося гаджет к платежному терминалу.

Платежные кольца

Такой необычный финансовый аксессуар появился в Беларуси в 2019 году. Его можно носить на пальце, как украшение, и при этом бесконтактно оплачивать кольцом товары и услуги. Для этого прямо в кольцо встроен специальный модуль NFC. В настоящее время ”привязать“ к кольцу можно только карточку международной системы Visa. Гаджет ударопрочный, водонепроницаемый и выглядит весьма стильно. Немудрено, что при этом он не бесплатный – платежный аксессуар стоит денег, и немалых. В настоящий момент этот продукт

больше подойдет для платежных гурманов и любителей экспериментов – ведь, в отличие от смартфона, который в современном мире нужен каждому, кольцо может выполнять лишь две функции: эстетическую и платежную.

Умные часы

Здесь, как и в случае со смартфонами, платежные сервисы в Беларуси будут доступны владельцам гаджетов от Apple, Samsung, HUAWEI и HONOR. Не трудно догадаться, что в умные часы тоже встроен NFC-модуль. Сама по себе привязка карточки будет осуществляться через смартфон, связанный с умными часами, с помощью специального мобильного приложения. Привязка осуществляется только один раз, после чего часами для оплаты можно пользоваться автономно, не прибегая к помощи смартфона. Помимо платежей, умные часы могут предложить вам множество других функций – от фитнес-трекера до управления аудиосистемой в автомобиле. Возможность бесконтактной оплаты станет лишь приятным дополнением.

И многое другое

Нательные наклейки, специальные перчатки, браслеты и даже накладные ногти с NFC-модулем – это не выдумки сценаристов фильмов о будущем, а реальность, в которой мы живем. Список платежных гаджетов постоянно расширяется. Подобрать устройство по душе сможет даже самый искушенный экспериментатор.

Слайд 6. 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. Функцию оплаты посредством QR-кодов активно внедряют в свои мобильные приложения банки Беларуси.

Чем же платеж по QR-коду может быть удобнее, чем, к примеру, оплата банковской платежной карточкой или смартфоном с функцией бесконтактной оплаты?

- Не требуется предъявления банковской платежной карточки, нужен лишь телефон, на котором установлено мобильное приложение банка. Деньги идут с привязанной банковской платежной карточки, счета или электронного кошелька покупателя на счет продавца.
- Для оплаты по QR-коду подойдет любой телефон с камерой, который поддерживает банковские приложения. Тогда как для

бесконтактной оплаты смартфоном с функцией бесконтактной оплаты требуется NFC-модуль.

- Оплата по QR-коду дает возможность платить там, где нет POS-терминалов, предоставляет идеальные условия для точек самообслуживания.
- Оплата по QR-коду имеет свои положительные моменты в части безопасности, так как при использовании мобильного приложения банка требуется дополнительная авторизация в нем.

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 нужно:

отсканировать QR-код, который соответствует желаемому товару или услуге. В зависимости от возможностей конкретного сервиса оплаты, это можно сделать или в специальном приложении мобильного банкинга, или стандартным сканером QR-кодов, установленным на мобильное устройство;

проверить информацию о товаре или услуге, названии магазина и сумму к оплате;

нажать кнопку ”оплатить“ и деньги спишутся с вашего счета. Вы получите электронный чек, а продавец получит уведомление об оплате.

Слайд 7. Электронные деньги

Электронные деньги используются в качестве средства платежа для расчетов как с организациями, выпустившими эти единицы стоимости, так и с другими организациями или гражданами, которые принимают такое средство платежа. Электронные деньги не требуют открытия отдельного банковского счета, а хранятся в специальных электронных кошельках.

Создать такой кошелек можно онлайн или при обращении в отделение банка, а чтобы в нем появилась какая-то сумма – его нужно пополнить реальными деньгами. Есть много способов это сделать: например, с карточки через интернет-банкинг или банкомат, наличными деньгами в кассе банка или на почте, переводом таких же электронных денег с другого электронного кошелька и пр.

После пополнения кошелька электронными деньгами можно ими пользоваться: например, платить товары или услуги в интернете и в офлайн-магазинах, которые принимают такой вид оплаты, делать частные переводы между электронными кошельками, погасить электронные деньги, т.е. получить в наличной или безналичной форме денежные средства в обмен на электронные деньги. Сегодня в мире систем электронных денег и сопутствующих им сервисов существует

достаточно много. Одними электронными деньгами удобно рассчитываться в интернете, с помощью других можно оплатить услуги мобильного оператора, третьи будут более удобны для переводов между частными лицами. Системы электронных денег отличаются разнообразием и развиваются.

У электронных денег есть несколько плюсов, особенно, при расчетах онлайн:

- Чтобы пользоваться электронным кошельком, не нужно открывать банковский счет.
- Необязательно выходить из дома – открыть электронный кошелек и пополнить его, например, со счета, к которому выдана карточка, можно дистанционно. Операции с электронными деньгами также как и операции с карточками осуществляются мгновенно. Только нужно учитывать особенность электронных денег и карточек – мгновенность проведения расчета владельцем электронного кошелька (держателем карточки), как правило, не означает такой же мгновенности поступления электронных денег в кошелек получателя (денежных средств на счет получателя). Поэтому есть временной разрыв момента оплаты и момента поступления денег, но это характерно для всех аналогичных систем.
- Можно открыть электронный кошелек специально для расчетов в интернете и пополнять его на нужную сумму непосредственно перед тем, как совершить платеж. Это безопаснее, чем платить в сети интернет, например, зарплатной карточкой. Не нужно вводить реквизиты вашей карточки, а значит, даже если вы попадете на поддельный сайт, мошенники не смогут получить доступ к вашему счету и всей зарплате.
- Организации, выпускающие электронные деньги, нередко предлагают своим клиентам программы лояльности. В некоторых случаях к электронному кошельку выпускается специальная (предоплаченная) карточка (не стоит путать ее с банковской платежной карточкой).

В любом случае электронными деньгами можно рассчитаться там, где продавец принимает такой способ оплаты и у него имеется об этом информация для покупателей. Так интернет-магазины размещают на своих страницах информацию о доступных способах оплаты, а офлайн магазины размещают в своих торговых залах такую информацию.

У электронных денег есть также и ряд особенностей: их нельзя разместить во вклад, на остаток электронных денег не начисляются проценты, электронные деньги не подпадают под действие закона о гарантированном возмещении банковских вкладов. Отсрочка оплаты за приобретаемые электронные деньги может быть предоставлена

владельцу электронного кошелька при определенных условиях, а кредиты электронными деньгами не выдаются.

Слайд 8. Что такое социальная инженерия?

Многие специалисты по информационной безопасности говорят, что, как не защищай программы и системы, но есть одно слабое звено – это сам пользователь. Люди зачастую оказываются очень доверчивыми и сами предоставляют мошенникам конфиденциальную информацию. С помощью специальных практик мошенникам добыть необходимую информацию намного проще, нежели получить ее путем взлома системы безопасности. Этим они и пользуются.

Социальная инженерия – это способ получения конфиденциальной информации с помощью психологического воздействия на человека с целью получения выгоды.

Социальная инженерия может принимать разные виды. Вот самые распространенные.

Фишинг – это вид мошенничества, основная суть которого завладение логинами и паролями от важных сайтов, аккаунтов, счетов в банке и другой конфиденциальной информацией путем рассылки писем с ссылками на мошеннический сайт, внешне очень похожий на настоящий. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести на поддельной странице свои логин, пароль и одноразовый код, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Вишинг – метод, который заключается в том, что злоумышленники, используя телефонную коммуникацию и, играя определенную роль (сотрудника банка, покупателя и т.д.), под разными предлогами выманивают у держателя платежной карточки конфиденциальную информацию или стимулируют его к совершению каких-то действий со своим счетом или банковской платежной карточкой.

Фарминг – при фарминге на персональный компьютер жертвы устанавливается вредоносная программа, которая меняет информацию по IP-адресам, в результате чего обманутый пользователь опять таки перенаправляется на поддельный сайт без его ведома и согласия.

Взлом социальных сетей – взламывается страница пользователя и от его имени идут сообщения его друзьям, чаще всего с просьбой ”скинь денег на карточку“.

СМС-атаки – мошенник создает фейковый аккаунт в социальных сетях либо регистрируется, к примеру, в Viber, с симкарты, которая оформлена не на его. Далее высылает различные сообщения и

объявления. Например, ”Помогите на лечение ребенку“, размещая фото и реквизиты. Если это действительно реальный человек, то реквизиты легко проверяются. Но, к сожалению, люди не часто проверяют такую информацию.

Дорожное яблоко – этот метод состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников), на котором на самом деле вредоносная программа. Нашедший такой носитель из любопытства открывает его на рабочем компьютере, тем самым заражая всю сеть организации.

Кви про кво (в английском языке это выражение обычно используется в значении ”услуга за услугу“) – злоумышленник представляется, например, сотрудником технической поддержки и информирует о возникновении каких-то проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе ”решения“ такой проблемы злоумышленник подталкивает человека на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое вредоносное программное обеспечение.

Методов мошенничества, которые используют социальную инженерию, – множество. Самые распространенные для нашей страны – фишинг, вишинг, взлом социальных сетей. Главный способ защиты от мошенников, использующих методы социальной инженерии, это проявление бдительности и осторожности.

Давайте рассмотрим **самые частые ухищрения**, которыми пользуются кибермошенники чтобы достичь желаемого и получить чужие деньги.

Слайд 9. Схема 1. Поддельные продавцы, поддельные покупатели…

Сегодня многие из нас пользуются популярными площадками для продажи или покупки товара как у магазинов, так и у частных лиц. Безусловно, крупным интернет-площадкам казалось бы нет смысла не доверять. Но и тут нас могут ожидать подводные камни.

Итак, схема ”разводки“ продавцов:

Преступник находит продавца на площадке объявлений, копирует его контактные данные, но на площадке не пишет, так как его могут заблокировать. Ищет номер продавца в мессенджерах, представляется якобы покупателем с интернет-площадки, на которой размещен товар, говорит, что готов купить товар по предоплате. Затем высылает продавцу ссылку на поддельную страницу предоплаты, где продавцу

нужно ввести номер своей банковской платежной карточки для того, чтобы получить деньги от покупателя. Естественно, никаких денег продавец не получит – как только он введет свои персональные данные, преступник получит доступ к его счету.

Схема ”разводки“ покупателей:

Преступник выставляет товар с очень выгодной ценой. Когда потенциальный покупатель пишет ему, злоумышленник под любым предлогом предлагает перейти в мессенджер. Говорит, что в мессенджере удобнее общаться, можно созвониться и т.п. Затем преступник уговаривает покупателя на предоплату по одной из причин: уехал из города, боится встречаться во время эпидемии коронавируса, нет времени и т.д. А чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств, которая появилась на данной интернет-площадке: если доставки не будет, компания автоматически вернет средства на карточку. Злоумышленник также высылает покупателю ссылку на поддельную страницу доставки, которая имитирует страницу данной интернет-площадки, где нужно ввести данные банковской платежной карточки, чтобы совершить предоплату. Как только пользователь вводит данные своей банковской платежной карточки, со счета списываются деньги, товар не приходит.

Эта ситуация может быть реализована мошенниками в различных вариантах. Например, после того, как предыдущая уловка сработала, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем. Он скажет, что произошла ошибка, товар уже забрали (или передумал подавать), и он готов вернуть деньги. Далее он высылает ссылку на поддельную страницу возврата средств, где покупателю нужно ввести данные своей карточки и точную сумму, которую ему должны вернуть. После того, как покупатель вводит данные своей карточки, с него повторно списывается та же сумма или (если повезет) все деньги.

Как обезопасить себя:

Ведите переписку только в рамках интернет-площадки, на которой находитесь. Как правило, подобные сайты блокируют возможность отправлять ссылки на сторонние сайты, и это сделано специально для того, чтобы оградить людей от попыток недобросовестных пользователей увести их на мошенническую страницу.

Не переходите по ссылкам, которые вам высылают посторонние люди.

Если нужно перевести деньги на другую карточку, то пользуйтесь мобильным приложением от вашего банка, либо же самостоятельно заходите на страницу вашего банка.

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;

Если сайт содержит грамматические или орфографические ошибки, неправильное название организации, ”поехавшую“ верстку то это повод насторожиться. Крупные компании имеют в штате или привлекают профессиональных дизайнеров, копирайтеров, редакторов и корректоров, которые строго следят за соблюдением правил оформления сайта.

Надо быть очень осторожными, если кто-то запрашивает вашу личную информацию (персональные данные).

Слайд 10. Схема 2. Не верь чужим речам

Сегодня злоумышленники часто звонят пользователям не по телефону, а в мессенджерах, например по Viber с поддельных аккаунтов различных банков и представляются их сотрудниками. При этом в качестве фотографии такого аккаунта используют логотип банка, а название аккаунта идентично названию банка. Злоумышленники под разными предлогами пытаются узнать у пользователей данные их банковских платежных карточек.

Мошенники могут рассказывать разные ”легенды“: 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“ карточки 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.

Также мошенники могут позвонить от имени службы безопасности банка и сообщить, что проводят расследование хищения денег клиента работником самого банка. При этом попросят не перезванивать в банк, поскольку звонок может помешать расследованию, и даже могут предупредить об ”уголовной

ответственности“ за препятствование расследованию. Для убедительности мошенники будут ссылаться на произвольный номер статьи Уголовного кодекса. Далее звонок переключается на псевдо-сотрудника правоохранительных структур (милиции, прокуратуры и др.), который продолжит вводить вас в заблуждение.

Мошенники также могут предложить установить специальное приложение, которое на самом деле служит для удаленного управления устройством и позволяет получить доступ к счету клиента для несанкционированного перевода денежных средств.

Как обезопасить себя:

Важно всегда помнить, что сообщать кому-то информацию о своей банковской платежной карточке, пароли и коды доступа, паспортные данные ни в коем случае нельзя.

Не паникуйте, если вам сообщают о блокировке счета или каких нибудь неприятностях.

Уточните ФИО и должность звонящего и скажите, что перезвоните ему сами.

Положите трубку и наберите официальный номер банка сами. Но даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер колл-центра банка вручную. Телефон банка можно найти на обратной стороне банковской платежной карточки или на официальном сайте банка.

Слайд 11. Схема 3. Мошенники в социальных сетях

В социальных сетях также орудуют мошенники. Нередко они умело маскируются под родственников, друзей, возлюбленных, выбранных для обманной комбинации. Большинство онлайн-мошенников действуют по стандартной схеме: взламывают учетную запись пользователя в социальной сети и пишут его знакомым.

Чаще всего преступники просят отправить реквизиты банковской платежной карточки, якобы они хотят переслать вам деньги. Или же под именем вашего друга говорят, что попали в трудную ситуацию и просят перевести им деньги. Арсенал злоумышленников очень широк и предлоги бывают абсолютно разные. К примеру, они могут утверждать, будто их карточка заблокирована, или же давят на жалость: мол, им срочно нужно оплатить операцию. Особенно изощренные могут даже подражать стилю общения человека, от лица которого отправляют сообщения, и еще больше входят в доверие. Если кто-то из друзей попадается на удочку и скидывает мошеннику свои конфиденциальные данные, то вуаля – личные данные и деньги в руках мошенника.

Тот человек, кого взломали, ничего не подозревает о мошенничестве, и поймет об этом только тогда, когда не сможет войти в свой аккаунт, ведь пароль уже изменен.

Невнимательность и пренебрежение минимальными мерами финансовой безопасности – основные причины, по которым человек может подвергаться атакам киберпреступников.

Иногда киберпреступники и вовсе не затрагивают в своих сообщениях финансовые вопросы. Взломав страницу в соцсети, злоумышленник может попросить проголосовать за девушку в некоем фотоконкурсе. Перейдя по ссылке в сообщении, пользователь попадает на поддельную (фишинговую) страницу, где необходимо ввести персональные данные.

Как обезопасить себя:

Если кто-то из друзей в соцсети просит перечислить деньги на карточку или мобильный телефон либо вы замечаете иную подозрительную активность, свяжитесь с человеком альтернативными способами и попросите прояснить ситуацию.

Также вы можете установить приложение, с помощью которого вход в аккаунт подтверждается приходящим на телефон кодом. Такая двойная защита учетной записи оставляет взломщикам меньше шансов.

Используйте сложный пароль и не сохраняйте его в браузере.

Не пользуйтесь для входа в социальные сети чужими устройствами. Но если это все-таки необходимо, то надо проверять не сохранились ли ваши персональные данные на чужом устройстве.

Пользуйтесь антивирусным программным обеспечением и обновляйте его.

Слайд 12. Заключение

Этот урок был подготовлен, чтобы познакомить вас, дорогие ребята, с новинками технологий в финансовой сфере, а также помочь безопасно ориентироваться в цифровом мире денег. И это очень актуально сегодня – в эпоху коронавируса. Теперь вы знаете как нужно себя вести, чтобы умело пользоваться достижениями цифровых технологий и уберечь свои деньги от мошенников.

Но злоумышленники изобретательны и постоянно придумывают все новые и новые схемы обмана. Поэтому главный способ защиты от мошенников, использующих методы социальной инженерии, это проявление бдительности и осторожности!

Пусть у вас все получится. Спасибо за внимание!