**Сценарий мероприятия по теме: «Финансовая безопасность для всей семьи»**

Возможное количество участников – без ограничений

Возраст аудитории – 14+

Продолжительность мероприятия – 90 минут

При необходимости можно заранее распечатать и раздать слушателям таблицы из слайдов 4–7, чтобы они могли сделать там пометки.

| **№ слайда** | **Название слайда** | **Время** | **Примерный текст спикера** | **Взаимодействие с аудиторией** |
| --- | --- | --- | --- | --- |
| 1 | Финансовая безопасность для всей семьи | 1 минута | Здравствуйте! Меня зовут \_\_\_\_\_\_\_\_\_\_\_\_\_, я работаю в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в должности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Сегодня я проведу для вас мероприятие в рамках всероссийской просветительской Эстафеты «Мои финансы», проводимой по инициативе Минфина России. Этот этап эстафеты называется «Финансовая безопасность для всей семьи».  Финансовая безопасность семьи – это залог спокойствия и уверенности в завтрашнем дне. Сегодня мы разберемся, что такое финансовая безопасность и чем она определяется. | Представление |
| 2 | Разминка | 5 минут | Перед изучением отдельных аспектов финансовой безопасности давайте в качестве разминки проверим себя. Ответьте, как бы вы поступили в конкретных ситуациях:  1. СМС-сообщение говорит о том, что мне необходимо оплатить штраф за нарушение правил парковки переводом на конкретный номер телефона. Платить или нет?  2. Звонок от человека, который представился сотрудником службы безопасности банка и сообщил, что моя карта заблокирована в связи с подозрительной транзакцией. Называл меня по имени-отчеству, упоминал номер карты и просил продиктовать остальные реквизиты «для проверки». Что делать?  3. При работе в сети Интернет появилось всплывающее окно с приглашением войти в бесплатную онлайн-игру с большими выигрышами. Что делать?  4. Новый для меня интернет-продавец предлагает товар намного дешевле, чем все остальные, и просит 100% предоплату на номер телефона или электронный кошелек. Что делать?  5. В мессенджере получено сообщение от имени начальства. Руководитель пишет, что в компании произошла утечка данных и в ближайшее время сотрудникам будут звонить люди из органов, которым нужно оказать содействие. Что делать?  Возможные комментарии ведущего при ответах на вопросы:  1. Прежде чем оплачивать штрафы за парковку, необходимо проверить, действительно ли вам начислен штраф. Сделать это можно на портале ГИБДД, на портале «Госуслуги», в приложении «Парковки России», во многих банковских приложениях и т. д. Через эти сервисы можно и оплатить штраф. Оплата на конкретный номер телефона из СМС, скорее всего, является мошенничеством.  2. Никогда не сообщайте реквизиты своей банковской карты по телефону. Их запрашивают только мошенники. Если вы хотите проверить полученную информацию, отклоните звонок и сами позвоните в банк по номеру телефона, указанному на вашей банковской карте.  3. Не переходите по подозрительным ссылкам – с высокой вероятностью при этом на ваш телефон или компьютер будет установлена вредоносная программа, которая может дать мошенникам доступ к вашим личным и платежным данным и даже получить контроль над телефоном.  4. Никогда не пересылайте предоплату непроверенному продавцу, тем более если речь идет об оплате не на счет организации, а о переводе на номер телефона. Впоследствии вы не сможете доказать, что деньги были переведены вами за неполученный товар или услугу.  5. Проверьте, что вам действительно написал ваш руководитель, а не фейковый аккаунт. Перезвоните своему руководителю и уточните детали. Описываемая ситуация похожа на распространенную схему мошенничества. | Участники отвечают, ведущий дает комментарий в конце каждого ответа. |
| 3 | Определяем свою цифровую финансовую грамотность | 0 минут | А теперь давайте попробуем оценить уровень своей финансовой грамотности в контексте финансовой безопасности. |  |
| 4 |  | 2 минуты | А теперь давайте попробуем оценить уровень своей финансовой грамотности в контексте финансовой безопасности.  *Первое измерение* – *это базовые знания о современных цифровых финансовых продуктах и услугах.*  Знаете ли вы о существовании нетрадиционных финансовых продуктов и услуг, предоставляемых с помощью цифровых средств, таких как Интернет и мобильные телефоны? Эти услуги, как правило, делятся на четыре основные категории, хотя есть и дублирующие друг друга:  а) платежи: электронные деньги, кошельки для мобильных телефонов, криптоактивы, услуги денежных переводов;  б) управление активами: интернет-банкинг, онлайн-брокеры, робо-советники, торговля криптоактивами, управление личными финансами, мобильная торговля;  в) альтернативное финансирование: краудфандинг, одноранговое кредитование (P2P), кредитование онлайн-баланса, финансирование счетов-фактур и цепочки поставок и т.д.;  г) прочее: страховые услуги через Интернет и т. д. | Вопрос слушателям, обсуждение. Можно спросить, в чем преимущества /недостатки данных продуктов, чем пользуются наши слушатели. Если человек знаком с перечисленными инструментами, он мысленно ставит себе + в этой строчке. Если не знаком – минус. Чем больше плюсов, тем более человек финансово грамотен.  При необходимости можно заранее распечатать таблицы со слайдов 4–7 и раздать их слушателям, чтобы расставлять + и  – на бумаге. |
| 5 |  | 3 минуты | *Второе измерение цифровой финансовой грамотности* – *это осознание цифровых финансовых рисков****.***  Пользователи цифровых финансовых услуг должны знать о существовании онлайн-мошенничества и рисков кибербезопасности. Они сталкиваются с множеством потенциальных рисков, таких как:  а) **фишинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. С помощью различных уловок (рассылок электронных писем или сообщений в социальных сетях, мессенджерах от имени известных брендов, банковских служб и т. д.) мошенник предлагает пройти по фишинговой ссылке, чтобы заставить пользователя заполнить информацию о себе и раскрыть личные данные, такие как имена пользователей или пароли;  б) **фарминг** – вирус перенаправляет пользователя на ложную страницу, заставляя его раскрыть личную информацию;  в) **шпионское программное обеспечение** (ПО) – вредоносное ПО внедряется в персональный компьютер или мобильный телефон пользователя и передает личные данные;  г) **замена SIM-карты** – мошенник выдает себя за пользователя и получает SIM-карту пользователя, тем самым получая личные данные;  д) **профилирование** – мошенники собирают данные о жертве в социальных сетях, узнавая информацию о финансовом состоянии и о составе семьи, чтобы затем создать для жертвы правдоподобную легенду;  е) **взлом** – воры могут, например, взломать ваш пароль от социальной сети и совершать мошеннические рассылки от вашего имени. | Вопрос слушателям о рисках, с которыми им приходилось сталкиваться, обсуждение. |
| 6 |  | 1 минута | *Третье измерение цифровой финансовой грамотности* – *это цифровой контроль финансовых рисков, связанный с пониманием того, как можно себя защитить.*  Знаете ли вы, как использовать компьютерные программы и мобильные приложения, чтобы избежать рассылки спама, фишинга и т. д.? Как защитить свой личный идентификационный номер (PIN) и другую личную информацию при использовании финансовых услуг, предоставляемых с помощью цифровых средств? | Обсуждение. |
| 7 |  | 1 минута | *Четвертое измерение* –  *это знание прав потребителей и процедур возмещения ущерба в случаях, когда пользователи становятся жертвами вышеупомянутых рисков.*  Понимаете ли вы свои права и знаете ли, куда можно обратиться и как получить компенсацию, если вы стали жертвой мошенничества? Понимаете ли вы свои права в отношении своих персональных данных? | Обсуждение, подведение предварительных итогов. |
| 8 | Финансовое мошенничество | 3 минуты | Все ситуации, которые мы с вами обсудили, связаны с финансовыми услугами и в той или иной степени с возможным мошенничеством.  Финансовое мошенничество – совершение противоправных действий в сфере денежного оборота путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.   1. Одним из самых распространенных видов мошенничества являются **финансовые пирамиды**. Их суть заключается в привлечении вкладчиков и обещании им высокой прибыли. Вкладчики получают деньги от новых участников системы, пока система не рушится из-за отсутствия или недостаточного количества новых вкладчиков. Примером такого мошенничества является легендарная пирамида Сергея Мавроди – МММ. Это финансовая схема, которая обещала огромную прибыль за счет вкладов новых участников. Мавроди был осужден по статье 159 УК РФ – мошенничество в крупном размере. 2. Еще одним распространенным видом мошеннических действий в финансовой сфере являются **инвестиционные махинации на финансовых рынках**. Безответственные инвесторы могут убеждать желающих вложить деньги в несуществующие или невыгодные проекты, обещая высокую доходность. Нередко такие проекты являются полной выдумкой. 3. **Кредитные аферы** происходят, когда заемщик вводит кредитора в заблуждение, оформляя кредит на другое лицо (жертву мошенничества) с помощью поддельных документов. От такой схемы страдают не только граждане, но и банки, которым не возвращаются выданные в кредит средства. 4. **Аферы с использованием банковских карт** включают в себя несанкционированный доступ к финансовым счетам, кражу карт и использование украденной информации для совершения покупок. | Обсуждение:  Приходилось ли слушателям сталкиваться с мошенничеством в финансовой сфере? |
| 9 | Кто подвержен рискам? | 2 минуты | Принято считать, что на уловки мошенников попадаются в основном пожилые люди. Это не так. Стать жертвой аферистов может любой – независимо от возраста и уровня когнитивных способностей. Конечно, наличие критического мышления и высокий уровень финансовой грамотности помогают избегать опасности, но любой может ненадолго потерять бдительность, особенно в стрессовой ситуации. Как же мошенники добиваются таких успехов? В основе почти всех мошеннических схем лежит так называемая социальная инженерия – то есть аферисты используют в преступных целях особенности психологии. Чаще всего они стараются играть на сильных чувствах – страхе или азарте.  Основные орудия финансовых мошенников различны:   * страх людей перед неопределенностью; * желание граждан быстро увеличить свой доход; * подавленное моральное состояние, страх перед болезнью; * высокий уровень доверия к атрибутам различных структур (удостоверения, униформа; представление сотрудником банка, силовых структур, медицинским работником и т. п.). |  |
| 10 | Психологический портрет жертв телефонного мошенничества | 2 минуты | Различные виды кибермошенничества могут распространяться через социальные сети, мессенджеры, электронную почту и СМС-рассылки. Для каждого вида мошенничества характерен тот или иной прием социальной инженерии и когнитивные искажения, которые используются мошенниками для убеждения жертв в своей правоте. Например, для мошенничества с использованием кредитных карт или банковских счетов характерны следующие эффекты: профайлинг (профилирование) и эффект авторитета.  Рассмотрим, к примеру, телефонное мошенничество (так называемый **вишинг**). Какие же люди составляют группу риска, подверженную манипулятивному воздействию телефонных мошенников? Можно перечислить следующие характерные черты:   * возраст 50+ (впрочем, если вы моложе, это не дает вам никаких гарантий безопасности); * выраженные ценности безопасности; * высокий самоконтроль; * ставят интересы группы выше собственных; * склонны к сотрудничеству. |  |
| 11 | Приемы работы мошенников с сопротивлением клиентов | 3 минуты | Пользуясь недостаточным уровнем финансовой грамотности населения, мошенники:   * используют специфическую терминологию, надеясь произвести впечатление на своих жертв и создать ситуацию собственного превосходства; * создают иллюзию срочности или безотлагательности конкретных действий; * используют угрозы: угрожают мнимой уголовной ответственностью за разглашение банковской тайны, блокированием счета, арестом денежных средств при отказе сообщать личные сведения.   Любые способы преодоления опасной ситуации, которые предлагаются жертвой, мошенники искусно обесценивают. Например, мошенники убеждают жертву, что с ее карты вот-вот будут списаны все деньги, а в случае звонка в банк возникшая проблема не решится, поскольку службы банка не обладают нужными инструментами. При этом потраченное на такой звонок время, как и любое прерывание мобильного соединения, якобы приведет к потере денег.  На этапе перевода и получения денежных средств мошенники призывают клиента к помощи. Они предлагают принять активное участие в поимке сотрудника, по вине которого были скомпрометированы личные данные, отключено СМС-информирование или произошли еще какие-либо изменения персональной информации.  Эта ситуация позволяет мошенникам развивать два основных сценария.  **Первый сценарий**будет реализовываться, если жертва демонстрирует высокий уровень владения средствами электронного платежа. В этом случае мошенники сообщают, что нужно создать специальный защищенный счет, куда жертва должна будет перевести все свои денежные средства, или продиктовать специальные коды из СМС-уведомления.  **Второй сценарий**разрабатывается для тех, кто не обладает такими техническими возможностями. Им предлагается посетить отделение банка и совершить перевод через банкомат.  В навязанном телефонном разговоре необходимо обращать внимание на психологические признаки использования методов социальной инженерии или иного воздействия. |  |
| 12 | Понятие социальной инженерии | 1 минута | **Социальная инженерия** всегда направлена на пользователя, а ее цель – убедить человека раскрыть информацию или перечислить деньги. Сценариев и способов подобных атак множество, но все они рассчитаны на слабости и психологию людей. Например, мошенники получают доступ к счетам жертвы, не взламывая при этом банковский онлайн-кабинет. Путем последовательных манипуляций преступники уговаривают человека добровольно передать пароли или перевести деньги на нужный счет. **Обратная социальная инженерия** – это техника манипулирования, противоположная классической схеме, при которой преступник первым инициирует контакт. При обратной социальной инженерии человека обманом вынуждают самостоятельно связаться со злоумышленником.Сценарии такой социальной инженерии различны. Например, мошенник сперва саботирует работу сети, а затем выдает себя за технического специалиста, чтобы якобы помочь жертве решить проблему. Причем информацию об услугах такого «профессионала» пользователь замечает как бы случайно: в рекламе всплывающего окна или в рассылке. | Можно обратиться к аудитории, найти примеры, с которыми сталкивались слушатели, и обсудить их. |
| 13 | Этапы социоинженерных атак | 3 минуты | Принципы социальной инженерии строятся вокруг того, как люди думают и действуют. Главная задача – сыграть на чувствах и слабостях человека, вывести его из психологического равновесия, а после заставить совершить определенные действия. Для этого киберпреступники используют широкий арсенал приемов, а подготовка жертвы к обману иногда занимает несколько месяцев. Социоинженерных сценариев для кражи данных много. Но, как правило, подобные атаки проходят в несколько этапов:   1. **Подготовка**. Мошенники предварительно изучают конкретного человека либо группу людей (например, сотрудников определенной компании). Большинство информации, как правило, есть в открытом доступе: корпоративные сайты, фото и посты в социальных сетях. 2. **Установление контакта**. Инициировав взаимодействие, преступник строит доверительные отношения. Для этого мошенники апеллирует к каким-то фактам, событиям и информации, имеющим отношение к человеку или группе. Это имена и фамилии друзей, начальника, сведения о сделке, которую недавно провела компания, информация о том, что человек недавно обращался к врачу и т. д. 3. **Начало атаки**. Как только доверие установлено, жертву атакуют. Например, просят перейти по ссылке, переслать письмо, открыть зараженный файл или перевести деньги. 4. **Отключение**. Сразу после того, как пользователь выполняет требования, все контакты прекращаются. Через некоторое время пострадавший осознает, что его обманули. |  |
| 14 | Признаки использования методов социальной инженерии | 5 минут | В навязанном телефонном разговоре необходимо обращать внимание на психологические признаки использования методов социальной инженерии или иного воздействия.  Признаки использования методов социальной инженерии:   * ведение диалога по типу «суфлера», то есть с использованием типовых схем и скриптов диалога; * использование заученных фраз; * смена ролей от представителей кредитных организаций до сотрудников правоохранительных органов; * призывы к помощи поймать преступников.   При выражении жертвой недоверия или отказе предоставить какие-либо сведения потенциальная жертва сталкивается с прямым раздражением или наигранным удивлением.  Преступников могут выдавать акцент, безграмотная речь, низкая общая осведомленность или сниженная интеллектуальная функция, хамство, угрозы или шантаж. Мошенник в телефонном разговоре может перейти на крик, нецензурную брань, раздражение, оскорбление.  Какие речевые манипуляции используют телефонные мошенники?   * использование образа авторитетного лица, которое не позволяет безразлично относиться к его словам; * использование образов попавших в беду близких людей, что вызывает у потерпевших сильные эмоции, чувство сопереживания; * использование эффекта неожиданности, что создает ощущение растерянности; * прямое или косвенное указание на ограниченность времени для принятия решения; * использование конструкции «или-или» («или вы переводите средства, или ваш внук будет посажен в тюрьму» и т. д.); * «перетасовка» как упоминание только положительных или отрицательных фактов и умалчивание противоположных. | Какие речевые манипуляции используют телефонные мошенники?  Обсуждение. |
| 15 | Примеры искажений, которые мешают объективно оценивать информацию | 3 минуты | Давайте рассмотрим примеры искажений, которые мешают объективно оценивать информацию:  **Эффект третьего лица**. Людям часто свойственна чрезмерная самоуверенность. Они считают, что их, в отличие от других, сложно обмануть.  Э**ффект однородности чужой группы**. Мы не доверяем чужакам, но знакомые люди и вещи вызывают больше доверия, чем незнакомые, и мошенники этим пользуются – например, пишут жертвам с поддельных аккаунтов от имени руководителей, коллег, друзей и знакомых.  **Эффект якоря**. Он возникает, когда при принятии решения люди полагаются на первую полученную информацию, а любые следующие сведения подсознательно соотносят с ней.  **Предвзятость оптимизма**. Людям часто кажется, что с ними точно ничего плохого не случится. Это притупляет их бдительность.  **Ошибка выжившего**. Люди обращают внимание исключительно на успешный опыт и не принимают в расчет неудачи. Это приводит к ошибочным решениям. Так, например, если аферист сообщает, что 65% вкладчиков вложили деньги в какой-то финансовый инструмент и получили прибыль, немногие зададут себе вопрос, что произошло с деньгами остальных 35%.  При принятии решений людей часто подводят ошибки мышления. Также большую роль играют защитные реакции организма, которые включаются в момент опасности и вызывают определенные психологические состояния. |  |
| 16 | Способы защиты от социальной инженерии | 3 минуты | Как же не стать жертвой мошенников?   * не предоставлять личную информацию, если нет уверенности в том, кто ее запрашивает; * не раскрывать личную или финансовую информацию в электронной почте, социальных сетях, мессенджерах, не отвечать на подобные сообщения и не переходить по ссылкам из них; * не отправлять конфиденциальную информацию через Интернет, не проверив безопасность веб-сайта.   Киберпреступники часто используют электронные адреса, которые очень похожи на оригинальные. Для этого достаточно изменить или опустить несколько символов. Необходимо проверить, как на самом деле выглядит адрес. Вредоносные веб-сайты также могут использовать похожий на настоящий домен или сокращенный URL. Электронные письма или сообщения в социальных сетях и мессенджерах с просьбой открыть вложение – распространенный способ доставки вредоносного ПО. |  |
| 17 | Утечка персональных данных | 5 минут | Особую проблему составляет утечка персональных данных. Это означает, что персональная информация похищена без ведома человека. Чаще всего причиной становятся кибератаки на приложения и сайты. Украденная информация появляется в открытом доступе и может быть использована мошенниками для фишинговых атак, взлома ваших аккаунтов и банковских карт.  Обычно публикуют следующие данные:   * адрес электронной почты; * номер телефона; * фактический адрес; * дату рождения, пол; * логин, пароль; * историю покупок в онлайн-магазинах; * данные банковских карт.   Отдельные утечки могут не представлять опасности. Например, если в доступ попал логин или пароль, но непонятно, от какого они аккаунта, мошеннику будет сложно нанести вам вред.  Наибольшую опасность представляет утечка банковских данных. В этом случае лучше немедленно обратиться в банк и заблокировать счета.  Признаком того, что учетная запись скомпрометирована, могут быть попытки авторизации по номеру телефона или адресу электронной почты, перевода денег с карты, письма с просьбой перейти по ссылке.  Мошенники могут взломать пароли методом их подбора, при котором посредством алгоритмов генерации перебирают все возможные комбинации символов. Также существуют программы, которые подставляют общие слова в поле пароля в поисках подходящего. |  |
| 18 | Защита персональных данных | 2 минуты | Кража персональных данных – очень распространенное правонарушение. Информация о человеке может многое рассказать о нем и стать поводом для шантажа, мошенничества или фишинга. При этом владелец нередко сам сообщает важную информацию о себе в социальных сетях, когда делится своими успехами и планами, или размещает информацию на досках объявлений при продаже-покупке вещей.  Ни в коем случае нельзя передавать третьим лицам пароли, коды подтверждения, присылаемые банком, не следует заходить в свой интернет-банк, соцсети и почту с компьютеров других людей. Если все же необходимо использовать чужой компьютер, нужно разлогиниться, а затем почистить куки и кэш в браузере. При оплате онлайн-покупок в интернет-магазинах окно для ввода номера карты должно появляться сразу после нажатия кнопки «Оплатить». Если всплывают промежуточные страницы со ссылками, это повод задуматься о надежности интернет-магазина и в принципе о намерениях его владельцев. За кражу персональных данных предусмотрена административная и уголовная ответственность. |  |
| 19 | Некоторые актуальные схемы мошенников | 7 минут | Мошенники регулярно придумывают новые способы обмана и модернизируют старые. В настоящее время самыми распространенными стали следующие схемы, рассмотрим и обсудим некоторые из них.**«Пришлите QR-код»****Схема:** Банки дают россиянам возможность снимать деньги с карты с помощью QR-кода – нужно просто сгенерировать его в мобильном приложении и поднести к сканеру банкомата. Злоумышленники звонят россиянам под видом сотрудников банка, сообщают, что к ним поступил несанкционированный запрос на снятие денег со счета, и просят прислать QR-код, чтобы отменить операцию, а затем получают по нему средства в банкомате.**Как это работает:** В этом случае аферисты используют один из самых мощных рычагов давления – чувство страха. *«Почти во всех классификациях страха присутствуют «социально-биологические страхи». В частности, это страх за жизнь и здоровье близких, страх потерять деньги, то есть лишиться ресурсов, необходимых для выживания.***Что делать:** сразу прервать разговор: банки рассылают информацию только через свои официальные каналы. Вы сами можете позвонить в банк по номеру телефона, указанному на банковской карте, чтобы проверить информацию.**«Одолжишь 50 тысяч рублей до вечера?»****Схема:** Злоумышленники научились подделывать аудио и видео с помощью нейросетей. Россияне получают в Telegram или во ВКонтакте аудиосообщения и видеокружочки от знакомых или родных с просьбой одолжить денег.**Как это работает:** ИИ пока не умеет идеально подделывать видео – есть незначительные размытия и искажения, человек на записи редко моргает, а его губы не всегда двигаются естественно, но потенциальные жертвы не всегда обращают на это внимание. *«Мы видим знакомое лицо, и это априори вызывает доверие, включается эмпатия — сложно отказать в помощи близкому человеку».***Что делать:** Связаться с человеком в другом мессенджере или позвонить ему, чтобы уточнить, действительно ли он обращался к вам с такой просьбой.**«Ваше банковское приложение устарело»****Схема:** Злоумышленники звонят от имени банков с просьбой обновить мобильное приложение, потому что предыдущее скоро перестанет работать. Аферисты направляют ссылку для скачивания новой версии. Это вирусная программа, которая крадет пароли и реквизиты карт. Если жертва сомневается, мошенники говорят, что банк будет вынужден в течение 15 минут заблокировать средства на счету на 90 дней – в целях безопасности, естественно.**Как это работает:** Мошенники действуют по проверенной схеме: запугивают и торопят, чтобы не дать жертве времени обдумать ситуацию, ставят условие – «сейчас или будет поздно». *Аферисты вызывают у людей стресс: потенциальная потеря доступа к деньгам повышает уровень адреналина в крови.* **Что делать:** Как можно быстрее закончить разговор – дождаться, когда уровень адреналина упадет и вернется способность мыслить логически. Банки распространяют информацию о новых версиях приложений только через официальные каналы информации.**4. «Обменяем кешбэк на рубли»****Схема:** Злоумышленники под видом сотрудников банка звонят россиянам и предлагают обменять накопленный за покупки кешбэк, бонусные баллы или мили на рубли. Чтобы перевести кешбек в деньги, аферисты просят назвать данные карты и СМС-код от банка, а затем – крадут деньги со счета жертвы.**Как это работает:** Жадность – сильная эмоция, на которую часто давят мошенники. *Мошенники в красках описывают баснословную прибыль.* **Что делать:** сразу положить трубку и набрать номер горячей линии банка, чтобы прояснить ситуацию. С вероятностью 99,9% это были мошенники | Обмен опытом: Какие еще схемы вам известны? С какими сталкивались? Как поступили в сложившейся ситуации? |
| 20 | Финансовая безопасность в цифровом мире | 2 минуты | Одним из важных признаков финансово грамотного человека становится знание правил кибербезопасности и, в частности, умение распоряжаться финансами в цифровом мире. О том, какие правила обращения с деньгами действуют в сети, полезно знать не только взрослым, но и детям.  Определение цифровой финансовой грамотности должно опираться на способность человека к совершению разумных финансовых операций в цифровом формате. Цифровая финансовая грамотность – способность принимать разумные решения по использованию цифровых финансовых услуг и управлению цифровыми финансовыми активами наиболее экологичным и безопасным способом.  Для этого требуется знание различных финансовых продуктов и услуг, включая банковские счета, инвестиции, страхование, пенсии, кредиты, ипотечные кредиты и другие цифровые платежные системы, а также понимание того, как использовать эти продукты и услуги для управления своими финансами и защиты от финансовых рисков. |  |
| 21 | Фишинг, вишинг, смишинг, фарминг | 7 минут | Из-за стремительного развития большого количества ресурсов появилось множество видов мошенничества, направленных на получение конфиденциальных данных и дальнейшее их использование в корыстных целях. Давайте еще раз вспомним эти определения.  **Фишинг** – вид интернет-мошенничества, направленный на получение доступа к логинам и паролям пользователей. Злоумышленники делают массовые рассылки электронных писем от имени популярных брендов, личных сообщений от имени банков в соцсетях. В письме есть прямая ссылка на сайт, внешне похожий, а то и вовсе идентичный настоящему. Когда человек переходит на эту страницу, мошенники пытаются побудить его ввести свои логин и пароль для доступа к определенному сайту.  Не следует обходить стороной такую актуальную проблему, как **вишинг** (англ. vishing – voice+phishing) – это одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка. Например, на телефон поступает звонок от сотрудника банка и оператор предупреждает, что если прямо сейчас не будет предоставлена полная информация банковской карты ему по телефону, то карту заблокируют. Доверчивый пользователь, слыша подобную угрозу, сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из СМС.  Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции.  Еще одним видом обмана посредством сервисов связи является **смишинг** (англ. smishing – sms+phishing). Данная преступная схема направлена на переход пользователем по вредоносной ссылке из СМС-сообщения. Смишинг-сообщение может иметь вид сообщения от известного банка, знакомой компании или быть просто оповещением о внезапном выигрыше в лотерее или в крупной акции. В случае с СМС выявить подвох несколько сложнее, нежели при фишинге, т.к. сообщения небольшие и содержат меньше информации, помимо самой ссылки. Скорее всего, это будет предложение перейти по ссылке и ввести данные или же просто позвонить или отправить обратное сообщение.  **Фарминг** – вид мошенничества, при котором вредоносный код устанавливается на компьютер или сервер жертвы. Этот код меняет IP-адреса, из-за чего пользователь перенаправляется на поддельные веб-сайты, сам того не зная, и там вводит свои личные данные. Этот способ часто применяется в отношении онлайн-банков или других финансовых сервисов. Подмена настоящего сайта на мошеннический производится посредством использования кэша DNS на конечном устройстве пользователя или же на сетевом оборудовании провайдера. Вирус активирует свою деятельность только в момент перехода на интересующую страницу. Уберечься от фарминга достаточно сложно, так как процесс подмены сайта происходит незаметно. |  |
| 22 | Как защититься от фишинга, вишинга, смишинга и фарминга? | 5 минут | [Как же защититься от фишинга, вишинга, смишинга и фарминга?](https://www.protectimus.com/blog/ru-phishing-vishing-smishing-pharming/#%D0%9A%D0%B0%D0%BA%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B8%D1%82%D1%8C%D1%81%D1%8F?)  Не переходить по ссылкам в письмах и СМС-сообщениях, не использовать нелицензионное ПО и не скачивать программное обеспечение на незнакомых сайтах, использовать надежные проверенные браузеры и антивирусы, активировать двухфакторную аутентификацию, не доверять первому встречному или звонящему и всегда перепроверять полученную информацию.  Кроме того, следует всегда придерживаться следующих рекомендаций при использовании интернета и любых других ресурсов связи:   * всегда обращайте внимание на отправителя и тему сообщения. Если они выглядят подозрительно, просто удалите письмо; * в письме с неизвестным отправителем не стоит переходить по предложенным ссылкам; * ни в коем случае не давайте ответы на письма, запрашивающие личную информацию; * следите за ошибками в тексте. Если они есть, то, скорее всего, письмо – обман; * файлы, прикрепленные к письму, с расширениями .exe, .msi, .bat, .pif, .com, .vbs, .reg, .zip, .apk, и т. д. могут устанавливать вредоносное программное обеспечение, не стоит их открывать.   Что касается технических средств защиты от фишинга и фарминга, то обратите внимание на следующие возможности:   1. В основных браузерах существует антифишинговая система со списком сайтов злоумышленников, которая предупреждает пользователя о переходе на вредоносный сайт. Такие же системы используют и многие ресурсы. 2. Антивирусное программное обеспечение дает довольно надежную защиту. 3. Некоторые спам-фильтры, используемые сервисами электронной почты, позволяют автоматически отсеивать письма злоумышленников. 4. Обязательно необходимо использовать [двухфакторную аутентификацию](https://www.protectimus.com/blog/ru-two-factor-authentication-how-it-works/). Если все аккаунты будут дополнительно защищены одноразовыми паролями, это в разы усложнит жизнь злоумышленникам. |  |  |  |  |
| 23 | Надежные пароли | 3 минуты | Необходимо понимать, как важны надежные пароли.  Пугающе большое количество пользователей использует во всех своих аккаунтах один и тот же пароль. В лучшем случае – два. Это все равно, что иметь один ключ на все случаи жизни: для квартиры, гаража, рабочего кабинета, банковского сейфа. Потеря такого ключа подвергнет серьезной опасности абсолютно все объекты, защищаемые им.  Надежные пароли – сложные, длинные, нестандартные. Очень важно определиться с тем, какой пароль надежный. Правильный пароль должен быть достаточно длинным – никак не менее 8–10 знаков.  Существуют оригинальные методики создания паролей – одновременно и надежных, и запоминающихся. Одной из них является мнемоническая техника. Для придумывания пароля нужно подобрать значимую для конкретного человека фразу из песни, фильма, любимого стихотворения. Далее следует выписать начальные буквы первых 5–7 слов, а между ними вставить какой-либо специальный символ. Для посторонних такая комбинация не будет иметь смысла, а хозяин пароля всегда сможет легко его вспомнить. Такой «ключ» не придется хранить на жестком диске или листочке бумаги, где до него смогут добраться мошенники. Пример приведен на слайде. |  |  |  |  |
| 24 | Современные способы мошенничества с использованием ИИ | 3 минуты | Нейросети развиваются на наших глазах, но, помимо плюсов, прогресс открывает для преступников всё больше способов обмана.  Активно распространяются дипфейки, голосовые клоны и фишинговые атаки с использованием искусственного интеллекта.  **Дипфейк** – это коммуникационный продукт, созданный с помощью искусственного интеллекта, имеющий определенную цель (получение выгоды или нанесение ущерба), направленный на создание фальсифицированного образа.  Слово deepfake появилось несколько лет назад и объединяет в себе два понятия:**глубокое обучение** (deep learning), то есть обучение нейросетей, и **подделка** (fake). Технология дипфейков заключается в синтезе искусственным интеллектом (ИИ) человеческих изображений.  Визуальные подделки можно разделить на 5 типов  1. Face-swapping – замена лица.  2. Lip-syncing – синхронизация губ.  3. Puppet master – реконструкция лица (куклоформирование).  4. Face-synthesis – синтез лиц.  5. Facial Attribute Manipulation – изменение атрибутов лица.  Какие признаки помогут распознать подделку?   * объект двигается неровно; * голос плохо синхронизируется с движениями губ; * у моделей может не совпадать цвет правого и левого глаза; * объект может вообще не моргать (или моргать странно).   Особое внимание нужно обращать на глаза и зубы: в глазах могут отсутствовать блики, а зубы – казаться плохо прорисованными. Дипфейки представляют собой захватывающее развитие технологий 21-го века, но они также потенциально невероятно опасны, представляя огромную угрозу для персональных данных, денег и бизнеса. |  |
| 25 | Современные способы мошенничества – атака с подменой | 3 минуты | Еще один способ мошенничества – это атаки с подменой. Основной мотив подменных атак заключается в сборе пользовательских данных для использования в дальнейших атаках.  Это ситуация, в которой человек или программа успешно подделывает личность и выдает себя за другого, чтобы получить доступ к конфиденциальной и засекреченной информации.  Чтобы атаки были успешными, киберпреступники сочетают саму подмену с тактикой социальной инженерии. Для этого киберпреступники используют множество различных методов:   * **подмена идентификатора вызывающего абонента** – может показаться, что звонок поступает от кого-то, кого вы знаете (например, от вашего коллеги, кого-то из вашего списка контактов, компании, которой вы доверяете), в попытке убедить вас поднять трубку. Когда вы отвечаете, киберпреступники используют тактику социальной инженерии, чтобы держать вас на телефоне и обманом заставить действовать; * **подмена электронной почты** использует доверие и наивность пользователей, чтобы обманом заставить их открывать вредоносные вложения, переходить по поддельным ссылкам, отправлять конфиденциальные данные и даже переводить корпоративные средства; * **подмена веб-сайтов** включает в себя разработку поддельных веб-сайтов, которые напоминают надежный веб-сайт. Киберпреступники используют поддельные веб-сайты, чтобы украсть информацию о кредитной карте, захватить имя пользователя и пароль (подделка входа) или загрузить вредоносное ПО на устройство. |  |
| 26 | Дроппинг | 5 минут | В последнее время случаи мошенничества с банковскими картами становятся все более изощренными.  Мошенники привлекают к своей деятельности подставных лиц, называемых дропами или дропперами (от английского drop – сбрасывать). Как правило, они просят перевести деньги с одной карты на другую, снять и передать наличные курьеру или внести их на чужой счет. В большинстве случаев это делается за вознаграждение.  Дропами становятся либо осознанно – человек сам соглашается стать участником мошеннической схемы, либо неумышленно – когда он сам стал жертвой злоумышленников и его используют втёмную. Например, к вам на счет «по ошибке» поступили деньги, вас просят вернуть их, но перевести уже на другой счет. В этом случае необходимо не предпринимать никаких действий по счету, а обратиться в свой банк и в правоохранительные органы.  Дропы различаются по виду выполняемых ими операций:   * «дропы-обнальщики» снимают в банкомате поступившие им денежные средства и передают их мошенникам или другим посредникам; * «дропы-транзитники» принимают денежные средства на свой счет, а затем переводят их на указанные мошенниками счета; * «дропы-заливщики» получают наличные денежные средства от других дропперов, вносят их на собственный счет, а затем переводят на счета мошенников.   Дропам грозит до шести лет лишения свободы и блокировка всех банковских карт. Более того, с июля 2024 года, если имя человека, замеченного в мошеннической схеме с использованием подставных лиц, попадет в специальную базу данных Банка России, такой человек не сможете пользоваться банковскими услугами. |  |
| 27 | Как бороться с мошенничеством? | 3 минут | Выделим несколько правил безопасности   * Обращать внимание, куда вам позвонили. Если звонок поступил в мессенджер, а представляются банком, кладите трубку и блокируйте номер. Банки, мобильные провайдеры и даже сотрудники правоохранительных органов никогда не будут звонить вам в мессенджеры. * Придумать кодовую фразу в общении с близкими. Чтобы не обмануться современными методами мошенников, такими как подделка голоса, заранее условьтесь со своей семьей о конкретной кодовой фразе, которую один из вас назовет, если засомневается в подлинности звонка. * Проверять номер телефона. Допустим, вам позвонили через обычную сотовую связь, однако номер телефона немного отличается от привычного. Заметили несоответствие – не берите трубку. Используйте программы для определения номера. Специализированные решения содержат регулярно обновляемые базы и позволят вам в большинстве случаев заблаговременно выявлять мошенничество или даже автоматически блокировать все подозрительные звонки. * Не предоставлять личную информацию. Никогда не сообщайте свои личные данные, финансовую информацию или одноразовые коды из СМС, даже если звонящий утверждает, что представляет банк, полицию или другую известную организацию. * Настроить двухфакторную аутентификацию. В эпоху цифрового мошенничества двухфакторная аутентификация является необходимым минимумом, позволяющим спать спокойно и не переживать о своих данных. |  |
| 28 | Как защититься от кредитного мошенничества? | 5 минут | В настоящее время часто встречается мошенничество в финансовой сфере, связанное с кредитованием. И здесь нужно быть не только финансово грамотным, но и заранее обезопасить себя от недобросовестных действий злоумышленников.К примеру, можно регулярно проверять свою кредитную историю. Кредитная история показывает, когда и в какие банки и микрофинансовые организации человек обращался за кредитами, на какие суммы брал займы. Чтобы получить свою кредитную историю, сначала нужно узнать, в каких Бюро кредитных историй она хранится. Сделать это удаленно можно через портал «Госуслуги» или [официальный сайт Банка России](https://cbr.ru/ckki/zaprosy_v_ckki/). Кредитную историю стоит регулярно проверять, чтобы, в том числе, вовремя узнать, если на вас был оформлен мошеннический кредит. Такое может случиться, например, если вы потеряли паспорт или ваши данные утекли в сеть.  Однако с 1 марта 2025 года гражданин может установить в своей кредитной истории самозапрет на заключение с ним кредитными организациями и (или) микрофинансовыми организациями договоров потребительского кредита (займа).  Основные цели использование механизма самозапрета – это профилактика мошенничества и сохранение ваших денежных средств.  Самозапрет можно установить, даже если у человека нет кредитной истории. На основании заявления о самозапрете, поданного через МФЦ или «Госуслуги», квалифицированные бюро кредитных историй сформируют кредитную историю человека и включат в нее сведения о самозапрете.  Обратите внимание, что самозапрет на кредиты НЕ распространяется на:   * уже полученные кредиты и кредитные карты; * ипотеку (она обеспечена залогом недвижимого имущества); * автокредиты (обеспечены залогом транспортного средства); * основные образовательные кредиты (на оплату обучения, которая сразу перечисляется в образовательную организацию). |  |
| 29 | Финансовая грамотность – это залог финансовой безопасности | 1 минута | Для того чтобы обезопасить себя и свою семью, необходимо повышать свою финансовую грамотность и формировать свою финансовую культуру.  Финансовая грамотность – это залог финансовой безопасности для вас и вашей семьи! Повышение финансовой грамотности позволит не только изменить свое финансовое поведение, сделать его более осознанным, развивать и поддерживать финансовую дисциплину, но и заставит хорошо подумать, прежде чем вложить деньги в финансовую пирамиду, совершить онлайн-покупку на подозрительном сайте, сообщить «сотрудниками Центробанка» или «правоохранительных органов» ПИН-коды, номера банковских карт, секретные коды из СМС или перевести по их просьбе деньги на «безопасный счет». | Можно спросить слушателей, каким они видят портрет финансово грамотного человека с позиции финансовой безопасности.  Обсуждение и составление портрета финансово грамотного человека. |
| 30 | Заключение | 1 минута | Больше информации вы можете получить на портале «Мои финансы» и в социальных сетях проекта.  Удачи Вам и спасибо за внимание! | Прощание |