**Приложение 7**

**ЭТАП 1: ПРЕДСТАВЛЕНИЕ И АНАЛИЗ ПРАКТИЧЕСКОЙ СИТУАЦИИ, СВЯЗАННОЙ С ФИНАНСОВОЙ БЕЗОПАСНОСТЬЮ (9 МИН.)**

На этом этапе спикеру важно оперировать терминологией.

**Подсказки по терминологии для спикера**

**Какие виды финансового мошенничества вы знаете?**

**Варианты мошенничества, которые могут назвать учащиеся**

| Вид мошенничества | Определение |
| --- | --- |
| Фишинг | Получение конфиденциальных данных о банковской карте (номер, ПИН-код) путем рассылки электронных писем об изменениях в системе безопасности банка и необходимости предоставить информацию по карте. |
| Фарминг | Это более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации. |
| Золото Лимпопо (Нигерийские письма) | Это вид интернет-мошенничества, когда злоумышленник пытается выманить у пользователя деньги или получить доступ к его банковскому счёту. |
| Злой близнец | Это кибер-атака, при которой хакер создает поддельную точку доступа Wi-Fi, имитирующую подлинную беспроводную сеть, к которой могут подключаться пользователи. Как только пользователь подключается к такой сети «злого близнеца», хакеры могут получить доступ к данным пользователя: от его сетевого трафика до личных регистрационных данных. |
| Снифферинг | Это способ мошенничества, при котором злоумышленник использует анализатор проходящего трафика Интернет-сети («сниффер») – специальную компьютерную программу для перехвата данных с возможностью их декодирования и анализа. Снифферинг особенно популярен в людных местах, везде, где есть общедоступная сеть wi-fi. |
| Кликджекинг | Это технология обмана пользователей Интернета, при котором мошенник получает доступ к конфиденциальной информации или к компьютеру пользователя. Например, на странице пользователя поверх видимых элементов располагают невидимые, и пользователь, совершая клик, подписывается на какую-то группу. |
| Кликфорд | Это разновидность мошенничества в сети (мошенническое нажатие) в виде обманных кликов на рекламные ссылки, которые совершают лица, не заинтересованные в рекламном объявлении. Такого рода ложные клики повышают расходы рекламодателя на показы объявлений. От кликфорда владельцы рекламных сетей могут потерять доверие рекламодателей и прибыль. |
| Семь кошельков | Один из видов мошенничества в сети, когда пользователь получает письмо с предложением перевести небольшую сумму на несколько электронных кошельков в надежде на то, что следующие участники тоже перечислят деньги на электронные кошельки, среди которых будет указан и его электронный кошелёк. Гарантия получения денег в свой электронный кошелёк полностью отсутствует. |
| Смишинг | Это вид мошенничества, при котором пользователь получает СМС-сообщение, в котором с виду надежный отправитель просит указать какую-либо ценную персональную информацию (например, пароль или данные кредитной карты). |
| Скимминг | Кража данных с банковской карты путем установки на банкомат специального считывающего устройства с накладной клавиатурой и (или) миниатюрной камеры для записи ввода ПИН-кода. |
| Траппинг | Мошенничество с целью получения банковской карты путем установки в банкомате устройства, не возвращающего карту из банкомата, а также информации о ПИН-коде |
| Шимминг | Усовершенствованный вид скимминга. В банкомат помещается устройство меньшего размера. Это устройство, толщиной не больше человеческого волоса, очень трудно обнаружить. Но шиммер не умеет считывать ПИН-код. |

**Что такое финансовое мошенничество?**

**Финансовое мошенничество** — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения

**Что грозит за мошенничество?**

**Штраф** в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года; **обязательные работы** на срок до трехсот шестидесяти часов; **исправительные работы** на срок до одного года; **ограничение свободы** на срок до двух лет; **принудительные работы** на срок до двух лет; **арест** на срок до четырех месяцев; **лишение свободы** на срок до двух лет.

**Что такое дроппинг?**

**Дроппинг** – вербовка в схему отмывания денег.

**Кто такой дроп (или дроппер)?**

**Дроп –** подставное лицо, задействованное в нелегальных схемах по обналичиванию денег.

**Что такое вишинг?**

**Вишинг – э**то форма финансового мошенничества, когда злоумышленники используют телефонные звонки и голосовые сообщения, чтобы обманом заставить жертву раскрывать конфиденциальную информацию, такую как номера счетов, пароли и данные карт для доступа к его деньгам.

**Что такое мошенничество с использованием QR-кода?**

**Мошенничество с использованием QR-кода** –использование сгенерированного QR-кода для кражи денег у ничего не подозревающих людей.

**Что такое бот-помощник?**

**Бот-помощник** – это виртуальный ассистент, который отвечает на однотипные вопросы. Обычно FAQ-боты используются на сайтах, в приложениях или мессенджерах.

**ЭТАП 2: ДЕТЕКТИВНАЯ ИГРА (20 МИН.)**

На этом этапе спикеру важно отслеживать тайминг, но давать какие-то пояснения уже нельзя, все пояснения – при подведении итогов.

**ЭТАП 3: ТВОРЧЕСКАЯ МАСТЕРСКАЯ (10 МИН.)**

На этом этапе спикеру важно донести информацию, что требуется составить алгоритм и внести в прилагаемую схему. По заданию предлагаются три пространства – телефон, соцсети и объявление на бумаге. Но спикер не ограничивает команды, можно указать и свои пространства, если команды понимают, какую ситуацию могут предложить.

Важно по трем направлениям (пространствам) описать ситуацию мошенничества, указать ее признаки и предложить вариант, что делать человеку в данной ситуации.

Возможные варианты (в дополнение к тем, которые предложены в заданиях трех туров, т. к. команды будут в первую очередь вдохновляться ими):

| Пространство | Ситуация | Признаки | Действия |
| --- | --- | --- | --- |
| Телефон | Позвонил «сотрудник безопасности банка» и предложил предоставить QR-код из мобильного приложения, чтобы «обезопасить» свои средства. | Это мошенничество с использованием QR-кода:  1) QR-код фактически является поручением банку на выдачу денег без ввода ПИН-кода, и настоящие сотрудники банка никогда не попросят у клиента такие данные.  2) QR-код при оплате ведет на какой-то неизвестный ресурс.  3) Мошенник торопит с оплатой с помощью QR-кода, ставит сроки действия. | * Следить за безопасностью QR-кодов. * С осторожностью относиться к статическим кодам. * С осторожностью относиться к электронным меню в кафе и ресторанах. * Не спешить активировать QR-код на смартфоне по пути или в очереди в кассу. Лучше сделать это непосредственно в момент покупки. |
| Объявления на бумаге | Мошенник наклеил поверх официального QR-кода свой, фальшивый. Герой отсканировал его в уверенности, что оплачивает покупку или услугу, а на самом деле перечислил деньги мошенникам. |
| Телефон | Звонят под видом сотрудников банков, сообщают о якобы несанкционированном запросе на снятие денег со счета и просят прислать QR-код, чтобы отменить операцию. Получив код, мошенники снимают по нему деньги в банкоматах со счета жертвы. |
| Телефон | Герою внезапно пришло на счет мобильного телефона 3 тыс. рублей. После этого позвонил человек и объяснил, что ошибся с адресатом. Попросил перевести 2500 руб. на номер карты, а 500 руб. оставить себе. | Это дроппинг:  1) Предлагается посредничество в переводе или обналичивании поступивших средств.  2) Предлагается процент за эту «работу». | * Не сообщать никому данные своей банковской карты. * Не передавать свою карту третьим лицам. * Не соглашаться перевести деньги по реквизитам по просьбе неизвестных лиц. * Не соглашаться снимать деньги в банкомате для кого-то. * Сообщать о подозрительных просьбах в Банк России и полицию. |
| Соцсеть | Написал контакт из списка друзей и предложил работу. Должность администратора «лотереи». Нужно рассылать выигрыши победителям. Герой «устроился на работу» и каждый день делал по несколько переводов, оставляя себе вознаграждение в 3% от суммы. |
| Телефон | Позвонил «сотрудник технической поддержки известной компании». Сказал, что зарегистрирована подозрительная активность в аккаунте жертвы и нужно подтвердить данные своего аккаунта. Для этого требуется установить обновленное программное обеспечение. После этого телефон заблокирован и средств на счету не осталось. | Это вишинг:  1) Звонящий утверждает, что он из государственного учреждения.  2) Наличие срочности.  3) Звонящий просит вас подтвердить данные вашего счета или аккаунта. | * Не отвечать на звонки с неизвестных номеров. * Не делиться своей персональной информацией по телефону. * Запросить документ, удостоверяющий личность. * Изменить пароли к аккаунтам. * Уведомить банк об инциденте и тщательно следить за финансовыми операциями. |
| Соцсеть | В социальной сети вы увидели рекламу интересного вам предложения. Вы перешли по указанной в ней ссылке. Но после этого увидели тот самый «синий экран» с якобы системным сообщением о возникшей проблеме. В конце сообщения значится телефон службы поддержки клиентов. Звонок, разумеется, бесплатный.  Расстроившись и испугавшись перспективы покупки новой дорогой техники, вы звоните по указанному номеру. Вам отвечает доброжелательный оператор, задаёт стандартные для такой ситуации вопросы. Он может даже предложить выполнить какие-то действия, только они ничем не помогут.  После этого «техподдержка» приходит к «выводу»: проблема серьёзная и грозящая тяжёлыми последствиями. Например, удалением всех данных. Ваш собеседник знает выход, но эта услуга уже платная. Для оплаты вас просят продиктовать данные карты. |

**ЭТАП 4: ПОДВЕДЕНИЕ ИТОГОВ И РЕФЛЕКСИЯ (6 МИН.)**

Спикер переходит к слайду с ответами: «Подводим итоги. Давайте посмотрим правильные ответы на задание 1 тура. В зоне риска у нас три героя, цветом выделены те признаки, которые позволили это определить. Как же справились с этим наши агентства?»

**Объявляет набранные баллы 1 тура.**

\*\*\*

Спикер, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, находящихся в зоне риска финансового мошенничества:

| Герой | Его описание | Комментарии спикеру |
| --- | --- | --- |
| Алексей | В свои 20 лет он учится в техническом вузе и подрабатывает графическим дизайнером, обожает технические новинки и копит на дорогостоящее профоборудование. Активно пользуется СБП. В обеденный перерыв в кафе занимается поиском новых заказов «на просторах интернета», откликается на все вакансии в соцсетях и иных ресурсах, оставляя свой телефон и ФИО. | Максимально небезопасно оставлять в соцсетях и иных ресурсах свой телефон и ФИО и другие контактные данные. Можно стать жертвой как вишинга, так и дроппинга (так как пользуется СБП, значит использует свой номер телефона). |
| Виолетта | Ей 22 года, и она хочет стать профессиональным киберспортсменом, обожает соревновательные головоломки, в кафе обязательно подключается к общественному бесплатному Wi-Fi и проверяет интересующие ее беседы в сетевых сообществах, совершает финансовые переводы. | Максимально небезопасно, подключаясь к общественному бесплатному Wi-Fi, совершать большое количество разнообразных финансовых переводов – есть риск, что данные будут использованы мошенниками. |
| Данила | Одноклассник Марины, любитель долгих телефонных разговоров, которые не прекращает и в обеденный перерыв. Сторонник открытого общения – даже с тем, кто ошибся номером, может проговорить полчаса. Любит спорт. Частый посетитель кафе, любит там назначать встречи своим многочисленным знакомым и просто посидеть за чашкой чая и смартфоном. | Как указано, Данила даже с тем, кто ошибся номером, может проговорить полчаса. Вспомните – первый совет, который дается при ситуации контакта с мошенниками, – не разговаривать с незнакомыми собеседниками. |

Максимальное количество баллов – три балла.

Продолжает подведение итогов: «Далее обратим внимание на результаты второго тура, тут надо было выявить дроппинг и вишинг. Вот эти герои столкнулись с мошенниками. Как же справились с этим наши агентства?»

**Объявляет набранные баллы 2 тура.**

Спикер, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, столкнувшихся в беседе с дроппингом и вишингом:

| Герой | Его описание | Комментарии спикеру |
| --- | --- | --- |
| Марина поговорила с администратором центра репетиторства | Добрый день, Марина. Вам звонят из центра репетиторства. Вы наш постоянный и любимый клиент. Напишите, пожалуйста, несколько отзывов на пройденные в течение последнего месяца занятия. За отзывы вам положено вознаграждение. Для перевода денежных средств мне нужно вас внести в базу, назовите свои фамилию, имя, отчество, номер банковской карты и CVC. Деньги поступят вам сразу после опубликования отзывов. | Это вишинг. Какие признаки позволяют это определить:  звонок с неизвестного номера, предлагают легкий заработок, для которого нужно заранее сообщить данные банковской карты и ее CVC. |
| Алексей поговорил с потенциальным работодателем | Здравствуйте, Алексей. Да, мы предлагаем вам интересную работу в IT-сфере, начнете работать и получать высокую оплату труда. Вы ведь видели отзывы в соцсети? Это новый и очень популярный инвестпроект, где ваши навыки очень пригодятся, быстро сделаете карьеру. Договор, конечно, мы с вами заключим, а теперь давайте поговорим про риски и проценты с вознаграждения. Видите, условия очень хорошие, нам просто нужны молодые и активные сотрудники. Да, для работы, так как проект растет, вам потребуется завести пять банковских карт. У вас есть предпочтения по банкам? Проект активный, каждый день нужно будет получать платежи и совершать с них транзакции членам нашей команды, это позволяет нарастить инвестиционные возможности и заработать, с каждой транзакции ваши – 10 %. Да, возможно, потребуется отдельный номер телефона для обеспечения большего доступа к проекту. Приступить можете с понедельника. | Это дроппинг. Какие признаки позволяют это определить: фразы «потребуется завести пять банковских карт», «нужно будет получать платежи и совершать с них транзакции членам нашей команды, это позволяет нарастить инвестиционные возможности и заработать, с каждой транзакции ваши – 10 %», «отдельный номер телефона». |
| Данила поговорил с «другом друга» | Привет, Данила, это Максим. Мы с тобой не знакомы, я друг Марины. Она сказала, что ты нуждаешься в подработке. Мы сейчас как раз ищем сотрудника. Работа достаточно легкая и не занимает много времени, но нужно быть внимательным. Я буду ежедневно перечислять на твою карту определенную сумму, а ты – снимать и отдавать человеку, который вечером будет приезжать к тебе. Суммы небольшие, но, чтобы не вызвать подозрения у сотрудников банка, нам нужны люди для проведения этих нехитрых операций. Но при этом 5% от суммы ты можешь оставить себе, это твое вознаграждение за оперативность. Все абсолютно законно и безопасно. Если ты знаешь еще кого-нибудь, нуждающегося в подработке, то скажи мне, я свяжусь с этим человеком. Но только нужны ответственные люди, которые умеют работать быстро. | Это дроппинг. Какие признаки позволяют это определить: фразы «ежедневно перечислять на твою карту определенную сумму, а ты – снимать и отдавать человеку, который вечером будет приезжать к тебе», «5% от суммы ты можешь оставить себе, это твое вознаграждение за оперативность». |
| Виолетта поговорила с представителем банка | Добрый день, Виолетта, вам звонят из службы безопасности банка N, к нам поступила информация, что по вашему счету обнаружены подозрительные транзакции, для проверки данных вашего счета необходимо срочно установить программу удаленного управления мобильным банкингом, чтобы сотрудники банка могли получить доступ и обезопасить вас. Если это не сделать сейчас, то ваш счет заблокируют. | Это вишинг. Какие признаки позволяют это определить: звонок от службы безопасности банка, нужно установить ПО для удаленного доступа; срочность и то, что торопят, указывая, что счет заблокируют. |
| Лилия ответила на звонок от потенциального работодателя | Добрый день, Лилия, наше агентство заинтересовали ваши фотографии, у вас неплохой блог, все эстетично, мы хотели бы пригласить вас на работу, для начала вам необходимо оформить страничку одного нашего продукта в соцсети. Мы посмотрим, как это повлияет на продажи, тогда заключим с вами договор. Оплата будет зависеть от того, насколько быстро будет расти аудитория, а компания – получать прибыль. Как вы понимаете, это отличная возможность показать свой талант людям и стать востребованным специалистом. Нам очень хотелось бы с вами сотрудничать. | Тут предварительно нет признаков вишинга или дроппинга. Абонент не просит данные банковской карты, персональные данные, не предлагает стать посредником для перевода средств. Но отнестись с осторожностью к предложению и проверить информацию, прежде чем соглашаться, конечно, стоит. |

За каждый правильный ответ – 1 балл.

Продолжает подведение итогов: «Переходим к результатам третьего тура. Ответы и герои у вас на экране, цветом выделены важные признаки, благодаря которым можно было выявить финансовое мошенничество. Как же справились с этим наши агентства?»

**Объявляет набранные баллы 3 тура.**

Спикер, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, находящихся в зоне риска финансового мошенничества:

| Герой | Его описание | Комментарии спикеру |
| --- | --- | --- |
| Марина | Марине пришло сообщение от близкой подруги, что она только что нашла ее фотографии с дня рождения, их разместили на странице кафе, где проходил праздник. Для быстрого перехода подруга прислала Марине картинку с QR-кодом | Тут мошенничество, которое можно увидеть по совокупности признаков. Во-первых, это непроверенное сообщение в соцсети. Во-вторых, срочность – торопят, что нужно быстро перейти, и сам QR-код, который действует 10 минут. |
| Алексей | Алексею прислали сообщение, в котором предлагают перейти по ссылке на страничку продавца графических планшетов, так как он оставлял заявку на приобретение и свой номер на сайте. Ему рекомендуют изучить технические характеристики и, если все подходит, подъехать в магазин для совершения покупки. Также в сообщении указано, что если он проведет оплату по QR-коду, то сможет воспользоваться скидкой в 5%. | Собеседник не торопит героя, предлагает все изучить и уведомляет о возможности получения скидки при выбранном варианте оплаты. |
| Виолетта | Виолетте принесли счет за обед, она оплатила его картой и решила оставить чаевые официанту, для этого нужно отсканировать QR-код, который ведет на страничку кафе, где перечислены официанты (есть фотография каждого сотрудника, указаны фамилия, имя и отчество), и выбрать нужно работника. | Виолетта видит ссылку на ресурс, есть контакты лиц, с которыми Виолетта лично встречалась, можно проверить эту информацию до проведения каких-то операций. |
| Данила | Даниле в соцсети пришло сообщение с QR-кодом, что только сейчас, перейдя по нему, он сможет практически бесплатно оформить слот на забег «Бежать нельзя остановиться», о котором он мечтал, но не мог себе позволить из-за нехватки денежных средств. Однако предложение ограниченно, нужно действовать максимально быстро. | Тут ситуация мошенничества. Есть ссылка на неизвестный ресурс, торопят и предоставляют ложную информацию о скидках и выгоде. |
| Лилия | Увидев модную заколку, только появившуюся в очередном интернет-магазине, она тут же ее заказала. Оплату магазин предложил произвести при помощи QR-кода, присланного продавцом. Лилия зашла в мобильное банковское приложение, увидела ссылку на нужный ресурс и перевела необходимую сумму, дав свое разрешение на транзакцию. | Действия героини правильные, она зашла в мобильное банковское приложение, увидела ссылку на нужный ресурс и перевела деньги. |
| Мурат | Мурату прислали сообщением инструкцию по блокировке транзакций из банка N: «Уважаемый Мурат! 30 минут назад с вашего счета пытались снять большую сумму денег. Зайдите в приложение банка, сформируйте QR-код и отправьте его скриншот на этот номер. Это необходимое действие для отмены операции. С уважением, служба безопасности банка N». | Это мошенничество. Совокупность признаков: обращение от службы безопасности, требование срочного действия и формирования QR-кода, который фактически является поручением банку на выдачу денег без ввода ПИН-кода. Настоящие сотрудники банка никогда не попросят у клиента такие данные. |

За каждый правильный ответ – 1 балл.