Как не попасться на уловки мошенников

Сценарий к презентации

Цель — информирование о мошеннических схемах, раскрытие способов, форм и средств мошеннического обмана.

Задачи:
— дать понятие мошенничества;
— рассмотреть основные виды мошеннических схем;
— сформировать навык распознавания мошеннических схем;
— развитие навыка критического мышления.

Время проведения: 30-40 минут.

Необходимые материалы:
— Презентация с материалом;
— Экран;
— Мультимедийное пространство;
— Столы и стулья для участников.

Ход мероприятия:

Слова модератора (куратора группы)

Добрый день! Сегодня мы поговорим с вами о том, что такое мошенничество, какие схемы мошенничества существуют, как нам с вами не стать жертвой обмана.

Мошенничество представляет собой присвоение имущества другого лица или приобретение прав на это имущество путем использования обмана или злоупотребления доверием. Лицо, занимающееся такими действиями, называется мошенником.

Вопрос на обсуждение: «Как вы думаете, что может являться целью мошенников?» (ответы участников).

Наиболее часто, целью мошенников являются:
1. Имущество (движимое/недвижимое, наличные деньги, крипто-валюта и т.п.).
2. Права на чужое имущество (ценные бумаги, доверенности, наследство и т.д.).
1. Информационные активы (игровые аккаунты, социальные сети, e-mail и др.).
2. Персональные данные (логины и пороли, реквизиты карт, номера телефонов и т.д.).

Теперь предлагаю обсудить, какие же мошеннические схемы могут встречаться нам в жизни. Возможно, с некоторыми вы уже встречались или слышали о них.

Давайте рассмотрим основные.

1. Служба безопасности «Сбербанка».
Думаю, вы слышали о таком способе обмана, как звонок, сообщение от «Сбербанка». Чаще всего мошенники представляются сотрудником банка и сообщают о якобы «странной активности счета». Злоумышленник просит у вас полные сведенья о банковской карте, CVV- или CVC-код, код из СМС или пароли от «Сбербанк Онлайн». Это нужно «для сохранности ваших денег».

Второй способ мошенничества касается трансляции экрана. Сначала мошенник регистрирует в мессенджере аккаунт, имитирующий принадлежность к компании «Сбербанк». В его названии может быть число 900 (номер банка), а на фото профиля - логотип организации. Злоумышленник от имени сотрудника банка спрашивает человека, обновлял ли он недавно приложение.

Если ответ отрицательный, «сотрудник» говорит собеседнику, что ему позвонит специалист банка и поможет обновить приложение.

Второй «сотрудник» звонит по видеосвязи, чтобы установить личность клиента по биометрии. Затем он просит включить режим демонстрации экрана для подключения некой «роботизированной системы для диагностики счета». После этого жертву мошенничества просят зайти в мобильное приложение банка, чтобы экран увидел робот.

На самом деле трансляция экрана позволяет злоумышленнику увидеть номера карт, суммы на счетах, коды в СМС от банка. Эта информация помогает заполучить доступ к личному кабинету в приложении. Мошенник может зайти со своего телефона в приложение «Сбербанк Онлайн» и перевести деньги на свой счет.

2. Представитель МВД.
Большинство мошенников уже давно используют чужие амплуа для того, чтобы обмануть людей. В наше время, помимо звонка от банка, мошенник может стать сотрудником правоохранительных служб, врачом и т.д.

Вот одна из схем мошенничества:
Вам звонит «сотрудник» банка или Центрального банка и спрашивает, оформляли ли вы заявку на кредит. После того как вы отвечаете «нет», он сообщает, что за на вас оформили кредит сотрудники банка, которые замешаны в мошеннической схеме.

Потом с вами связывается человек из МВД, прокуратуры или ФСБ и подтверждает все слова и ФИО «сотрудника» банка. Вам могут прислать выписки из банка, удостоверения и другие документы с печатями, чтобы убедить вас, что ситуация реальная и мошенникам можно доверять.

В итоге вам предлагают обратиться в отделение банка (или сразу в несколько банков) и подать новую заявку на кредит, чтобы предыдущая отменилась. При этом советуют «как можно меньше общаться» с сотрудниками банка в офисе. Как только вы получили деньги, вас просят перевести их на новый «безопасный» счет, который принадлежит мошенникам.

3. Предложение работы

Если вы когда-нибудь искали работу, то, наверное, сталкивались с тем, что многие работодатели отправляют информацию о вакансии и предпочитают вести диалог в мессенджере. Поэтому, для многих людей не удивительно, что в социальных сетях им могут приходить предложения о работе. Однако под видом реальных работодателей могут скрываться мошенники. Они предлагают людям хорошие вакансии с высокой заработной платой, удобным графиком или удалённой работой, однако, вначале нужно пройти обучение.

Согласитесь, что предложение выглядит заманчиво. Однако тут скрывается одна из схем мошенничества.

Перед началом работы вас просят пройти вводное обучение и присылают ссылку. Данная ссылка ведет на зараженное приложение, с помощью которого мошенники получают доступ к банковским картам.

4. Выпуск виртуальных карт

Мошенничество с банковскими картами существует уже давно. Однако сейчас мошенники вышли на новый уровень. Они стали массово обманывать людей с помощью выпуска виртуальных карт для оплаты смартфоном.

Злоумышленники убеждают клиента привязать к своему электронному кошельку некую карту, а затем через банкомат перечислить на нее наличные ради их спасения.

Это создает иллюзию «безопасности», что с деньгами все в порядке, так как пользователь пользуется собственным телефоном и деньги под контролем.

5. Мошенничество под видом трудоустройства в ПВЗ

Мир онлайн-магазинов набирает обороты. Все больше людей предпочитают делать заказы на популярных маркетплейсах, такие как Wildberries и Ozon. Это приводит к росту пунктов выдачи заказов (ПВЗ) и поиску работников для выдачи товаров. Этой возможностью воспользовались и злоумышленники.

Людям предлагают работу по приему и выдаче заказов через объявления на популярных онлайн-площадках.

Злоумышленники пишут в один из мессенджеров с предложением работы. Во время разговора они уточняют операционную систему смартфона, интересуясь исключительно пользователями с системой «Android».

Затем, под предлогом оформления, собираются личные данные, и жертву просят установить определённое приложение, которое маскируется под приложения маркетплейсов. На самом же деле, внутри файла скрывается вредоносное программное обеспечение, позволяющее мошенникам получить доступ к банковским счетам жертвы.

6. Дипфейк-атаки

Помните новость о том, что недавно мошенники из Африки создали дипфейк Бреда Питта и получили 800 тысяч евро с француженки по имени Анна?

Это один из крупных примеров того, как мошенники используют технологии для создания не только голосовых подделок, но и самой личности человека.

Вопрос на обсуждение: как вы думаете, что такое дипфейк? В каких целях его могут использовать? (Ответы участников).

Дипфейк — это подделка голоса или внешности человека на фото или видео, созданная с помощью искусственного интеллекта и нейросетей.

Для нас с вами это может быть опасно тем, что мошенники могут писать, звонить и выдавать себя за близких нам людей, с целью извлечения нужной информации или перевода денег.

Злоумышленники способны применять искусственный интеллект для воспроизведения интонации, ритма и индивидуальных особенностей речи конкретного человека, что позволяет создавать правдоподобные аудиосообщения.

Наибольшую опасность использования дипфейков представляют для пожилых людей. Кроме того, под угрозой находятся родственники публичных фигур, поскольку образцы их голосов доступны в открытом доступе.

Чаще всего, мошенник собирает данные о человеке на основании информации, которую он сам размещает в интернете, включая сведения о родственниках, друзьях, работе и увлечениях.

7. «Коллегия присяжных заседателей»

Мошенники ушли далеко в своих способах обмана и разработали новые способы хищения данных:

Первый способ заключается в том, что мошенники начали писать от имени сотрудников силовых структур и направлять вызовы в правоохранительные или налоговые органы в связи с подозрением в соучастии в мнимом преступлении. Злоумышленники к таким «вызовам» зачастую прикрепляют активные ссылки, переход по которым предоставит мошенникам доступ к паролям от различных приложений, включая банковские.

Второй способ заключается в том, что на электронную почту могут приходить сообщения о том, что гражданин выбран для участия в коллегии присяжных заседателей. При этом за неявку обещают наступление административной и уголовной ответственности. Для того, чтобы отказаться от этой обязанности, необходимо нажать на ссылку для указания причин невозможности участия в коллегии присяжных. Эта ссылка ведет на поддельный сайт, где злоумышленники также получают доступ к паролям пользователя и вносят в его устройство вирус.

8. Обман по фейковому QR-коду

QR-коды встречаются на каждом пути. Они стали удобным способом получения информации. Мошенники тоже стали использовать QR-коды. В интернете часто публикуются фейковые объявления о гарантированной социальной выплате. В них есть ссылка на портал, похожий на «Госуслуги». На сайте пользователь сканирует QR-код и переходит в чат-бот в одном из мессенджеров. В нем человеку сообщают о положенной ему выплате: например, пособии для пенсионеров или семей с детьми, студенческой стипендии. Затем под предлогом оформления выплаты злоумышленники узнают личные данные и сведения о банковских счетах жертв.

Второй способ мошенничества касается самокатов. Мошенники начали наклеивать поддельные бумажные QR-коды поверх настоящих — сначала на товары и счета в кафе, а с недавних пор и на арендные самокаты. Поэтому внимательно смотрите и обращайте внимание на QR-коды.

9. Обман от «YouTube»

После замедления видеохостинга «YouTube», многие пользователи стали искать различные способы просмотра видеороликов, что открыло возможности для обмана.

Многие злоумышленники стали рассылать пользователям электронные письма со ссылками, которые маскируют под уведомления от видеохостинга. Потенциальным жертвам предлагают пройти опрос для определения их скорости загрузки приложения, а также подписаться на «увеличение скорости» от «YouTube». В отельной графе предлагают ввести свои личные данные через специальную форму.

Другой вариант, когда злоумышленники рассылают письма с замаскированными под уведомления от Youtube ссылками. За ними скрываются шпионские и вредоносные программы. Таким образом, аферисты могут отследить действия пользователя и сохранить их историю.

10. Работа за «лайки»

В погоне за быстрым заработком многие люди ищут простую и легкую работу. К такой можно отнести работу по поставке «лайков» в социальных сетях или на маркетплейсах (например, нужно поставить хорошую оценку продавцу). Цену за такую работу предлагают от 40 рублей за лайк. Однако вместо денег многие мошенники получают ценные сведения.

Схема может выглядеть так: мошенники размещают объявление о заработке в мессенджерах или на официальных страницах по поиску работы. Всё, что требуется от пользователя, — поставить лайк или оставить отзыв. После того, как человек откликается на предложение, его добавляют в группу участников, где публикуются отчеты о проделанной работе. Все задания отправляет мошенник под видом менеджера. Далее происходит несколько вариантов событий:

В первом, после выполнения задания мошенники просят сообщить платежные данные карты для начисления вознаграждения. Естественно, жертва не получит никаких денег, а только лишится их.

Во втором случае, после начисления денег мошенники могут попросить сообщить им номер телефона и код из SMS для подтверждения перевода.

В третьем варианте, мошенники могут прислать ссылку на поддельный сайт, где надо ввести платежные данные с карты. После того, как человек отправляет свои реквизиты, мошенник получает ценные данные для вывода денег.

Завершение.

Вопрос на обсуждение: как вы думаете, как можно защитить себя и близких от мошенников? Какими способами это можно сделать? (Ответы участников).

Как можно защитить себя от телефонного мошенничества?
— Блокируйте номера, с которых поступают подозрительные звонки.
— Не сообщайте логины и пароли от аккаунтов, платёжные данные, одноразовые коды из смс.
— Не переводите деньги на счета, номера которых вам называют по телефону.
— Если вам поступило подозрительное сообщение от «руководителя организации», позвоните руководителю напрямую и уточните, присылал ли он подобное сообщение.
— Установите лимит на карту. Если вы получаете уведомление, о том, что кто-то попытался снять сумму денег, блокируете банковскую карту.
— Если сомневаетесь, можно самостоятельно позвонить в организацию по официальному номеру телефона, из которой вам якобы звонили, чтобы убедиться, что все в порядке.

Как защитить себя от интернет-мошенничества?
— Внимательно проверять ссылки на сайты, требующие ввода учетных данных, не ходить по ссылкам из писем, смс и т.п.
— Для входа в интернет-банк используйте приложение банка, а не сторонние серверы.
— Если к вам обращаются с выгодным предложением работы, то перепроверьте другие вакансии у данного работодателя.
— Будьте бдительны, всегда находите первоисточник и анализируйте материал, прежде чем совершать какие-либо действия.
— Если же вдруг вы поняли, что стали жертвой преступления, незамедлительно сообщайте об этом в правоохранительные органы. При этом не забудьте приложить скриншоты всех переписок, подтверждающих обоснованность вашего обращения.