РАЗГОВОРЫ О ВАЖНОМ

Сценарий занятия

Кибербезопасность

СПО

23 января 2023 г.

ЗАНЯТИЕ
для обучающихся СПО по теме
«КИБЕРБЕЗОПАСНОСТЬ»

Цель занятия: формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

Формирующиеся ценности: жизнь, права и свободы человека.

Продолжительность занятия: 30 минут.

Рекомендуемая форма занятия: эвристическая беседа. Занятие предполагает использование видеороликов, учебную игру и включает в себя анализ информации, групповую работу.

Комплект материалов:
- сценарий;
- методические рекомендации;
- иллюстративные материалы и инструкции к игре;
- видеоролики.

Структура занятия

Часть 1. Мотивационная.
Анонс темы и просмотр мотивационного ролика.

Часть 2. Основная. ДВА ВАРИАНТА.
Вариант первый (для педагогов и обучающихся, обладающих повышенным уровнем компетенций в области ИТ).
Игра на тему кибербезопасности в группах. Разбор и обсуждение предлагаемых ситуаций и вывод правил безопасного и эффективного использования цифровых ресурсов. Обсуждение вопросов, связанных с правилами информационной безопасности.
Вариант второй.
Игра в группах на тему безопасного поведения в Интернете. Разбор и обсуждение предлагаемых ситуаций и вывод правил безопасного и эффективного использования цифровых ресурсов. Обсуждение вопросов, связанных с правилами поведения в интернете.

Часть 3. Заключение.

Подведение итогов занятия: фиксация правил, которые узнали обучающиеся, просмотр закрепляющего видеоролика от эксперта информационной безопасности.

Сценарий занятия. ВАРИАНТ №1.

Часть 1. Мотивационная (до 5 минут).

Педагог.

Сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch [Инфо-вОтч].

Демонстрация видео с Н. И. Касперской.

Педагог.

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем командную игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать.

Часть 2. Основная (до 20 минут).

Описание игры «Кибербезопасность».

Аудитория делится на две команды – «Кибермошенники» и «Специалисты по информационной безопасности» (как вариант, можно предложить разделить аудиторию на несколько команд - специалистов по информационной безопасности; в этом варианте педагог сам озвучивает все карточки с киберугрозами).

Каждая команда получает набор карточек с возможными действиями (*см. дополнительные материалы*).

Механика игры:

1. Педагог выбирает одну из карточек-угроз (в любой последовательности) и озвучивает её.

2. Задача команды «Кибермошенники» — подобрать из набора карточек с действиями те, что злоумышленники типично используют в такой ситуации.

3. Задача команды «Специалисты по информационной безопасности» – оставить план защиты из своего набора карточек-действий и описать модель поведения пользователя.

На обсуждение отводится 3–5 минут.

4. «Кибермошенники» презентуют свой вариант плана «нападения», а «специалисты по информационной безопасности» – план защиты.

5. Педагог оценивает, отражена ли атака (при необходимости используя ключи к ситуациям, в которых представлены примерные планы атаки и защиты), если да, то присваивает балл команде «специалистов по ИБ».

Возможен вариант выбора команды экспертов из числа обучающихся, которые будут качественно оценивать планы действий команд и при необходимости дополнять их.

Тематики заданий из сферы кибербезопасности, которые встречаются в игре:

- фишинговые ссылки;
- социальная инженерия;
- защита личной информации;
- защита профиля.

Карточки-угрозы, карточки-действия для команды «Кибермошенники» и «Специалисты по информационной безопасности», ключи к ситуациям *представлены в Приложении к сценарию и дополнительных материалах.*

Пример проведения одного тура игры «Кибербезопасность».

Педагог.

Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации — потерять аккаунт для него будет обидно.

Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля.

Педагог.

Команда «Кибермошенников» из своих карточек–действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленники

типично используют в такой ситуации (можете добавить свои варианты действий).

Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача – собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий).

Работа в группе 3–5 минут.

Педагог.

Время для обсуждения закончилось, давайте дадим слово каждой группе и узнаем, какие планы получились у команд. Слово команде «кибермошенников».

(Ответ представителей команды «кибермошенников».)

Педагог.

Теперь время ответить на атаку, вторая команда, вам слово.

(Ответ представителей команды «специалистов по информационной безопасности».)

Педагог.

С учетом планов команд я могу объявить победителей этого тура *(Педагог комментирует ответы команд, при необходимости используя ключ с примерными планами атак и защиты, и называет команду-победителя первого тура.).*

Следующие туры проходят по такой же схеме. Количество туров педагог определяет самостоятельно.

Методический комментарий.

Игра может проходить и в формате, когда все обучающиеся играют роль специалистов по информационной безопасности.

В таком варианте педагог озвучивает угрозу и выводит на экран примерный план атаки кибермошенников (из ключа к ситуациям, представленным в приложении).

Задача – всем вместе найти вариант отражения атаки и обезопасить профиль молодого ученого Алексея.

Педагог.

Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас.

Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить

список – топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.

Обучающиеся предлагают полезные привычки кибербезопасности, педагог модерирует составление списка.

Педагог.

Спасибо вам за ваши идеи и комментарии, предлагаю подвести итоги занятия.

Часть 3. Заключение (до 5 минут).

Педагог.

Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK [вэ-кА] и популярного российского певца Егора Крида.

Демонстрация видео с Р. Газизовым.
Демонстрация видео с Е. Кридом.

Сценарий занятия. ВАРИАНТ №2.

Часть 1. Мотивационная (до 5 минут).

Педагог. Сегодня мы с вами поговорим о том, с чем постоянно сталкивается современный человек — это использование Интернета для решения повседневных задач: для учебы, общения, творчества, профессиональной деятельности. Возможности, доступные нам благодаря подключению к сети, могут принести много пользы, но там же можно столкнуться и с разными угрозами. Важно использовать доступ в Интернет с умом, эффективно и безопасно. Как и в реальной жизни, в Интернете стоит придерживаться некоторых правил, именно их мы сегодня с вами обсудим. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch [Инфо-вОтч].

Демонстрация видео с Н. И. Касперской.

Педагог.

В продолжение занятия предлагаю вам разобрать несколько ситуаций, которые иногда случаются в сети. Вы выступите в роли сторонних наблюдателей и предложите свои решения.

Часть 2. Основная (до 20 минут).

Методический комментарий. В основной части представлено два вида заданий.

1. **Интерактивное задание в форме анимационных фрагментов**.

Рекомендуется групповой вариант работы, но возможен и фронтальный.

Порядок работы с каждой ситуацией-кейсом строится по следующему алгоритму:

• *просмотр первой части видеофрагмента;*

• *обсуждение ситуации в группе и формулировка правил-выводов безопасного поведения;*

• *обсуждение правил-выводов безопасного поведения;*

• *проверка правила-вывода на основе просмотра второй части ролика.*

2. **Работа с заданиями-карточками**, описывающими конкретные ситуации, с которыми обучающиеся могут столкнуться в реальной жизни.

Предложена следующая тематика ситуаций-кейсов:

1) фишинговые ссылки;
2) социальная инженерия;
3) защита личной информации;
4) защита профиля.

Количество заданий педагог определяет самостоятельно.

Работа с интерактивным заданием.

Педагог.

Мы посмотрим небольшой ролик с ситуацией, которая знакома каждому из вас, ведь все мы общаемся с друзьями и заводим новые знакомства.

Смотрим первую часть ролика, думаем, что случилось и как можно было бы предотвратить эту ситуацию.

Видео-кейс № 1. Фишинговые ссылки.

Педагог.

Предлагаю вам разделиться на группы и попробовать сформулировать правила, при соблюдении которых можно было бы избежать подобной ситуации.

(Обучающиеся делятся на мини-группы по 4 человека и обсуждают возможные правила. На эту работу отводится 1–2 минуты.)

А теперь давайте обсудим получившиеся у вас правила. Что вы можете посоветовать делать в подобных ситуациях?

(От каждой группы один обучающийся предлагает одно правило. Педагог фиксирует на доске.)

Педагог.

Мы с вами обсудили, что пошло не так в ситуации Вани, теперь давайте досмотрим ролик и узнаем, какие цифровые привычки и правила нам предлагают создатели ролика, чтобы не попасться на удочку мошенников.

Продолжение демонстрации видео-кейса № 1. Фишинговые ссылки.

Методический комментарий.

Дополнительно в этом кейсе можно обсудить значение слова «фишинговая» ссылка. Действия мошенников называют «фишингом» из-за английского слова «фиш», что означает «рыба» или «рыбачить», то есть буквально мошенники стараются «выудить» информацию у пользователя.

Педагог.

Есть ещё одна ситуация, которую описывает в своем блоге герой мультфильма. Давайте посмотрим его, следите за сюжетом и поведением персонажей.

Видео-кейс № 2. Социальная инженерия.

Педагог.

Как вы считаете, какую ошибку допустил герой мультфильма? Каких правил надо придерживаться, чтобы не попадать в ловушки, в которые попала Кира? Давайте, как и в предыдущем случае, сначала обсудим это в группах, а потом все вместе.

(Работа в группах, обсуждение и последующие ответы обучающихся.)

Педагог.

Вы отлично справились, давайте досмотрим видео и узнаем, какие правила поведения в интернете мы с вами должны запомнить.

Продолжение демонстрации видео-кейса № 2. Социальная инженерия.

Методический комментарий.

Социальная инженерия — разные виды манипуляций и обмана, цель которых заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.

Педагог.

Я предлагаю вам посмотреть другую ситуацию, которая произошла с любительницей классического искусства Ариной. Как и в прошлый раз, будьте внимательны и отмечайте поведение персонажей, чтобы ответить на мой вопрос. Смотрим.

Видео-кейс № 3. Защита личной информации.

Педагог.

Как думаете, что произойдет дальше? Что в этой ситуации в поведении Арины вы считаете опасным? Есть ли здесь ошибка? На что мы должны обращать внимание, чтобы не попасть в такие же ситуации, как Арина? Поработайте, пожалуйста, в тех же группах, а потом мы обменяемся с вами мыслями.

(Работа в группах, обсуждение, ответы обучающихся.)

Педагог.

Вы молодцы, сейчас мы посмотрим развязку, узнаем не только, что случилось с Ариной, но и то, как обезопасить свою личную информацию и какие правила в этом помогут.

Продолжение демонстрации видео-кейса № 3. Защита личной информации.

Педагог.

Сейчас мы посмотрим ещё один ролик, где рассказывается история Жанны. Предлагаю узнать, что с ней приключилось и как друзья смогли прийти на помощь. Следите за сюжетом, у меня будет вопрос для вас.

Видео-кейс № 4. Защита профиля.

Педагог.

Как вы считаете, почему в аккаунте появилась такая информация? Как друзья Жанны поступят дальше? Что важно помнить и соблюдать, чтобы сохранить свой профиль в безопасности? Попробуйте составить правила, которые помогут вам обезопасить ваш профиль в социальной сети.

(Работа в группах, обсуждение, ответы обучающихся.)

Педагог.

Вы хорошо справились с заданием. Теперь время узнать, как правильно защищать свой профиль, какие правила для этого нужно знать.

Продолжение демонстрации видео-кейса № 4. Защита профиля.

Педагог.

Давайте ещё раз назовем правила, которые мы узнали на нашем занятии сегодня? Почему важно их соблюдать, как вы думаете?

(Ответы обучающихся, обсуждение.)

Работа с заданиями-карточками

Педагог.

Предлагаю вам посмотреть на знакомые действия и ситуации со стороны. Сыграем в игру и проверим, как хорошо вы умеете пользоваться цифровыми сервисами и приложениями.

Методический комментарий.

Педагог делит обучающихся на команды (*3–4 команды*). Каждая команда получает карточку с описанием ситуации, дополнительно карточка выводится на экран (*при наличии технических условий*). Также возможен и фронтальный формат работы.

Командам необходимо ответить на два вопроса:

1. Какую ошибку герой или герои ситуации допустили?
2. Какие правила для пользователя можно вывести из этой ситуации?

На обсуждение каждой ситуации дается 3 минуты. Дальше каждая группа представляет результаты обсуждения.

Педагог сверяет полученные результаты с ключом к заданию.

Карточка-задание №1

Ваша однокурсница Катя ведет видеоблог про образ жизни, увлечения, учебу. Она делится всем тем, чем живет современный обучающийся. Катя выкладывает на свой канал рассказы о своей жизни, увлечениях, занятиях. В очередном выпуске своего блога Катя решает попробовать один из популярных форматов — прямой эфир с обзором комнаты.

В начале эфира Катя сообщает, что сегодняшнюю встречу она ведет из дома, называя свой адрес.

В одном из кадров она показывает, что есть у неё в комнате, как она всё украсила к Новому году, где делает уроки, какие у неё хобби, заходит в комнату к брату, который с друзьями разучивает на гитаре новую песню.

Во время эфира в кадр попадает фамильная реликвия — шкатулка с уникальными украшениями.

Педагог.

Подумайте, в чем могли быть ошибки Кати? Что она сделала не так, и о чем нужно помнить, когда что-то выкладываешь в сеть?

Работа обучающихся в группах.

Педагог.

Время для обсуждения закончилось, давайте обсудим, какие ошибки совершила Катя и что можно ей посоветовать?

Ответы обучающихся (по одному пункту поочерёдно от каждой группы), комментарии и дополнения педагога в соответствии с ключом к заданию.

Ключ к заданию.

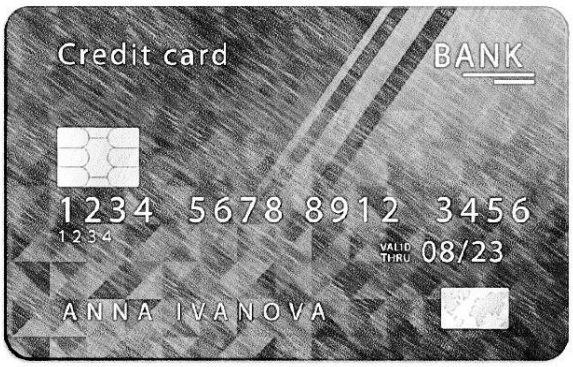
- не оставляйте информацию о себе и родственниках в открытом доступе: домашний адрес, телефоны, номер образовательного учреждения, свой возраст, геолокации;
- в прямом эфире, где у вас нет заранее подготовленного текста и сценария вы говорите все, что придет в голову и ненамеренно можете сообщить информацию потенциально опасную;
- не размещайте фото или видео, на которых видно обстановку вашей квартиры, все то, что может притягивать мошенников;
- не выкладывайте фото или видео с участием ваших родственников, друзей без их разрешения;
- используйте настройку «для близких друзей», чтобы контролировать доступ к своему профилю и информации о себе.

Педагог.

Отлично, спасибо за ваши ответы! На данном примере стало понятно, что даже в таких знакомых ситуациях могут быть подводные камни.

Дополнительно к этому заданию обучающимся можно предложить набор фотографий и обсудить, стоит ли размещать их в социальных сетях, и объяснить почему.

Примеры фотографий (полный набор и ключ к заданию представлены в дополнительных материалах).



Карточка-задание №2.1 *(команды получают разные варианты карточек).*

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. persik1234
2. ANNa11
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.2

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. Jack4321
2. ANNa11
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.3

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNA_JACK
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.4

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она выбирает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNAPERSIK
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Педагог.

Обсудите, какие из вариантов паролей надежные, какие нет, и почему? Надёжный ли пароль выбрала Аня? Сформулируйте правила, о которых нужно помнить при создании паролей.

Работа обучающихся в группах.

Педагог.

Время для обсуждения закончилось, давайте обсудим надежность паролей, представленных на карточках, и выбор Ани.

Ответы обучающихся, комментарии и дополнения педагога в соответствии с ключом к заданию.

Ключ к заданию.

- на всех карточках последний пароль подходит под критерии надежного пароля: содержит специальные знаки, заглавные буквы, цифры, при этом комбинация не связана с пользователем;
- не следует использовать общеизвестные факты для создания паролей (ваши имя, возраст, дату рождения, клички животных, имена близких родственников и т. п.);
- легко взломать пароли, состоящие только из цифр или букв;
- не следует использовать элементарные пароли типа 123456…, абвгд…;
- подключайте дополнительное подтверждение входа — двухфакторную аутентификацию.

Педагог. Проверить надежность пароля можно на сайте 2ip.ru/passcheck. Предлагаю проверить, за какой период можно взломать пароли, которые были представлены у вас на карточках.

Обучающиеся проверяют надежность паролей

persik1234 – ненадежный, возможно взломать за 254 часа

ANNa11 – ненадежный, возможно взломать за 14 секунд

Jack4321 – ненадежный, возможно взломать за 910 минут

123456789 – ненадежный, возможно взломать за 0 секунд

ANNA_JACK – ненадежный, возможно взломать за 1889 часов

ANNAPERSIK – ненадежный, возможно взломать за 588 минут

A!-2na1234 – надежный, может быть взломан за 6810 лет

A!-7n9aj234 – надежный, может быть взломан за 544770 лет

Дополнительно к этому заданию педагог может предложить обучающимся проверить на надежность свои пароли от социальных сетей.

Часть 3. Заключение (до 5 минут).

Педагог. Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK [вэ-кА] и популярного российского певца Егора Крида.

Демонстрация видео с Р. Газизовым.
Демонстрация видео с Е. Кридом.

Приложение

Карточки-угрозы
• кража профиля пользователя через взлом логина/пароля
• манипуляция, чтобы пользователь самостоятельно передал свои данные
• получение доступа к сохраненным личным данным/данным банковской карты
• продуманное мошенничество на основе доступной информации о человеке
• мошенничество через подменные/анонимные профили
• мошенничество на основе утечки данных пользователя на сторонних ресурсах

Набор карточек для группы «Специалисты по информационной безопасности»

- Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
- Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
- Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
- Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
- Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
- Не переходите по ссылкам от малознакомых людей.
- Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
- Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.

- Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
- Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
- Не поддавайтесь агрессии и не ведитесь на провокации.
- Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
- Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
- Защищайте всю информацию, даже если думаете, что она не важна.
- Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Набор карточек для группы «Кибермошенники»

- Проследить за открытой информацией в профиле, изучить подробности жизни человека.
- Спровоцировать на эмоции, вызвать интерес у пользователя, использовать приём ограниченного времени.
- Начать торопить пользователя, чтобы не дать разобраться в происходящем.
- Разослать спам-сообщение друзьям пользователя.
- Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
- Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
- Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
- Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.

- Представиться сотрудником технической поддержки и выманить конфиденциальные данные или склонить к выполнению сомнительных действий.
- Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
- Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
- Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Ключи к ситуациям угрозы (примерные планы атаки и защиты)

Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Начать торопить пользователя, чтобы не дать разобраться в происходящем.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.
4. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
3. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
4. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего

телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

1. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
2. Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

1. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
2. Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
3. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

1. Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
2. Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
3. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
2. Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
3. Не переходите по ссылкам от малознакомых людей.
4. Защищайте всю информацию, даже если думаете, что она не важна.

Угроза: продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
3. Разослать спам-сообщение друзьям пользователя.

Пример защиты:

1. Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
2. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
3. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
4. Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза: мошенничество через подменные/анонимные профили.

Пример атаки:

1. Проследить за открытой информацией в профиле, изучить подробности жизни человека.

2. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.

3. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.

4. Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.

2. Не поддавайтесь агрессии и не ведитесь на провокации.

3. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

4. Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.

5. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

1. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

2. Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

1. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

2. Не переходите по ссылкам от малознакомых людей.

3. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.

4. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.

5. Защищайте всю информацию, даже если думаете, что она не важна.