ЦИФРАтека
cifrateka.ru

Рекомендовано
Российской академией
образования

Внеурочное занятие для обучающихся 7-11 классов по теме

МОШЕННИЧЕСТВО

Цель занятия:

Знакомство обучающихся с различными формами мошенничества и способами их предотвращения.

Задачи занятия:

- Ознакомить учащихся с основными видами интернет-мошенничества.
- Развить навыки распознавания мошеннических схем.
- Обучить методам защиты личных данных и финансов в интернете.
- Сформировать осознание важности ответственного поведения в сети.

Формирующиеся ценности:

Безопасность Осознание важности защиты своих данных и личной информации в интернете.

Ответственность Развитие ответственности за свои действия в сети и понимание последствий мошенничества.

Честность Приверженность честному и этичному поведению как в реальной жизни, так и в виртуальном пространстве.

Критическое мышление Способность анализировать информацию и распознавать потенциальные угрозы.

Рекомендовано
Российской академией
образования

Основные смыслы:

Информационная грамотность: Понимание того, как работают различные виды мошенничества в интернете (фишинг, финансовые пирамиды, взломы аккаунтов).

Профилактика: Знание мер предосторожности и защиты, которые помогут предотвратить мошенничество.

Правовая осведомленность: Понимание юридических аспектов интернет-мошенничества и ответственности за участие в подобных деяниях.

Поддержка и помощь: Осознание важности поддержки и помощи тем, кто стал жертвой мошенничества, а также умение правильно реагировать на такие ситуации.

Продолжительность занятия:
45 минут

Рекомендуемая форма проведения занятия:
беседа

Рекомендовано
Российской академией
образования

Структура занятия

Часть 1: Введение в тему интернет-мошенничества

Учитель: Сегодня мы поговорим о важной и актуальной теме — интернет-мошенничестве. В современном мире мы всё больше полагаемся на интернет для общения, покупок, учебы и работы. Однако, к сожалению, с ростом технологий увеличивается и число случаев мошенничества в сети.

Как вы думаете, что такое интернет-мошенничество?
Какие виды мошенничества вы знаете? Давайте обсудим это вместе.

Вопросы для обсуждения:
Что вы знаете о мошенничестве в интернете?
Слышали ли вы о случаях мошенничества среди своих знакомых или в новостях?
Какие виды мошенничества вы могли бы назвать?

Учитель: Интернет-мошенничество может принимать различные формы. Это могут быть фишинговые письма, которые пытаются выманить у вас пароли и личные данные, финансовые пирамиды, которые обещают лёгкий заработок, или даже взломы аккаунтов. Очень важно быть бдительными и знать, как защитить себя и свои данные.

Давайте рассмотрим несколько примеров интернет-мошенничества и подумаем, почему они так опасны и как можно защититься.

Примерные сценарии для обсуждения:
Фишинг — письма или сайты, которые маскируются под настоящие, чтобы украсть ваши данные.

Финансовые пирамиды — схемы, которые обещают высокие доходы при минимальных вложениях.

Взлом аккаунтов — когда мошенники получают доступ к вашим личным страницам и используют их в своих целях.

Учитель: Теперь, когда мы обсудили основные виды интернет-мошенничества, давайте подумаем о том, почему люди попадаются на уловки мошенников.
Как вы думаете, какие факторы делают людей уязвимыми для мошенничества в интернете?
Ответы учащихся

Часть 2: Различение форм интернет-мошенничества и способы защиты

Учитель: Теперь, когда у нас есть общее понимание интернет-мошенничества, давайте перейдем к обсуждению конкретных способов защиты и предотвращения этих угроз.

Начнем с фишинга. Фишинг — это попытка мошенников выманить у вас конфиденциальную информацию, такую как логины, пароли, данные кредитных карт. Фишинговые письма и сайты часто выглядят очень правдоподобно, и даже опытные пользователи могут попасться на уловку.

Вопросы для обсуждения:
Как вы думаете, по каким признакам можно распознать фишинговое письмо или сайт? Какие меры предосторожности вы можете предпринять, чтобы не стать жертвой фишинга?
Ответы учащихся.

Учитель: Хорошие ответы.
Вот несколько ключевых признаков фишинга:

Неожиданные сообщения от неизвестных отправителей.

Ссылки, ведущие на подозрительные сайты.

Ошибки в тексте письма.

Требование немедленного действия или предоставления личных данных.

Чтобы защититься от фишинга, следует:

Не открывать подозрительные письма и не переходить по ссылкам из них.

Проверять URL-адреса сайтов.

Использовать антивирусное программное обеспечение и регулярно обновлять его.

Быть внимательными к мелким деталям в письмах и на сайтах.

Учитель: Теперь давайте поговорим о финансовых пирамидах. Мошенники часто обещают быстрый и легкий заработок с минимальными вложениями. На самом деле, такие схемы основаны на привлечении новых участников, деньги которых используются для выплат предыдущим «инвесторам». Рано или поздно пирамид рушится, и многие люди теряют свои деньги.

Вопросы для обсуждения:
Слышали ли вы о финансовых пирамидах? Какие примеры вы знаете? Как можно распознать финансовую пирамиду и не стать её жертвой?
Ответы учащихся

Учитель: Правильно. Чтобы распознать финансовую пирамиду, следует обратить внимание на:

- Нереально высокие и быстрые доходы.
- Требование вложить деньги перед получением выгоды.
- Отсутствие реального продукта или услуги.
- Сложные и непрозрачные схемы выплат.

Защита от финансовых пирамид включает:

Тщательную проверку Интернет-компании перед инвестированием. Избегание предложений, которые кажутся слишком хорошими, чтобы быть правдой. Консультации с финансовыми экспертами перед вложением крупных сумм.

Учитель: Теперь поговорим о взломе аккаунтов. Мошенники могут использовать различные методы для получения доступа к вашим учетным записям, такие как подбор паролей, использование вредоносных программ или социальная инженерия.

Вопросы для обсуждения:
Как вы думаете, почему важно использовать сложные пароли и не повторять их на разных сайтах? Какие меры безопасности можно принять, чтобы защитить аккаунты от взлома?
Ответы учащихся.

Учитель: Верно. Вот несколько советов для защиты аккаунтов: Используйте уникальные и сложные пароли для каждого аккаунта. Регулярно меняйте пароли и не используйте одинаковые пароли для разных сайтов. Включите двухфакторную аутентификацию (2FA), где это возможно. Будьте осторожны при использовании общественных Wi-Fi сетей и не вводите пароли на подозрительных устройствах.

Учитель: Мы рассмотрели основные формы интернет-мошенничества и способы защиты от них. В следующей части занятия мы проведем практическое упражнение, чтобы закрепить полученные знания и научиться применять их на практике.

Часть 3: Практическое применение знаний

Учитель: Теперь, когда мы обсудили различные виды интернет-мошенничества и способы защиты от них, давайте применим наши знания на практике. Мы проведем несколько упражнений, которые помогут лучше подготовиться к реальным ситуациям.

Практическое упражнение 1: Распознавание фишинговых писем

Учитель раздает учащимся распечатки различных электронных писем, среди которых есть как настоящие, так и фишинговые. Учащиеся должны определить, какие письма являются фишинговыми, и объяснить свои выводы.

Учитель: Перед вами несколько примеров электронных писем. Ваша задача — внимательно их прочитать и определить, какие из них являются фишинговыми. Обратите внимание на отправителя, текст письма, ссылки и любые другие подозрительные элементы.
Ответы учащихся.

Учитель: Отлично! Давайте обсудим ваши выводы.
Какие признаки фишинга вы обнаружили в этих письмах?

Практическое упражнение 2: Создание безопасных паролей

Учитель предлагает учащимся создать сложные пароли для своих аккаунтов, следуя определенным правилам (длина пароля, использование различных символов, букв и цифр). Затем учащиеся проверяют свои пароли с помощью специального инструмента для оценки сложности паролей.

Учитель: Теперь давайте создадим сложные пароли для ваших аккаунтов. Помните, что пароли должны быть длинными и содержать буквы разных регистров, цифры и специальные символы. После того, как вы создадите пароли, мы проверим их сложность с помощью специальной программы.
Ответы учащихся.

Учитель: Какие трудности у вас возникли при создании паролей? Как вы можете запомнить такие сложные пароли?

Практическое упражнение 3: Обнаружение подозрительных сайтов

Учитель демонстрирует учащимся несколько веб-сайтов на экране, среди которых есть как легитимные, так и мошеннические. Учащиеся должны определить, какие сайты являются подозрительными, и объяснить свои выводы.

Учитель: Посмотрите на эти веб-сайты и определите, какие из них могут быть мошенническими. Обратите внимание на URL-адрес, дизайн сайта, наличие контактной информации и других важных элементов.
Ответы учащихся.

Учитель: Отлично! Давайте обсудим ваши выводы. Какие признаки мошеннических сайтов вы обнаружили?

Практическое упражнение 4: Реагирование на взлом аккаунта

Учитель предлагает учащимся сценарий, в котором их аккаунт был взломан. Учащиеся должны описать шаги, которые они предпримут, чтобы восстановить доступ к аккаунту и защитить свои данные.

Учитель: Представьте, что ваш аккаунт был взломан. Опишите, какие шаги вы предпримете, чтобы восстановить доступ к своему аккаунту и защитить свои данные.
Ответы учащихся.

Учитель: Правильно! Вот несколько важных шагов, которые нужно предпринять:

- Немедленно изменить пароли.
- Уведомить службу поддержки сайта о взломе.
- Проверить другие аккаунты на наличие подозрительной активности.
- Включить двухфакторную аутентификацию.
- Обновить антивирусное программное обеспечение и провести проверку устройства на наличие вредоносных программ.

Учитель: Отлично справились! В заключительной части нашего занятия мы подведем итоги и обсудим, какие шаги можно предпринять, чтобы постоянно улучшать свою интернет-безопасность.

Часть 4: Заключение и подведение итогов

Учитель: Итак, мы подходим к завершению нашего занятия на тему интернет-мошенничества. Давайте подведем итоги.

Повторение ключевых моментов:
Различные виды интернет-мошенничества, такие как фишинг, скимминг, вишинг и мошенничество в социальных сетях. Признаки, по которым можно распознать мошеннические письма, сайты и звонки. Способы защиты от интернет-мошенничества, включая создание сложных паролей, использование двухфакторной аутентификации и осторожное отношение к подозрительным ссылкам и сообщениям.

Учитель: Важно помнить, что интернет-мошенничество может затронуть каждого, независимо от возраста и уровня знаний. Поэтому очень важно быть бдительными и следовать рекомендациям, которые мы сегодня обсудили. Теперь я хотел бы услышать, какие шаги вы планируете предпринять для повышения своей безопасности в интернете? Поделитесь своими мыслями.
Ответы учащихся.

Учитель: Отличные идеи! Вы действительно понимаете, насколько важно защищать себя и свои данные в интернете. Кроме того, помните, что если вы столкнулись с мошенничеством или подозрительными действиями в интернете, всегда можно обратиться за помощью к взрослым, которых вы доверяете, или к специалистам по интернет-безопасности. Не стесняйтесь сообщать о своих проблемах и спрашивать совета.

Постразговор: Что делать после урока

Учитель: Теперь, когда наше занятие подошло к концу, я хотел бы обсудить, что вы можете сделать для закрепления и применения полученных знаний.

Проверьте текущие пароли. Убедитесь, что они сложные, содержат комбинацию букв, цифр и символов, и что они уникальны для каждого аккаунта.

Настройте двухфакторную аутентификацию (2FA) на всех доступных аккаунтах. Это дополнительный уровень защиты, который значительно усложняет доступ злоумышленникам.

Проведите аудит своих онлайн-аккаунтов. Убедитесь, что настройки конфиденциальности в социальных сетях установлены правильно и ограничивают доступ к вашей личной информации.

Регулярно проверяйте свои банковские и финансовые отчеты на предмет подозрительных транзакций. Сообщайте о любых странных или несанкционированных операциях своему банку.

Социальная ответственность:

Если вы стали свидетелем мошеннических действий в интернете или получили подозрительное сообщение, сообщите об этом соответствующим службам или специалистам по кибербезопасности.

Знания, которые вы получили сегодня, помогут вам защитить себя и своих близких от интернет-мошенничества. Помните, что ваша бдительность и ответственность играют ключевую роль в обеспечении безопасности в цифровом мире. Спасибо за вашу активность и участие в сегодняшнем занятии. Продолжайте учиться и делиться знаниями, чтобы интернет стал безопаснее для всех.

Селиванов Филипп Сергеевич.
Кандидат технических наук, доцент, преподаватель, Финансово-технологический колледж, г. Саратов