Департамент образования администрация г. Перми
Муниципальное бюджетное учреждение
«Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

РАССМОТРЕНО

утверждено на заседании
НМС МБУ «ЦППМСП» г. Перми
Протокол № 4 от 29.12.2022г.

СОГЛАСОВАНО

_____ О.В. Полторак,
начальник управления
воспитания и социализации
департамента образования
администрации города Перми

УТВЕРЖДАЮ

_____ О.А. Митина
и.о. директора МБУ
«ЦППМСП» г. Перми

ПРОГРАММА
кибеурока «Моя безопасность в сети»
(для учащихся 11 класса)

г. Пермь, 2022

77. КИБЕРУРОК
«Моя безопасность в сети» (для 11 класса)

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

Структура занятия

Часть 1. Мотивационная (до 5 минут).

Педагог.

Ребята, 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.

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».

Класс делится на две команды – «Кибермошенники» и «Специалисты по информационной безопасности» (как вариант, можно предложить разделить класс 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 детей, 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 и популярного российского певца Егора Крида.

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.