ВНЕУРОЧНОЕ ЗАНЯТИЕ
для 4-7 классов по теме
«ПРОБЛЕМЫ ХАКЕРСТВА»

ВНЕУРОЧНОЕ ЗАНЯТИЕ
для 4-7 классов по теме
«ПРОБЛЕМЫ ХАКЕРСТВА»

Цели занятия: ознакомить учащихся с проблемами, связанными с использованием социальных сетей, причинами взломов сайтов и кибератак.

Основные смыслы: познакомить учащихся с историей развития социальных сетей и социальных медиа; обсудить проблемы, связанные с использованием социальных сетей и социальных медиа; рассмотреть поведение молодежи в сети; обсудить проблему лайков в социальных сетях.

Продолжительность занятия: 30 минут.

Рекомендуемая форма занятия: беседа, обсуждение, занятие включает просмотр видеоматериалов.

Комплект материалов:

− сценарий,

− методические рекомендации,

− видеоролики,

− презентационные материалы.

Структура занятия

1. Часть 1. Мотивационная

Актуализация знаний учащихся о социальных сетях, сайтах, сообществах.

2. Часть 2. Основная

Ознакомление учащихся с проблемами, связанными с использованием социальных сетей, причинами взломов сайтов и кибератак.

3. Часть 3. Заключение

Поведение итогов. Важным моментом будет напоминание учащимся о правилах поведения в социальных сетях.

СЦЕНАРИЙ ЗАНЯТИЯ

Часть 1. Мотивационная

Слайд 1. Титульный

Учитель: здравствуйте, ребята.

Прошу своими словами напомнить всем что такое социальные сети, сайты, сетевые сообщества.

Слайд 2

Кто создаёт киберугрозы? Кто пишет вирусы, взламывает банковские счета, блокирует компьютеры, занимается иной противозаконной деятельностью в цифровом пространстве? Многие скажут: «Хакер». Но знаете ли вы, что хакеры бывают «разных цветов», а самыми популярными категориями являются чёрные, серые и белые хакеры?

Кто такие хакеры?

Предлагаю выбрать наиболее подходящее определение данному слову:

Хакер (от англ. to hack — рубить, обтёсывать) — это:

— профессионал, способный взломать системы электронной защиты, найти в них бреши и уязвимости;

— программист, который исправлял ошибки в программном обеспечении каким-либо быстрым или элегантным способом;

— «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасности.

Ответы ребят.

Учитель: мнения разделились, но все вы правы – данные определения в равной степени подходят к слову хакер.

Цели хакеров могут быть различными: корысть, месть, идеологические или политические причины, исследовательский интерес и прочее.

В глазах обывателя хакер — это компьютерный взломщик, который стремится завладеть важной информацией и с её помощью украсть деньги. Либо проникнуть в сеть или компьютер, чтобы заразить их вредоносным ПО, а потом потребовать с владельца выкуп за деактивацию вируса или разблокировку данных.

Но не все хакеры и их цели одинаково плохи. Иногда навыки и компетенции таких специалистов используются во благо, например, для проверки надёжности защиты информационных систем организаций.

Часть 2. Основная

Слайд 3

Учитель: расскажу немного о «цветовой дифференциации» хакеров:

Black hats («Чёрные шляпы») —— это преступники, злонамеренно взламывающие компьютерные сети. Они также создают вредоносные программы, которые уничтожают файлы, блокируют компьютеры, крадут пароли, номера кредитных карт и другую личную информацию.

Черные шляпы мотивированы корыстными целями: финансовая выгода, месть или просто сеяние хаоса. Иногда их мотивация может быть идеологической – их атаки нацелены на людей, с которыми они категорически не согласны.

Gray hats («Серые шляпы») — Между Белыми и Черными шляпами работают Серые шляпы. Действия Серых шляп представляют собой смесь действий Черных и Белых шляп. Серые шляпы часто ищут уязвимости в системе без разрешения или ведома владельца. При обнаружении уязвимостей они сообщают о них владельцу, иногда запрашивая небольшую плату за устранение проблем.

Некоторым хакерам из группы Серых шляп нравится думать, что они приносят компаниям пользу, взламывая их веб-сайты и вторгаясь в их сети без разрешения. Однако владельцы компаний редко ценят несанкционированные вторжения в инфраструктуру своих бизнес-данных.

Часто реальный мотив Серых шляп – продемонстрировать навыки и добиться известности, возможно, даже признательности за то, что они считают своим вкладом в кибербезопасность.

White hats («Белые шляпы») — используют свои знания и опыт для обнаружения недостатков в системе безопасности, чтобы защитить организации от опасных хакерских атак. Иногда они могут быть штатными сотрудниками или подрядчиками, работающими в компании на должности специалистов по безопасности, задача которых – поиск недостатков систем безопасности.

Работа Белых шляп – одна из причин, почему в крупных организациях обычно меньше простоев и проблем с веб-сайтами. Большинство хакеров знают, что проникнуть в системы, управляемые крупными компаниями, труднее, чем в управляемые малыми предприятиями, у которых, вероятно, нет ресурсов для изучения возможных уязвимостей систем безопасности.

Более подробная информация по ссылке: Типы хакеров: Черные шляпы, Белые шляпы и Серые шляпы (kaspersky.ru)

Как стать белым хакером

Для кого-то перспектива стать белым хакером звучит заманчиво. Чтобы работать в сфере информационной безопасности, обязательно необходимы

базовые знания в сфере информационных технологий (ИТ). Получить соответствующее образование можно в вузе.

Квалифицированный белый хакер должен быть внимательным и уметь критически мыслить. Обязательно знать английский язык, основы программирования и построения сетей, иметь опыт администрирования, уметь настраивать системы защиты.

Не нарушать закон!

Если «белые шляпы» — это легитимные помощники организаций, то действия «чёрных шляп» расцениваются как противоправные. «Плохие хакеры» нарушают сразу три закона:

- «О персональных данных» (№ 152-ФЗ);
- «Об информации, информационных технологиях и защите информации» (№ 149-ФЗ);
- «Об авторском праве и смежных правах (№ 5351-1)».

За нарушение может грозить административная и уголовная ответственность вплоть до лишения свободы сроком до 7 лет.

Важно никогда не становиться «чёрной шляпой». Участие в противоправной деятельности (даже если удастся избежать административного или уголовного наказания) навсегда закроет доступ к этичному хакингу. Многие вакансии белых хакеров размещают государственные организации, чьи службы безопасности проводят серьёзные проверки кандидатов, включая полиграф.

Методы «серой шляпы» тоже не являются этичными. Их действия нарушают вышеуказанные законы. Интересно, что деятельность «белых шляп» также до сих пор официально не легализована. Поэтому даже белые хакеры рискуют быть привлечёнными к административной и уголовной ответственности.

Просмотр фильма (6 минут):
https://dzen.ru/video/watch/632edeffa017c6121654fdb5?share_to=telegram

Слайд 4

Учитель: Каждый день киберпреступники взламывают тысячи сайтов. Злоумышленники используют взломанные сайты для широкого спектра задач, от создания фишинговых страниц до рассылки SEO-спама. Владельцы небольших веб-сайтов наивно полагают, что находятся в безопасности, так как их сайты хакерам не интересны. К сожалению, обычно это не так.

Целью киберпреступников может стать практически любой сайт. Я приведу 10 возможных причин, по которым злоумышленники могут взломать сайт.

1. **Платежные реквизиты**

Веб-сайт, на котором что-либо продается - самая очевидная цель для киберпреступников. Хакеры могут украсть платежные реквизиты, а затем использовать их самостоятельно или кому-то продать.

2. Информация любого рода

Веб-сайты часто собирают личную информацию посетителей, например адреса электронной почты. На веб-сайте, используемом для ведения бизнеса, может храниться информация о сотрудниках компании или предстоящих выпусках продуктов.

Любая подобная информация может оказаться полезной для хакера. Киберпреступники либо продадут информацию в даркнете, либо предложат ее приобрести владельцу пострадавшего сайта в обмен на безопасный возврат данных.

3. Фишинговые страницы

Фишинговая страница - веб-страница, предназначенная для кражи конфиденциальной информации. Фишинговые страницы выглядят точно также как обычные веб-страницы, полностью повторяя их оригинальный дизайн. Киберпреступники создают фальшивые страницы, имитирующие веб-сайт банка, заманивая пользователей в свои сети. Ничего не подозревающий пользователь вводит на фишинговой странице данные для входа в банк, и конфиденциальная информация оказывается в руках злоумышленников.

4. Спам по электронной почте

Спам-рассылки доставляют пользователям неудобства, забивая почтовый ящик. Однако, на спам-рассылках можно заработать. Поэтому злоумышленники часто взламывают сайты, чтобы отправить спам и получить прибыль.

Взломав веб-сайт, киберпреступники будут использовать домен, чтобы избежать попадания в папку со спамом. Кроме того, хакеры смогут отправить большие партии сообщений, не отключаясь от собственного почтового провайдера.

Наихудшим последствием атаки является потеря репутации. Получатели спама, скорее всего, будут считать отправителем владельца взломанного сайта.

5. Вредоносное ПО

В настоящее время получение доступа к вредоносному ПО не является сложной задачей. Многие киберпреступники даже не создают вредоносные программы, а просто покупают их. Самое сложное в заработке на вредоносном ПО - найти способ установить его на чужие компьютеры.

Взломанный веб-сайт идеально подходит для подобной цели. Если Google доверяет вашему сайту, его можно использовать для распространения вредоносных программ без каких-либо предупреждений со стороны поисковика.

Доверяя сайту, пользователь, не задумываясь, может разрешить загрузку странного файла.

6. Бесплатная реклама

Сайты с большим трафиком рискуют быть взломанными в рекламных целях. Например, злоумышленник может разместить на сайте рекламу своего продукта.

Другим вариантом является перенаправление трафика. Пользователи, заходящие на взломанный сайт, будут автоматически отправляться на сайт хакеров.

7. Практика

Взлом - навык, требующий практики. Конечно, научиться взламывать можно в безопасной среде, многие онлайн-сервисы были созданы для такой цели. Однако, большинство хакеров начинают свою деятельность с реальных веб-сайтов.

Начинающий киберпреступник, вероятно, выберет для практики небольшой веб-сайт, прежде чем перейти к чему-то более прибыльному.

8. Развлечения

Иногда хакерам просто нравится взламывать. Множество громких кибератак осуществлялось исключительно по одной причине: злоумышленники хотели проверить свои возможности. Другими словами, хакер может выбрать целью ваш веб-сайт, чтобы проверить, сможет ли он его взломать.

Еще одна популярная мотивация - хвастовство. Хакер просто хочет похвастаться перед друзьями, что контролирует ваш сайт.

9. Перевод сайта в автономный режим

Хакеры часто взламывают веб-сайты с целью отключения. Сайты отключают из мести. Возможно, вы сказали или сделали что-то, что не понравилось хакеру. Также отключение сайта производят ради прибыли.

Сайты, приносящие деньги, - лакомая добыча для киберпреступников. Переведя такой сайт в автономный режим, хакер будет требовать у владельцев оплату в обмен на возобновление работоспособности ресурса.

Подробнее: https://www.securitylab.ru/analytics/524702.php

Часть 3. Заключительная

Слайд 5

Учитель: предлагаю подвести итоги!

Мы рассмотрели какие хакеры бывают: «Черные шляпы», «Серые шляпы», «Белые шляпы».

Помним с вами о том, что интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и Реальный мир – сеть тоже может быть опасна!

Всем до свидания! Хорошего дня!!

ПРОБЛЕМЫ ХАКЕРСТВА

ХАКЕР - ЭТО…

- профессионал, способный взломать системы электронной защиты, найти в них бреши и уязвимости;
- программист, который исправлял ошибки в программном обеспечении каким-либо быстрым или элегантным способом;
- «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасности

КАКИЕ ХАКЕРЫ БЫВАЮТ…

Black hats

(«Чёрные шляпы»)

Gray hats

«Серые шляпы»)

White hats

«Белые шляпы»)

Причины, по которым киберпреступники взламывают сайты

1. Платежные реквизиты
2. Любая информация
3. Фишинговые страницы
4. Спам по электронной почте
5. Вредоносное ПО
6. Бесплатная реклама
7. Практика
8. Развлечения
9. Перевод сайта в автономный режим

Как не стать добычей мошенников

Киберпреступники не спят

Правила общения с незнакомцами в сети Интернет

Интернет всё помнит

Быть анонимным в сети невозможно

Общайся с друзьями в реальной жизни, а не в онлайне!