Безопасный интернет - детям

Социальные сети — это не парк, а опасные «цифровые джунгли»

- Много хулиганов, троллей, травли, ссор и драк.
- Много мусора: ругани, негатива, оскорблений.
- Много опасных взрослых, вербовщиков, манипуляторов.
- Выстроены целые системы вовлечения в цифровые ловушки.

За порядком и безопасностью в социальных медиа не следит никто!

Кибербезопасность — это деятельность, направленная на защиту систем, сетей и программ от цифровых атак. Целью таких кибератак обычно является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей или нарушение нормального бизнес-процесса.

ТИПЫ УГРОЗ

ФИШИНГ

Это отправка подложных электронных писем, которые похожи на сообщения от надежных адресатов. Целью этого вида мошенничества является кража конфиденциальных данных, таких как номера кредитных карт и учетные данные. Это наиболее распространенный тип кибератак. Защититься от фишинга можно с помощью обучения пользователей или решения, которое блокирует вредоносные электронные письма

Вирусы-вымогатели

Один из видов вредоносного ПО. Они вымогают деньги, блокируя доступ к файлам или компьютерным системам до уплаты выкупа. При этом уплата выкупа не гарантирует восстановления доступа к

Вредоносное ПО

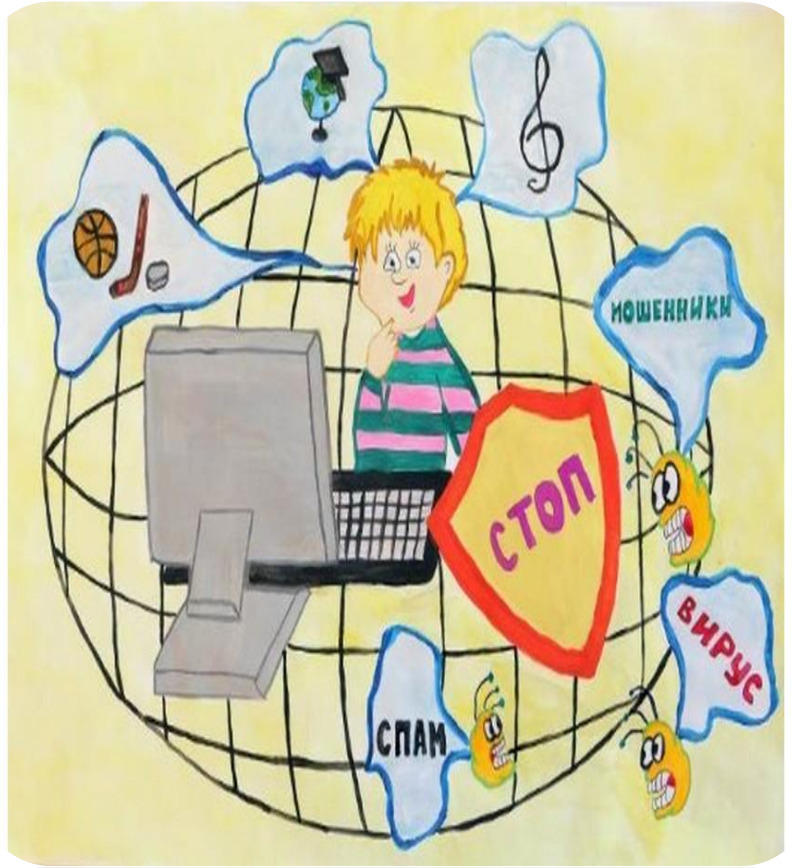
Это программное обеспечение, предназначенное для несанкционированного доступа к компьютеру или причинения ущерба

Социальная инженер

Социальную инженерию злоумышленники используют, чтобы обманом заставить вас раскрыть конфиденциальную информацию. Они могут попросить вас сделать денежный перевод или предоставить доступ к конфиденциальным данным. Социальная инженерия может сочетаться с любым из перечисленных выше типов угроз, чтобы вы с большей вероятностью переходили по ссылкам, загружали вредоносное ПО или доверяли вредоносному источнику

Советы по соблюдению кибербезопасности:

- не открывать электронные почты с неизвестных и подозрительных адресов;
- не открывать и не запускать неизвестные файлы;
- не скачивать и не устанавливать новый софт на рабочие компьютеры без уведомления технических специалистов;
- закрытый доступ к внутренним файлам (например, путем паролирования);
- использование сложных паролей с регулярным их изменением;



Защита личных мобильных устройств:

- никому не сообщайте свои пароли. Злоумышленники с лёгкостью могут воспользоваться данной информацией в мошеннических целях;
- используйте только официальные приложения, установленные из App Store, Google Play и Microsoft Store;
- используйте двухфакторную аутентификацию во всех приложениях, где это возможно, особенно в приложениях в социальных сетей;
- не переходите по подозрительным ссылкам: мошенники могут заразить ваше устройство вирусом и украсть ваши данные и, возможно, денежные средства с банковских счетов;
- заведите вторую Сим-карту для подключения к банковским сервисам и используйте её на телефоне, где нет доступа в интернет и возможности устанавливать стороннее ПО, что позволит сократить риск отправки СМС сообщений в банк без вашего ведома.

Правила безопасности в сети Интернет

Не рассказывать о себе и друзьях незнакомым людям в сети Интернет

Не встречаться со знакомыми из сети Интернет без предупреждения родителей

При регистрации придумывать сложный логин и пароль, не говорить их никому

Не отправлять смс для получения доступа к информации без ведома взрослых

Компания «Крибрум» основана в 2010 году Группой компаний InfoWatch и компанией «Ашманов и партнеры» с целью разработки интеллектуальной системы мониторинга и анализа социальных медиа

- Компания Криорум анализирует все социальные сети, блоги и СМИ Рунета
- Фейсбук, Твиттер, ВКонтакте, Инстаграм, Ютьюб, ЖЖ, каналы Телеграм, 22 тысячи интернет-СМИ блоги, форумы
- Выкачивается 80-100 миллионов сообщений в день, со скоростью от 15 секунд до 2 часов
- Мы анализируем группы, лидеров мнений, темы обсуждений, связи и психологические портреты пользователей

Мы видим всё, имеем архив с 2010 года

Социальные медиа в России

230 млн активных аккаунтов, пишущих на русском языке, которые принадлежат 80 млн человек.

89% пользователей Интернет в России имеют аккаунты в социальных сетях.

143 минуты в день пользователь в среднем проводит в социальных сетях.

90 млн сообщений в сутки публикуют в социальных медиа на русском языке.

В среднем у аккаунта 155 друзей в социальных сетях.

100 тысяч лайков в секунду ставят пользователи ВКонтакте.

публичным;
- Когда вы пишите как бы друзьям, читает весь Интернет;
- Даже в закрытой группе есть незнакомые или анонимные наблюдатели, о которых вы ничего не знаете;
- Даже переписка «один-на-один» может стать публичной (опубликует собеседник, его сестра или его родители);
- Есть «технические» наблюдатели — сама социальная сеть или мессенджер, системы мониторинга.

никогда не делайте в сети того, что вы побоялись или стеснялись бы делать публично

Поговорим о будущем !

Всё, что вы пишите в сети — навсегда, поисковики найдут сказанное через годы

Вы вырастите, станете другими людьми, с новыми друзьями и знакомыми, будет работа и, возможно, другие взгляды на жизнь

Через годы может быть неудобно, стыдно или невыгодно иметь такие цитаты, такие фотки и такие связи на публике

Сетевое поведение в школьном возрасте может сказаться при поступлении в ВУЗ или на работу, подаче документов на визу

Интернет — это машина времени. Но помнит он то, что люди о себе сообщают сами

ПОМНИТЕ О НАШИХ СОВЕТАХ

И ТОГДА ИНТЕРНЕТ СТАНЕТ ВАШИМ НАДЕЖНЫМ И ПОЛЕЗНЫМ ДРУГОМ