Театрализованное мероприятие

« Персональные данные в сети Интернет»  
  
Вступление :

Ведущий: Сегодня у нас в гостях великие рассказчики: Знайка, Многознайка и Всезнайка. Они всем расскажут много интересного и полезного. Ну не будем торопиться и начнем по порядку. Перед вами выступит Знайка.

Знайка : « Я вам расскажу о персональных данных в сети Интернет».

**Что такое персональные данные?**

*Персональные данные* - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Персональные данные и личная информация в Интернете**

Персональные данные – твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 – ФЗ  
 «О персональных данных»

**Кому и зачем нужна твоя персональная информация?**

* 80% преступников берут информацию в соц. сетях.
* Личная информация используется для кражи паролей.
* Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг , хищение!

При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!

Настрой приватность в соц. сетях и других сервисах

Не публикуй информацию о своём местонахождении и (или) материальных ценностях

Хорошо подумай, какую информацию можно публиковать   
в Интернете

Не доверяй свои секреты незнакомцам из Интернета.

Ведущий: Продолжает Многознайка.

Многознайка: « Я вам поведаю о киберугрозах».  
**Киберугроза** – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

Как обманывают в интернете?

1. Просят подтвердить логин/пароль.
2. Предлагают бесплатный антивирус.  
   А устанавливают вредоносное ПО, вирусы.
3. Просят отправить СМС (платное).

Серьёзные киберугрозы:

* Шпионское ПО
* Спам
* Фишинговые атаки
* Вирусы и вредоносные программы
* Мошеннические операции

Осторожно , спам! Первоначально слово «SPAM» появилось в 1936 г.   
Оно расшифровывалось как SPiced hAM (острая ветчина) и было товарным знаком для мясных консервов.

**Спам** – это анонимные массовые рассылки электронных писем на электронную почту пользователя, который не давал согласие не ее получения.

ПОМНИ: идя на поводу у СПАМа есть риск:

* Отправить платное СМС, оплатить навязанную услугу.
* Получить платную подписку на ненужную информацию.
* Потерять учётные и (или) иные данные.
* Стать жертвой обмана.

**Фишинг** - это особый вид компьютерного мошенничества.

Цель: получение доступа к персональным данным пользователя (логин и пароль)

**Компьютерный вирус** – это специально созданная программа, которая способна создавать свои копии, иногда не точные, но полное совпадение с оригиналом не обязательно.

**DDoS-атака**-распределенная атака-отказ в обслуживании, которая являет собой одну из самых распространенных и опасных сетевых атак.

**Кардинг** - способ мошенничества с использованием банковских карт. Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя.

Ведущий: А завершает Всезнайка.  
Всезнайка: « Я вас научу правилам защиты от этих угроз».

Осторожно, МОШЕННИКИ! Предупреждён – значит, вооружён

**Кардинг** - способ мошенничества с использованием банковских карт. Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя.

**Фишинговые сообщения** - это уведомления,отправленные от имени администраторов банковских или других платежных систем. Они призывают пользователей пройти по фальшивой ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету.

**Уведомления о выигрыше:** В письме сообщается о том, что ты выиграл крупную сумму денег. Цель мошенника - выманить у тебя деньги за получение выигрыша. Обычно он списывает это на налог. Потеряв бдительность, ты можешь перевести крупную сумму на счет мошенников.

Защита от мошенничества!

1)Удаляй письма, которые содержат не относящуюся к тебе информацию, связанную с денежными средствами, особенноот неизвестных людей.  
2) Не сообщай посторонним лицам свои персональные данные, номера счетов, пин-коды и т.п.  
3)Не переходи по ссылкам , указанным в подозрительных письмах.

**Запомни простые правила безопасности:**

Не уверен в своих знаниях? Используй учетную запись с ограниченными правами!

Не работай от имени администратора (root) - это убережет от большинства заражений; без необходимости не делай «джелбрейк», «разлочку», «рутование».

Используй антивирусную защиту (лучше бесплатный антивирус,   
чем никакого; коммерческие программы предоставляют дополнительные функции и удобства); Регулярно обновляй систему и антивирус.

Настрой дополнительные функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска);

Используй официальное лицензионное и (или) свободное программное обеспечение;

Учитывай рекомендации программ защиты (не заходи на сайты, которые помечены как опасные, не открывай файлы, которые блокирует антивирус);

Ограничивай время работы в Интернете – живи реальной жизнью!

Ведущий: А сейчас вы увидите маленькое, но очень «страшное» и поучительное театральное представление.

Театральное представление.

В одном маленьком селе, в одной маленькой школе, в одном маленьком классе – один большой Ученик нажимал большими руками на клавиши маленького компьютера. С целью найти в интернете много маленьких фактов о Великой истории.

Но внезапно, когда он вышел на незнакомый сайт, на него напал Могучий Вирус, желая уничтожить всю ее интеллектуальную базу знаний.

Но не знал Могучий Вирус , что на страже маленького компьютера стоит Всесильный Антивирус Касперского.

Одним ударом был уничтожен вероломный вирус.

И до сих пор в одном маленьком селе, в одной маленькой школе, в одном маленьком классе, один большой ученик и все его друзья нажимают руками на клавиши маленьких компьютеров.

Знайка , Многознайка, Всезнайка говорят вместе : « А ты подключил антивирус? Не тормози, подключи».

Заключение

Ведущий: Наше мероприятие подошло к концу. Но не забудьте извлечь из него правильный урок. Мы просим вас ответить на вопросы анкеты, прямо сейчас и высказать своё мнение о мероприятии.

**Анкета**

* Какую новую информацию вы узнали?
* Будет ли она вам полезна?
* Оцените результативность увиденного мероприятия по пятибалльной шкале.
* Оставьте свои комментарии об увиденном.