**Внеклассное мероприятие «Приватность в сети Интернет»**

**Цель:** создание условий для формирования правильной культуры поведения в глобальной сети Интернет.

**Задачи:**

1. Познакомить детей с понятием «Интернет», с правилами ответственного и безопасного поведения в современной информационной среде.
2. Расширить представление детей об интернете, формировать основы коммуникативной грамотности, чувства ответственности за своё поведение.
3. Воспитывать нравственное общение, информационную культуру обучающихся, внимательное отношение к информационным ресурсам, побуждать детей к самовыражению, саморазвитию.

**Форма мероприятия:** мотивационная беседа.

**Ход беседы:**

Распространение смартфонов, появление социальных сетей и других интернет-сервисов открыло для людей новые возможности: общаться с близкими и друзьями на большом расстоянии, делать покупки не выходя из дома, быстро распространять и получать информацию.

В то же время этим пользуются и злоумышленники. Персональная и личная информация, попавшая в Сеть, все чаще используется против ее владельцев в форме шантажа, буллинга и мошенничества.

Овладение основами цифровой грамотности и знание правил информационной безопасности является неотъемлемой частью жизни современного человека, а умение защитить свою приватность — важный навык 21 века.

Предлагаю вам сперва немного меня послушать, проверить или освежить свои знания. Затем мы их проверим.

Определения:

● Персональная информация — это та информация, по которой можно определить, кто вы.

● Приватность в Интернете — это право человека на сохранение в секрете своей персональной информации.

Приватность данных

Информация о ваших персональных данных попадает в Интернет множеством способов.

Например, когда…

● Заполняем анкету при регистрации на ненадежном сайте.

● Участвуем в сомнительных онлайн-опросах, конкурсах.

● Оплачиваем покупки в Сети на фишинговом сайте. ([Фишинг — это атака, пытающаяся украсть ваши деньги или вашу учетную запись.](https://support.microsoft.com/ru-ru/windows/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BE%D1%82-%D1%84%D0%B8%D1%88%D0%B8%D0%BD%D0%B3%D0%B0-0c7ea947-ba98-3bd9-7184-430e1f860a44)

Фишинговый сайт – это платформа для интернет-мошенничества, при котором злоумышленник получает…)

● Публикуем посты или сториз в социальных сетях, где рассказываем что-то о себе, отправляем данные в чатах, мессенджерах.

● Выкладываем фотографии, на которые случайно попадает персональная информация, например, табличка с названием улицы и номером дома.

Перечисленные варианты, касаются того, что мы САМИ можем контролировать. Но иногда наша приватность может зависеть от кого-то или чего-то другого, например:

● Публикации других людей о нас. Например, друзья размещают совместную с вами фотографию без разрешения.

● История наших поисковых запросов и посещенных сайтов. Ее обычно собирают поисковые системы, чтобы предложить вам более подходящую рекламу.

● А также установка и использование сомнительных приложений. Например, приложению «Фонарик» нужен доступ только ко вспышке, но если такое приложение просит доступ к контактам и сообщениям, это повод задуматься. Под видом благонадежного приложения, может на самом деле оказаться зловредное программное обеспечение или рекламный софт.

Чтобы уменьшить риски и сохранить приватность в Интернете надо соблюдать ряд простых правил:

● Когда регистрируетесь на сайтах, помните, что можно рассказать о себе, а что нет.

● В социальных сетях используйте «Настройки приватности». Ограничьте доступ незнакомых людей к вашей странице.

● Не сообщайте персональную информацию незнакомым людям. Мошенники могут маскироваться под знакомых ваших родителей, дальних родственников или сотрудников банка, писать вам в соцсетях или даже позвонить.

● Пользуйтесь защитными решениями и определителями номеров, а также VPN, когда подключаетесь к неизвестным общественным Wi-Fi сетям.

● Не переходите по подозрительным ссылкам в социальных сетях, почте или мессенджерах, даже если их прислали знакомые.

● Когда устанавливаете приложения на смартфон, не давайте им доступ к тем функциям, которые им не нужны. Например, приложению «Фонарик» явно не нужен доступ к вашим фотографиям или камере.

● Скачивайте приложения и программы только из официальных магазинов приложений.

● Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.

● Если хотите разместить фотографию со своим другом, не забудьте уточнить у него, разрешает он вам это сделать или нет. То же самое просите делать и по отношению к вам.

● Используйте двухфакторную авторизацию — это способ защитить свой аккаунт от несанкционированного доступа, даже в том случае, если ваш логин и пароль знают злоумышленники. Обычно это выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или электронной почте.

Знания освежили. Теперь можно их проверить на практике.

**● Овершеринг — стремление человека рассказывать окружающим больше, чем стоило бы, заходя слишком далеко с откровенностью и забывая о приватности**

Также давайте вспомним правила, которые касаются паролей. Пароль — это одна из важнейших составляющих вашей приватности.

Чтобы пароль был сложным для взлома, нужно придерживаться следующих правил:

● Если связка логин/пароль «утекла», то как можно скорее поменяйте пароль. Как это узнать? Есть специальные сайты для проверки утечек учетных записей. Обращайте внимание на новости о том, в каких сервисах произошли утечки.

● Меняйте пароль регулярно.

● Пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы.

● В пароле не должно быть общедоступной или личной информации, например, имени вашего питомца или номера телефона.

● Используйте разные уникальные пароли для разных сайтов.

● Не храните пароли на листочках, в текстовых файлах на компьютере. Для этого лучше использовать специальные программы — менеджеры паролей.

Безопасного пользования интернетом!