*Атрощенко Елена Александровна*

*Государственное бюджетное образовательное учреждение среднего профессионального образования Ростовской области «Ростовский-на-Дону автодорожный колледж»*

**План-конспект урока на тему:**

«Безопасность в сети Интернет»

для студентов 1 курса

**Тип урока:** Урок «открытия» нового знания.

**Деятельностная цель:** формирование информационной и компьютерной грамотности.

**Образовательная цель:** изучение основных принципов работы в сети Интернет с обеспечением информационной безопасности.

**Формирование УУД**

**Личностные действия:**

* Совершенствование информационной культуры;
* Соблюдение норм сетевого этикета.

**Регулятивные действия:**

* Планирование работы в сети Интернет в соответствии с санитарными нормами;
* Оптимизация работы в сети Интернет;
* Оценка эффективности работы в сети Интернет.

**Познавательные действия:**

* Изучение способов защиты ПК;
* Изучение безопасной работы в сети Интернет.

**Коммуникативные действия:**

* Безопасное общение в сети Интернет.

Ход урока

1. **Организационный момент (3 мин)**

Приветствие студентов, проверка присутствующих/отсутствующих на занятии.

1. **Актуализация знаний (7 мин)**
* Что такое Интернет?
* Какова польза от сети Интернет?
* Как вы думаете, опасен ли Интернет? Если да, то какой вред от использования Интернета?
1. **«Открытие» нового знания (35 мин)**

Стремительное развитие информационных технологий оказывает благотворное влияние на все сферы деятельности человека, в том числе и образовательную. Использование сети Интернет в учебном процессе, несомненно, имеет большое количество преимуществ, но при всей своей популярности Интернет не всегда дает желаемый результат и заключает в себе ряд опасностей. Происходит это чаще всего по причине низкого уровня информационной культуры и отсутствия компьютерной грамотности у всех участников образовательного процесса.

Поэтому нам с вами предстоит сегодня повысить уровень информационной культуры и безопасности. Сделаем мы это благодаря таблице, в которой отразим проблему и способы ее преодоления.

*табл. 1 «Опасности в сети Интернет, пути их преодоления»*

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Проблема** | **Способы преодоления** |
| 1 | Вирусы | * Установка антивирусной программы
* Осуществлять веб – серфинг по проверенным сайтам
* Блокировать всплывающие окна
* Внимательно проверять доменное имя сайта
* Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
* Проверять сохраняемые файлы, скачанные в Интернете
* Удалять электронные письма с вложениями от неизвестных и подозрительных адресатов
 |
| 2 | Спам, мошеннические письма | * Сообщать свой основной адрес электронной почты только хорошим знакомым
* Составлять адрес электронной почты, состоящий из букв и цифр
* Никогда не отвечать на спам, не переходить по содержащимся в нем ссылкам, не отписываться от спама и тем более не пересылать его по цепочке.
* Установить программу анти-спам
* Использовать сложные пароль и никому его не сообщать
* Не передавать учетные данные — логины и пароли — по незащищенным каналам связи
 |
| 3 | Фальшивые Интернет - магазины | * Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в Интернете
* Не доверять объявлениям о подозрительно дешевых товарах
 |
| 4 | Бесплатное скачивание файлов с подпиской | * Не указывать свой мобильный номер на незнакомых сайтах.
* Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.
 |
| 5 | Безопасность при оплате картами в сети | * Храните банковскую карту в надежном месте.
* Не держите записанные пароли и коды рядом с картой.
* Заведите отдельную карту для покупок в Интернете.
* Используйте для покупок в Интернете только личный компьютер.
* Регулярно обновляйте антивирусную защиту компьютера.
* Старайтесь делать покупки в известных и проверенных интернет-магазинах.
* Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
* Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех
* совершаемых платежах.
* Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.
* Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.
 |

*табл. 2 «Опасности общения в социальных сетях»*

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Проблема** | **Способы преодоления** |
| 1 | Проблема конфиденциальности | Размещая информацию о себе в социальных сетях, необходимо помнить, что ее может увидеть большое количество людей, в том числе родителей, работодателей и др. В итоге, личная жизнь становится достоянием общественности. |
| 2 | Взлом страницы мошенниками и злоумышленниками | Создавать безопасный пароль, который будет содержать в себе больше 10 символов и включать буквы, цифры и символы. |
| 3 | Страницы – фэйки, страницы – двойники  | Необходимо ограниченно сообщать личную информацию о себе, чтобы злоумышленники не смогли воспользоваться ею в своих целях. (не указывать домашний адрес, номер телефона, номер паспорта, и др.) |
| 4 | Интернет – зависимость  | Необходимо планировать время, проводимое в Интернете, и строго следовать этому, соблюдать санитарные нормы |
| 5 | Зависть и агрессия | Лучше размещать в социальных сетях фото проще. Успехами делиться с самыми близкими: теми, кто искренне за вас порадуется. |

1. **Первичное закрепление (20 мин)**

Создание личного и надежного электронного почтового ящика средствами почтового сервера **mail.ru**.

*Инструкция по созданию почтового ящика.*

* в адресной строке наберите <https://www.mail.ru>;
* выберите «Регистрация в сети»;
* заполните форму достоверными данными;
* выберите имя почтового ящика, из предложенных логинов сервером или придумайте свое;
* составьте надежный пароль, состоящий из 10 и более символов, запомните его;
* можете привязать почтовый ящик к номеру мобильного телефона, а можно выбрать альтернативный способ с секретным вопросом;
* зарегистрироваться.
1. **Рефлексия деятельности (20 мин)**

А теперь проверим, как вы усвоили важную информацию. Каждому из вас, необходимо зарегистрироваться на сайте [www.Сетевичок.рф](http://www.Сетевичок.рф) и поучаствовать в он-лайн квесте, который посвящен безопасности в сети Интернет.

*Инструкция по регистрации на сайте и участию в викторине.*

* запустить сайт [www.Сетевичок.рф](http://www.Сетевичок.рф);
* выбрать пункт меню вход/регистрация;
* заполнить форму регистрации достоверными данными;
* указать имя созданного вами ранее почтового ящика;
* зарегистрироваться;
* перейти в почтовый ящик;
* открыть письмо от сайта [www.Сетевичок.рф](http://www.Сетевичок.рф);
* перейти по ссылке на страницу [www.Сетевичок.рф](http://www.Сетевичок.рф);
* прочитать правила участия в квесте;
* запустить викторину и постараться правильно ответить на вопросы.
1. **Подведение итогов урока(5 мин)**

Сегодня мы познакомились с проблемами и способами их преодоления в сети Интернет. Участники викторины, набравшие наибольшее количество баллов получают оценку «отлично». Участники, недостаточно справившиеся с заданиями, получают оценку «хорошо». А также все участники викторины могут получить главные призы квеста, продолжив участие в квесте на своих домашних компьютерах, обязательно соблюдая правила безопасности в сети Интернет.

Спасибо за урок. Помните основные правила поведения в сети, и вы всегда сможете защитить себя от мошенников и злоумышленников.