Муниципальное бюджетное дошкольное образовательное учреждение детский сад общеразвивающего вида с приоритетным осуществлением деятельности по физическому развитию воспитанников № 113

г. Екатеринбург, ул. Шарташская, 16, тел./факс (343)350-13-08 e-mail: mdou113@eduekb.ru https://113.tvoysadik.ru/

Консультация для родителей: «Цифровая грамотность»

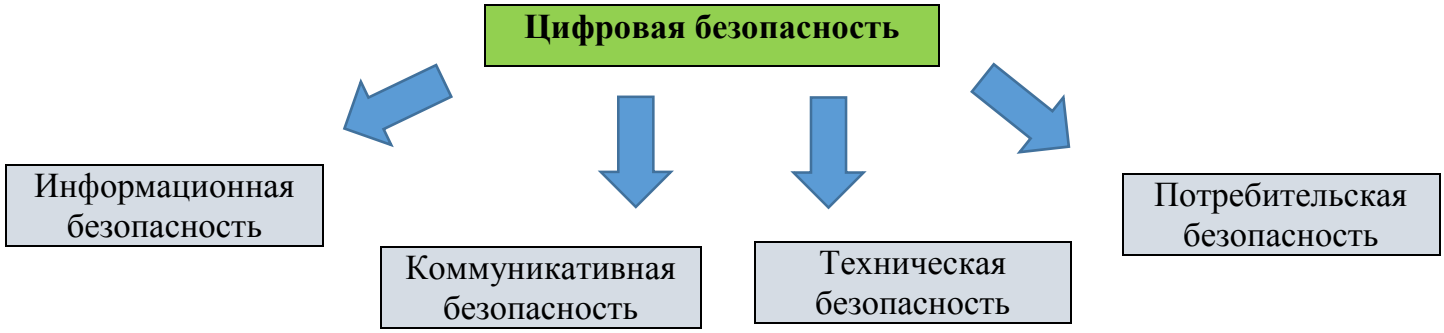
Выполнила: Пономарёва Лидия Васильевна
воспитатель I квалификационной категории

Екатеринбург
Апрель, 2025

Консультация для родителей:
«Цифровая грамотность»

В современном мире большие обороты набирает работа в информационной системе. Без выхода во всемирную сеть интернет не представляется возможной практически не одна профессия. Целесообразным поэтому считается быть человеком грамотным в области информационной безопасности.

Разберемся для начала, что же такое цифровая грамотность. Цифровая грамотность — это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета. Включает в себя: цифровое потребление, цифровые компетенции и цифровую безопасность. Последняя играет самую важную роль при работе в сети интернет.



Информационная безопасность

Сюда включается защита от клипового мышления, умение проверять достоверность информации. Сегодня всё чаще говорят о таком диковинном пока навыке, как информационная диета, когда человек умеет избегать лишней информации.

Коммуникативная безопасность

Это культура сетевого этикета, ваш цифровой имидж. Каждый из нас оставляет следы на тысячах серверов: комментарии, фото и видео, о которых мы даже не помним. Сеть помнит всё и по этим следам формируется ваш цифровой слепок. Чтобы узнать ваши увлечения, мировоззрение необязательно вас расспрашивать. Специальная программа проанализирует профили в социальных сетях и предоставит более точную и правдивую информацию о вас.

Техническая безопасность

Что в Интернете является оконечным устройством? Смартфон, телефон, планшет, компьютер, сервер. Именно они являются вашим терминалом выхода в сеть и хранителем информации о вас. Насколько ваши личные данные будут надежно сохранены, зависит от ваших навыков по работе с этими устройствами.

Потребительская безопасность

Сегодня в сети играют, учатся, работают, делают покупки. В силу сетевого характера это всё осуществляется немного по-иному, чем в офлайне. Иные правила, традиции и даже законы. Стоит это знать, чтобы не разочаровываться.

Клиповое мышление

Информационная индустрия гигантская. В сети около 2 миллиардов сайтов с текстами, видео, картинками и музыкой. Каждый год объем накопленной человечеством информации увеличивается на 30 %. Мозг человека, конечно, не успевает обрабатывать всю поступающую информацию. Он начинает защищаться от перегрузки и снижает глубину

анализа, переходя на обработку всё более коротких фрагментов. Мышление мозга, уставшего от потока информации, получило название «клипового мышления». Всего шесть основных последствий клипового мышления, конечно, у каждого человека по-своему проявляется этот синдром. У кого-то может быть один или несколько проявлений, ну а кто-то может быть обладателем всех.

Цифровая компетентность

Очень многие люди говорят, что им не зачем беспокоится о защите своих устройств. Ну, кроме того, что хакеры могут украсть что-то, они могут использовать ваше устройство в противоправных действиях. Атаковать банковскую сеть с вашего компьютера или разослать спам с вашего телефона.

Основная опасность для устройств со стороны хакеров. Хакер - это программист, который намеренно обходит системы компьютерной безопасности. Они используют две технологии для достижения своих целей. Первая техническая (различные вирусы), вторая социальный инжиниринг (социальные и психологические методы, которые принуждают жертву выполнить приказ хакеров).

1. Вирусы. В борьбе с вирусами помогает антивирусник. Программа различает поведение отдельных программ и выявляет подозрительные. Одна лишь проблема - вначале появляется вирус, а только после этого лекарство от него. Надо поставить лицензионный антивирус, зарегистрироваться на сайте компании и в случае проблем обращаться в техническую поддержку за помощью. Специалисты антивирусной компании оценят угрозу, помогут быстрее её устранить.

2. Социальный инжиниринг (фишинг). В основном фишеры подделывают сайты социальный сетей, онлайн-казино, сайты государственных организаций и т. д. Так же фишеры имитируют блокировку аккаунта в банке, соцсетях или электронном кошельке и от имени техподдержки выпрашивают логин и пароль. Почему так часто пользователи клюют на наживку фишеров? Фишеры - отличные психологи и используют социальную инженерию, от которой нет антивирусной защиты.

Об общении в сети

В Сети мы учимся, работаем, дружим, соримся, покупаем, общаемся. Интернет - это гигантский банк знаний человечества. Теперь в любом месте вы можете связаться практически с любым человеком на планете посредством телефона, электронной почты и социальных сетей.

В социальной сети сплетни эффективно распространяются в группе порядка 150 человек. Там у человека может быть тысяча друзей, но постоянные контакты поддерживает с теми же 150 людьми.

С ростом числа социальных связей снижается качество общения, уровень эмпатии, качество обмениваемой информации, растет агрессивность, разрушаются традиционные социальные связи с близкими и родными.

Сетевое взаимодействие регулируется уже специальными законами, которые делают наше сетевое общение более безопасным и эти законы надо знать.

Рекомендации, помогающие избежать интернет-угроз

1. Р*егулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.*

2. В интернете *не стоит переходить по ссылкам и нажимать кнопки* во всплывающих сообщениях, *которые кажутся подозрительными*. Даже если вас будут уверять, что там находится нечто очень важное лично для вас.

3. Для защиты личной информации придумайте *надежный пароль* и никому его не сообщайте. Для каждого ресурса стоит использовать *уникальные логины и пароли.*

4. Никогда *не предоставляйте секретные сведения*, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.

5. Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и *значка в виде закрытого замка* рядом с адресной строкой, который обозначает безопасное соединение.

6. Для безопасности общения в социальных сетях оставляйте *как можно меньше данных о себе* и избирательно подходите к предложениям о дружбе.

7. Откройте пункт ***«Настройки»*** *или* ***«Параметры»*** в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей.

8. Перед просмотром входящих писем на электронном ящике, *проверьте адрес отправителя.* Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.

9. В чатах и системах мгновенного обмена сообщениями вы никогда *не можете быть уверенными, кто с вами общается*. Постарайтесь избегать общения с незнакомцами и ни в коем случае *не соглашайтесь с ним на встречу в реальной жизни.*

10. Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.