СОГЛАСОВАНО:

Педагогическим Советом
МБОУ Жирновской СОШ

Протокол № 1 от 31.08.2023 г.

Секретарь М.В. Фисенко

УТВЕРЖДАЮ:

Директор МБОУ Жирновской СОШ

Приказ № 216 от 31.08.2023 г.

С.Я. Шкодин

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЖИРНОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
c=RU, st=Ростовская область, street=ул.Крупской д.7, l=п.Жирнов, title=Директор, o=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЖИРНОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА, 1.2.643.100.1=120D31303236313031363434393735, 1.2.643.100.3=120B303637303535363938383835, 1.2.643.100.4=120A36313334303031393630, 1.2.643.3.131.1.1=120C363133343031343730333232, email=tacmu@tacina.donpac.ru, givenName=Сергей Яковлевич, sn=Шкодин, cn=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЖИРНОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
2024.01.25 09:45:09 +03'00'

Инструкция для обучающихся МБОУ Жирновской СОШ по информационной безопасности

п. Жирнов

1. Общие требования информационной безопасности

1.1. Настоящая инструкция по информационной безопасности для обучающихся составлена с целью проведения инструктажа с учащимися 1-11 классов.

1.2. Основными опасными факторами в сети Интернет являются:

- использование ваших персональных данных для того, чтобы при помощи рекламы продать вам какую-то вещь;
- в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;
- с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;
- вредоносные программы могут испортить ваше программное обеспечение;
- участие несовершеннолетнего в группах смерти и тому подобных сайтах;
- можно попасть в поле зрения профессиональных преступных сообществ, радикальных экстремистских и террористических группировок, тоталитарных сект, использующих социальные сети для поиска и вербовки новых последователей.

1.3. Защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными

1.4. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

1.5. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

1.6. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.

1.7. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

1.8. Используйте только сложные пароли, разные для разных учетных записей и сервисов.

1.9. Старайтесь периодически менять пароли.

1.10. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

1.11. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.

1.12. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.

1.13. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов - читать такие высказывания так же неприятно, как и слышать.

1.14. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.

1.15. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.

1.16. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.

1.17. Не используйте Сеть для распространения сплетен, угроз или хулиганства.

1.18. Не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

2. Меры защиты от вредоносных программ:

2.1. Используйте современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2.2. Постоянно устанавливайте патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своейоперационной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
2.3. Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на вашем персональном компьютере;
2.4. Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
2.5. Ограничьте физический доступ к компьютеру для посторонних лиц;
2.6. Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
2.7. Не открывайте компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

3. Меры безопасности работы в общедоступных сетях Wi-fi:

3.1. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
3.2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3.3. При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
3.4. Не используйте публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
3.5. Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
3.6. В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

4. Меры безопасности в социальных сетях:

4.1. Ограничьте список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
4.2. Защищайте свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
4.3. Защищайте свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4.4. Если общаетесь с людьми, которых не знаете, не используйте свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
4.5. Избегайте размещения фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше местоположение;
4.6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
4.7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному

месту, а не во все сразу.

5. Меры безопасной работы с электронными деньгами

5.1. Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;
5.2. Используйте одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
5.3. Выберите сложный пароль. Преступникам будет не просто угадать сложный пароль.
5.4. Не вводи свои личные данные на сайтах, которым не доверяешь.

6. Меры безопасной работы с электронной почтой:

6.1. Выбирайте правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаете и кто первый в рейтинге;
6.2. Не указывайте в личной почте личную информацию.
6.3. Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
6.4. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
6.5. Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым вы доверяете. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
6.6. Не открывайте файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточните у них, отправляли ли они эти файлы;
6.7. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

7. Меры борьбы с кибербуллингом

7.1. Не ввязывайтесь в конфликт. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если начнете отвечать оскорблениями на оскорбления, то только еще больше разожжете конфликт;
7.2. Управляйте своей киберрепутацией; Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
7.3. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все ваши действия и сохраняет их. Удалить их будет крайне затруднительно;
7.4. Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7.5. Блокируйте агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
7.6. Если вы - свидетель кибербуллинга. Ваши действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

8. Меры безопасности для мобильного телефона:

8.1. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
8.2. Думайте, прежде чем отправить SMS, фото или видео. Вы не можете знать, где они окажутся в конечном итоге.
8.3. Необходимо обновлять операционную систему твоего смартфона;
8.4. Используйте антивирусные программы для мобильных телефонов;
8.5. Не загружайте приложения от неизвестного источника, ведь они могут содержать

вредоносное программное обеспечение;
8.6. После того как выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите cookies;
8.7. Периодически проверяйте какие платные услуги активированы на вашем номере;
8.8. Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете;
8.9. Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

9. Меры безопасности игрового аккаунта:

9.1. Если другой игрок ведет себя нехорошо или создает вам неприятности, заблокируйте его в списке игроков;
9.2. Пожалуйтесь администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
9.3. Не указывайте личную информацию в профайле игры;
9.4. Уважайте других участников по игре;
9.5. Не устанавливайте неофициальные патчи и моды;
9.6. Используйте сложные и разные пароли;
9.7. Даже во время игры не стоит отключать антивирус. Пока вы играете, ваш компьютер могут заразить.

10. Меры борьбы с фишингом (интернет-мошенничеством):

10.1. Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
10.2. Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
10.3. Используйте сложные и разные пароли. Злоумышленники получат доступ только к одному вашему профилю в сети, а не ко всем.
10.4. Если вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены в друзьях, о том, что страницу взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
10.5. Отключите сохранение пароля в браузере;
10.6. Не открывайте файлы и другие вложения в письмах даже если они пришли от друзей. Лучше уточни у них, отправляли ли они эти файлы.

11. Меры по защите цифровой репутации:

11.1. Подумайте, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
11.2. В настройках профиля установите ограничения на просмотр своего профиля и его содержимого, сделайте его только «для друзей»;
11.3. Не размещайте и не указывайте информацию, которая может кого-либо оскорблять илиобижать.
11.4. Помните:
- комментарии, размещение фотографий и другие действия могут не исчезнуть даже после того, как вы их удалите. Вы не знаете, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред.
11.5. Соблюдайте авторские права:
- авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. никто без разрешения автора не может воспроизводить его произведение, распространять,

публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в интернете.
- использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к вашим аккаунтам до блокировки вашего устройства, где установлена нелегальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

12. Правила безопасности по профилактике экстремизма.

Находясь в состоянии активного поиска, анонсируя в своем статусе наличие личных проблем, юноши и девушки часто сами натыкаются на вербовщика, который вводит молодого человека в свой круг общения, со временем формирует у нового знакомого устойчивый интерес к изучению исламской культуры, исламских традиций. Объект вербовки втягивается в изучение новой для него культуры в игровом режиме: он не замечает, как погружается в виртуальный мир-халифат, в котором постепенно и незаметно подлинные ценности мусульманской культуры подменяются более примитивными пропагандистскими идеологическими установками.
Экстремистскими будут те действия, которые связаны со стремлением разрушить, опорочить существующие в настоящее время общественные и государственные институты, права, традиции, ценности. При этом такие действия могут носить насильственный характер, содержать прямые или косвенные призывы к насилию. Лидеры экстремистских группировок различного толка завлекают молодежь в свои объединения, часто обещая ей легкое решение всех проблем. Наиболее эффективным средством массового информационного воздействия террористов на молодых людей стал Интернет.
12.1. Для того чтобы не попасться на уловки вербовщиков, стоит быть избирательным в общении с незнакомыми людьми, особенно онлайн, и соблюдать правила:
- будьте внимательны, когда к вам «стучится» новый знакомый. не принимайте в друзья всех подряд. выясняйте, кто он и откуда вы можете быть знакомы.
- если вам пришло сообщение непонятного содержания с незнакомого номера, не отвечайте на него.
- сохраняйте осознанность, понимание, что с вами происходит сейчас. вырабатывайте навык наблюдателя, задавайте вопросы: «зачем вы мне это говорите?», «для чего вам это нужно?».
- перепроверяйте любую информацию, исследуя предмет полностью, начиная с отзывов в интернете и заканчивая сводками МВД.
- не вступайте в диалог с проповедниками, подошедшими к вам на улице и предлагающими посетить собрание религиозной организации.
- если вам предложили листовку, брошюру, журнал религиозной направленности, поблагодарите и вежливо откажитесь.
- помните, что цель миссионеров-проповедников — убедить вас принять их учение. ваша цель — разобраться и не попасть в сети деструктивной религиозной организации.
- если вам предлагают заняться экстремистской деятельностью - не соглашайтесь, никакие доводы и уговоры не должны зародить в вас сомнения.
если возникли угрозы, то следует рассказать об этом близким людям и незамедлительно обратиться в правоохранительные органы.