ИНФОРМАЦИОННАЯ ПАМЯТКА
ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ ОБУЧАЮЩИХСЯ

С каждым годом молодежь всё более активно наполняет просторы глобальной сети «Интернет», при этом особую роль играют школьники – одни из самых активных пользователей Рунета. Вместе с неограниченными перспективами и доступностью информации Интернет несет и ряд угроз. Представленная памятка направлена на обеспечение безопасного пребывания в сети «Интернет» для данной категории пользователей.

Компьютерные вирусы

Компьютерный вирус – это вредоносная программа, способная самостоятельно распространяться и заражать компьютеры, системы или сети.

Он может выполнять различные вредоносные действия, такие как уничтожение, изменение или кража данных, блокировка работы компьютера или сети, перехват информации, нарушение работы аппаратной части и т. д.

Вирусы в персональный компьютер (ПК) обычно проникают через заражённые файлы, программы или внешние носители данных. Они могут быть скрыты под обычными файлами или программами, что затрудняет их обнаружение.

Чаще всего вирусы попадают в персональный компьютер в составе файлов, вложенных в сообщения электронной почты. Они могут проникнуть также в составе веб-страниц, полученных с инфицированных веб-сайтов, и с файлами, доставленными по компьютерной сети или скопированными с внешних информационных носителей.

Способы защиты от вредоносных программ:

Осуществляйте работу с использованием современных операционных систем, обладающих надежной защитой от вредоносных программ.

Регулярно устанавливайте патчи – цифровые обновления, предназначенные для исправления программных ошибок и улучшения работы системы. Скачивайте их исключительно с официального сайта разработчика операционной системы. Если доступен режим автоматического обновления, активируйте его.

Обязательно используйте антивирусные программы от именитых разработчиков с автоматической актуализацией баз данных.

Не позволяйте посторонним лицам иметь физический доступ к компьютеру.

Не открывай интернет-файлы, если их отправил неизвестный отправитель, даже если кажется, что это твой знакомый. Для большей уверенности лучше свяжись с ним и уточни, действительно ли он тебе их присылал.

Сети WI-FI

Wi-Fi – это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Бесплатный Wi-Fi в заведениях общепита, гостиницах и аэропортах предлагает удобный доступ к интернету. Однако многие специалисты считают, что общедоступные Wi-Fi сети представляют собой потенциальную угрозу безопасности.

Рекомендации по обеспечению безопасности при работе в общедоступных сетях Wi-Fi:

– не стоит делиться личной информацией через общедоступные Wi-Fi сети. Во время работы в таких сетях лучше воздержаться от ввода паролей, логинов и номерных данных;

– используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

– при использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

– не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

– используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;

– в мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети стали активной частью нашей жизни, и многие люди постоянно работают и «живут» в них. Многие пользователи не знают, что информация, которую они

размещают в социальных сетях, может быть обнаружена и использована кем угодно, даже если не всегда с добрыми намерениями.

Основные советы по безопасности в социальных сетях:

– ограничьте список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

–защитите свою конфиденциальность. Не сообщайте пароли, номера телефонов, адреса, даты рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести отпуск;

– защищайте свою репутацию – держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Думайте, прежде чем публиковать, писать или загружать;

– в разговоре с незнакомыми людьми не используйте свое настоящее имя или другую личную информацию (например, имя, место жительства, место учебы). Не размещайте в сети свои фотографии в местах, где вас могут обнаружить;

– при регистрации в социальных сетях используйте сложные пароли, состоящие из букв и цифр и не менее чем из одинакового количества символов. Используйте разные пароли для социальных сетей, электронной почты и других сайтов. Таким образом, если вас взломают, злоумышленник получит доступ только к одному месту, а не ко всем сразу.

Электронные деньги

Электронные деньги – цифровой эквивалент наличных денег, которые хранятся или обмениваются в цифровых компьютерных системах через Интернет. Электронные деньги являются очень удобным средством платежа, но есть и мошенники, которые хотят получить эти деньги. Сегодня Россия, по разным оценкам, относится к числу стран, проводящих активную деятельность по развитию электронных цифровых денег. В соответствии с положениями российского законодаательства электронные денежные средства представляют собой денежные средства, которые предварительно предоставлены одним лицом другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счёта, для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. Также необходимо различать электронные фиатные деньги (эквивалент государственной валюты) и электронные нефиатные деньги (не эквивалент государственной валюты).

Основные советы по безопасной работе с электронными деньгами:

– привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

– используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

– выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли – это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $nW7uh!;;

– не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта – это технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе – Интернета). Обычно электронный почтовый ящик выглядит так: имя_пользователя@имя_домена (например, somebody@example.com) и дает возможность передачи как простого текста, так и форматированного, а также произвольных файлов (текстовые документы, медиафайлы, программы, архивы и т. д.). Недостатки электронной почты: наличие такого явления, как спам (массовые рекламные и вирусные рассылки), возможные задержки доставки сообщения (до нескольких суток), ограничения на размер одного сообщения и на общий размер сообщений в почтовом ящике (персональные для пользователей).

В настоящее время любой начинающий пользователь может создать свой бесплатный электронный почтовый ящик, достаточно зарегистрироваться на одном из почтовых интернет-порталов.

Основные советы по безопасной работе с электронной почтой:

– необходимо выбрать правильный сервис электронной почты. В интернете существует огромное количество бесплатных почтовых сервисов, но лучше доверять тем, которые вам знакомы и имеют лучшую репутацию;

– не указывать в личной почте личную информацию. Например, вместо «theme13» выберите «music_fan@» или «rock2013». Когда помимо пароля нужно ввести код, присланный по SMS; выбирайте сложный пароль. Каждый почтовый ящик должен иметь сложный пароль, устойчивый к взлому;

– используйте несколько почтовых ящиков. Первый почтовый ящик может быть предназначен для личной переписки с лицами, которым ты доверяешь. Этот адрес электронной почты не должен использоваться для регистрации на форумах или сайтах.

– не открывайте файлы и другие вложения, даже если они получены от друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

– после завершения работы с почтовым сервисом не забудьте нажать кнопку «Выход», прежде чем закрыть вкладку на сайте.

Кибербуллинг или виртуальное издевательство

Кибербуллинг – это различные формы травли, где агрессор и жертва встречаются в сети Интернет. Чаще всего пострадавшими становятся дети и подростки как самая уязвимая категория пользователей. Он может проходить в социальных сетях, в приложениях для обмена сообщениями, на игровых платформах и мобильных телефонах. Это повторяющиеся эпизоды, цель которых – напугать, разозлить или опозорить тех, кого преследуют.

Условно можно выделить несколько видов кибербуллинга:

Флейминг. Нередко пользователи, высказывая свое мнение по теме поста, вступают в пререкания между собой. Несовпадение точек зрения становится толчком к насыщенной эмоциями дискуссии, собеседники начинают переходить на личности, применять оскорбления и постепенно вообще забывают о вопросе, с которого началось взаимное неприятие. Даже если один из них попытается свернуть перепалку, второй может не успокоиться и продолжит строчить злобные комментарии в адрес оппонента.

Задействование нескольких каналов коммуникации. Объект кибербуллинга может получать от инициатора травли сотни сообщений, комментариев, электронных писем, звонков. Все это крайне негативно отражается на психологическом состоянии жертвы.

Клевета. В виртуальном пространстве распространить о человеке ложную информацию в разы легче, чем в реальном мире. Киберслухи могут разлетаться со скоростью несколько сотен кликов в секунду. Этот способ навредить оппоненту применяют не только подростки, его берут на вооружение нечистоплотные пиарщики, когда надо испортить репутацию конкурента – коммерческого или политического.

Самозванство. Сюда относятся случаи использования имени или фейкового аккаунта жертвы для рассылки негативной информации его подписчикам. Праведный гнев знакомых жертвы будет обращен в его сторону, и объекту кибербуллинга придется долго доказывать, что он не имеет отношения к поступившим от его имени сообщениям.

Выманивание и распространение личной информации. Инициаторы травли любят

привлекать внимание к жертве, поставив ее в неудобное положение перед знакомыми и друзьями. В ход идут фото интимного содержания, видео, представляющие человека в неприглядном виде, переписка, в которой он позволил себе ненормативную лексику и т. д. Информация, не предназначенная для посторонних, после ее обнародования наносит серьезный вред жертве кибербуллинга.

Социальная изоляция. Для подростков важно быть членом социальной группы, поэтому исключение из нее воспринимается крайне болезненно. В результате длительного игнорирования падает самооценка, растет напряжение, ребенок перманентно находится в состоянии стресса. Бойкот в виртуальном пространстве даже более эффективен, чем в реальности: один клик, и человек полностью исключен из общественной жизни.

Киберпреследование. Более опасная форма, поскольку травля переходит из виртуального пространства в реальность. Злоумышленник отслеживает цифровые следы жертвы, выявляет адреса, пути перемещения, чтобы нанести ему физический вред (напасть, избить, изнасиловать и т. д.).

Хэппислепинг (happy slapping). Разновидность кибербуллинга, при которой жертву избивают, фиксируя процесс на камеру мобильного телефона, а затем выкладывая запись в Интернет.

Бороться с этим явлением можно и нужно. Не стоит бояться рассказать о нападках, «кормить» агрессора страхом и чувством стыда.

Основные советы по борьбе с кибербуллингом:

1. Игнорировать нападки.

Сдержите эмоции, не вступайте в перепалку с человеком, который явно хочет спровоцировать вас на ответную грубость. Моральное удовлетворение от флейминга вы вряд ли получите, а времени и нервов потратите немало.

2. Не винить себя.

Многие из нас склонны искать причину агрессивного поведения оппонента в себе: что я не так сказал, чем я вызвал волну негатива? Успокойтесь, лично вы тут ни при чем. Такому пользователю все равно, с кем затеять свару.

3. Исключить вероятность общения.

Создайте условия, при которых инициатор кибербуллинга не сможет продолжать свои действия. Внесите его в черные списки, поставьте запрет на поступление звонков и сообщений с его номера, а также писем с его электронных адресов.

4. Поделиться проблемой.

Кибербуллинг для подростков часто становится невыносимым испытанием, потому что им не с кем разделить свои переживания. Рассказать родителям – не всегда хороший

вариант, некоторым взрослым беды ребенка кажутся надуманными. Лучше позвонить в анонимную службу психологической поддержки: специалист внимательно выслушает, успокоит и даст дельный совет.

5. Бороться за свое спокойствие.

Травля в Интернете – явление распространенное, поэтому администрации соцсетей уже выработали алгоритм действий в случае жалоб на действия агрессивных пользователей. Они могут заблокировать профили, модерируют фотографии и посты, отслеживают появление комментариев с грубыми выражениями. Если дело дошло до угроз и клеветы, жертва кибербуллинга имеет все основания обратиться в полицию.

6. Дать отпор инициатору травли.

Агрессор рассчитывает, что вы будете оправдываться, отвечать на его выпады колкостями, то есть поддаваться на провокации. Любая другая реакция собьет его с толку. Попробуйте сразу заявить о своем намерении обратиться в суд с иском о клевете и угрозах. На многих грубиянов это действует отрезвляюще.

7. Повысить устойчивость к стрессу.

Жертвами травли часто становятся люди, плохо переносящие неблагоприятные жизненные ситуации. Любая мелочь может стать для них причиной серьезных переживаний, они легко впадают в панику, склонны к неадекватной реакции на происходящее. Стать более устойчивыми к стрессу таким чувствительным натурам помогут медитация, творческое хобби, дыхательная гимнастика.

8. Соблюдать цифровую диету.

Радикальный способ избавиться от виртуального преследования – полностью отказаться на время от социальных сетей. Удалите приложения из телефона, переключитесь на приятные дела в реальной жизни. Спустя некоторое время инициаторы буллинга забудут о вас, и вы сможете вернуться в любимые сообщества.

9. Изменить поведение в сети.

Если предыдущий способ вам не подходит, пересмотрите свое отношение к интернет-ресурсам. Сократите до минимума возможность использовать ваши аккаунты во вред вам: ограничьте количество пользователей, которым доступен размещаемый вами контент, удалите фотографии, которые могут спровоцировать травлю, и так далее.

10. Соблюдать правила цифровой грамотности.

Защищайте свое личное киберпространство при помощи регулярно сменяемых сложных паролей. Так вы предотвратите взлом ваших страничек и снизите вероятность кибербуллинга. Не переходите по сомнительным ссылкам, не устанавливайте непроверенные приложения.

Закон против кибербуллинга

Пока в российском законодательстве не предусмотрено меры ответственности за травлю в Интернете. Однако это не значит, что инициатора кибербуллинга нельзя привлечь к ответственности. Такие действия подпадают под статью 5.61 Кодекса Российской Федерации об административных правонарушениях, предусматривающую наказание в виде штрафа за совершение оскорбления с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

Наказание может быть назначено и по другим основаниям:

1. Клевета (статья 129 УК РФ).
2. Нарушение неприкосновенности частной жизни (статья 137 УК РФ).
3. Угроза убийством или причинением тяжкого вреда здоровью (статья 119 УК РФ).
4. Доведение до самоубийства (статья 110 УК РФ).
5. Оскорбление (ст. 5.61 КоАП РФ).
6. Вымогательство (статья 163 УК РФ).

Доказательствами для суда могут стать аудио- и видеозаписи, распечатки переписок в Сети, содержащих оскорбления и заверенных нотариусом. Пострадавший от кибербуллинга может написать заявление в полицию или обратиться с иском в суд.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

– ничего не является по-настоящему бесплатным. Помните, что в бесплатном контенте могут быть скрыты платные услуги – подумайте, прежде чем отправлять SMS, фотографии или видео. Ты точно знаешь, где они будут в конечном итоге?

– поддерживайте операционную систему смартфона в актуальном состоянии;

– используйте антивирусное программное обеспечение для своего мобильного телефона;

– не загружайте приложения из неизвестных источников, так как они могут содержать вредоносные программы;

– удаляйте файлы cookie в настройках браузера после того, как вы покинули сайт, на котором вводили личные данные;

– регулярно проверяйте, какие платные услуги подключены на вашем номере;

– сообщайте номер своего мобильного телефона только тем людям, которых вы знаете и которым доверяете;

– выключайте Bluetooth, когда он не используется. Не забывайте периодически проверять его.

Online игры

Современные онлайн-игры – это красочный и увлекательный вид развлечений, объединяющий сотни тысяч людей по всему миру. Игроки исследуют заданный мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. Они покупают диски, подписки и другие опции.

Все эти средства идут на поддержание и развитие игры, а также на обеспечение безопасности. Безопасность игры также является ключевым фактором ее успеха: улучшение системы аутентификации, выпуск новых патчей (цифровых исправлений для программного обеспечения) и устранение уязвимостей в серверах.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности игрового аккаунта:

– если другой игрок ведет себя плохо или раздражает вас, заблокируйте его в списке игроков;

– пожалуйтесь администратору игры на плохое поведение игрока, желательно с доказательствами, например скриншотами;

– не указывайте личную информацию в игровом профиле;

– уважайте других участников игры;

– не устанавливайте неофициальные патчи и моды;

– используйте сложные и разные пароли;

– не отключайте антивирус, даже играя в игру. Ваш компьютер может быть заражен во время игры.

Фишинг или кража личных данных

Кража денег и документов – повседневное явление, но с развитием интернет-технологий преступники переместились в Интернет, чтобы продолжить свое «любимое» дело.

В связи с этим появилась новая угроза. Интернет-мошенничество или фишинг, основной целью которого является получение конфиденциальных данных пользователей, то есть логинов и паролей. В английском языке фишинг читается как phishing (от phishing – пароль).

Основные советы по борьбе с фишингом:

– следите за своим аккаунтом. Если вы подозреваете, что ваш профиль был взломан, необходимо как можно скорее заблокировать его и сообщить об этом администратору ресурса;

– пользуйтесь безопасными веб-сайтами, включая интернет-магазины и поисковые системы;

– используйте сложные и разные пароли. Убедитесь, что в случае взлома злоумышленник сможет получить доступ только к одному профилю, а не ко всем вашим онлайн-профилям;

– установите надежные пароли (PIN-коды) на мобильном телефоне;

– отключите хранение паролей в браузере.

– не открывайте файлы и другие вложения, даже если это электронные письма от друзей.

Цифровая репутация

Цифровая репутация – это негативная или позитивная информация о вас в Интернете. Повреждающая информация, размещенная о вас в Интернете, может иметь серьезные последствия для вашей реальной жизни. Цифровая репутация – это образ вас, сформированный на основе информации о вас в Интернете.

Где вы живете, куда ходите в школу, каково ваше финансовое положение, какие черты характера и рассказы о близких хранятся и накапливается в Интернете.

Многие подростки легкомысленно относятся к размещению личной информации в сети и не подозревают о возможных последствиях, они могут даже не осознавать, что их отвергли из-за фотографии, которую они разместили пять лет назад.

Такие действия, как публикация комментариев или фотографий, могут не исчезнуть, даже если их удалить. Кто хранил информацию, сохранилась ли она в поисковых системах и, самое главное, что думают о вас окружающие, которые ее нашли

или увидели. С хорошими или плохими намерениями любой человек может найти эту информацию спустя годы. Это может случиться с каждым.

Основные советы по защите цифровой репутации:

– дважды подумайте, прежде чем публиковать или делиться чем-либо в блогах или социальных сетях;

– ограничьте доступ к своему профилю и его содержимому в настройках профиля и сделайте его «только для друзей»;

– не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные обучающиеся – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права – одно из средств защиты интеллектуальной собственности. Оно отличается от товарных знаков, которые позволяют их владельцам запрещать использование названий брендов, слоганов, логотипов и других характерных символов третьими лицами. 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. Авторское право распространяется на широкий круг произведений: книги, музыкальные произведения, произведения изобразительно искусства, скульптуру и кинофильмы, компьютерные программы, базы данных, рекламу, карты и технические чертежи.

Запрещается воспроизводить, распространять, публично демонстрировать, продавать, импортировать, сдавать в аренду, одалживать, публично исполнять, транслировать или размещать в Интернете любые материалы, защищенные авторским правом, без разрешения автора. Использование «пиратского» программного обеспечения сопряжено с рядом рисков, включая потерю учетных данных и блокировку устройств, на которых было установлено нелегальное ПО. Не забывайте также, что в сети существует легальное бесплатное программное обеспечение.