Автономная некоммерческая организация по содействию развития цифровых компетенций молодёжи и профилактике негативных явлений в информационной среде «Цифровые волонтеры»

Методическое пособие по информационной безопасности для участников проекта «Цифровой рост»

Москва, 2023

УДК 004.056.5
ББК 16.8

Методическое пособие по информационной безопасности для участников проекта «Цифровой рост» / Под ред. С. В. Большакова, Е. М. Пащенко, Г. В. Пащенко. М.: АНО «Цифровые волонтеры», 2023. 20 с.

В методическое пособие по информационной безопасности включены материалы, которые содержат основные правила, методы противодействия злоумышленникам в сети Интернет, составлены алгоритмы действий, согласно которым подросток сможет четко понимать, как ему поступить в ситуациях, создающих угрозу безопасности его персональных данных.

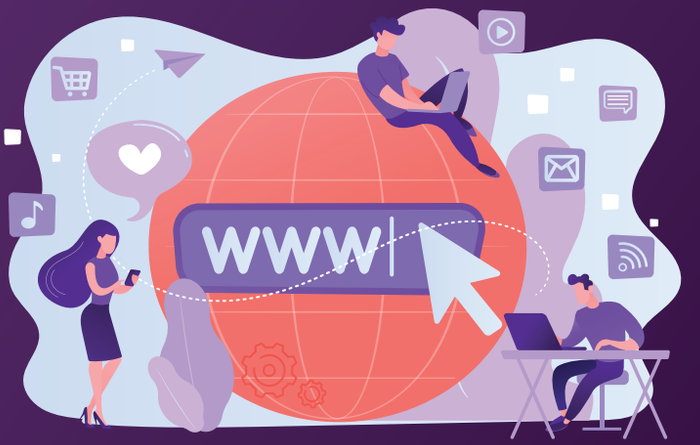
Содержание

Введение

Интернет уже давно стал незаменимым помощником современного человека.

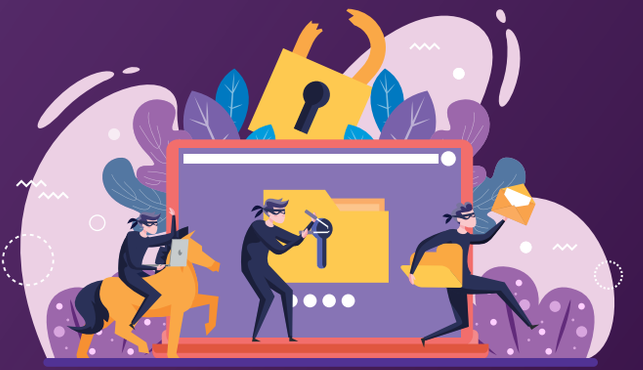
Всемирная сеть является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Именно поэтому молодежь активно пользуется Интернетом, а зачастую проводит в сети даже больше времени, чем взрослые. Юные пользователи осваивают сервисы мгновенных сообщений и интернет-телефонию, общаются на форумах и в чатах, каждый день узнают много новой увлекательной и образовательной информации.

Однако не стоит забывать, что Интернет может быть не только средством для обучения, отдыха или общения с друзьями, но и – как реальный мир – может быть опасен.



Личная информация представляет повышенную ценность и не может быть общедоступной. В компьютерах, смартфонах и прочих устройствах всегда присутствует риск потери, изменения, кражи и уничтожения данных, особенно если они подключены к сети Интернет. Для противодействия этому применяют разнообразные способы защиты информации, реализованные с помощью установки специального программного обеспечения (например, антивирус, файрвол), и основные правила при работе на устройствах и в сети Интернет.

Наиболее часто встречающиеся угрозы при работе в Интернет



1 **Угроза заражения вредоносным программным обеспечением (компьютерные вирусы, троянские программы и т.д.).**

Для распространения вирусов и проникновения в компьютеры используется почта, флеш-носители, CD-диски и прочие сменные носители, компьютерные и браузерные игры или скачанные из сети Интернет файлы.

2 **Доступ к нежелательному содержимому.**

Это насилие, наркотики, страницы, подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией, онлайн казино. Независимо от желания пользователя на многих сайтах отображаются всплывающие окна, а также специальные рекламные блоки, содержащие подобную информацию.

3 **Контакты с незнакомыми людьми с помощью чатов, электронной почты, Discord и т.д.**

Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи.

4 **Поиск развлечений (например, игр) в Интернете.**

Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег. Скачивая взломанную игру на свой компьютер, как правило можно заразить свое устройство ботнет вирусом, программой для майнинга криптовалюты, вирусом шифровальщиком и прочими компьютерными вирусами.

5 **Неконтролируемые покупки.**

Мошеннические сайты могут предлагать покупку игровых персонажей, читов для популярных игр и прочее, однако оплачивая данные покупки с банковских карт, вы можете остаться без самой покупки, и к вашей карте может быть подключен автоплатеж, чтобы незаметно списывать деньги с банковской карты.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению.

Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

Как правило, современные компьютерные вирусы направлены на использование вычислительных мощностей вашего устройства, например, для майнинга криптовалют, однако могут использоваться для кражи личных данных, в том числе игровых аккаунтов, сохраненных файлов с паролями и другое, а также давать злоумышленнику полный доступ к вашему устройству. В большинстве случаев распространяются вирусы через сеть Интернет.

Методы защиты от вредоносных программ

1. **Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.**
   Регулярно обновляйте операционные системы, драйверы устройств и другие программы и игры. В новых версиях, как правило, помимо нового функционала устраняются найденные уязвимости, что позволит защитить свое устройство от проникновения компьютерных вирусов и взлома.

2. **Работайте на своем компьютере под правами пользователя, а не администратора.**
   Это не позволит большинству вредоносных программ установиться на вашем компьютере.

3. **Используйте антивирусное программное обеспечение известных производителей с автоматическим обновлением баз.**
   Специалисты антивирусных лабораторий ежедневно находят вирусы и мошеннические сайты, что поможет им заблокировать вредоносный сайт, либо не допустить проникновение вируса в ваше устройство, а если по какой-то причине вирус смог попасть, то оперативно обезвредить его.

4. **Ограничьте физический доступ к компьютеру или смартфону для посторонних лиц.**
   Посторонние лица помимо хищения личных данных могут своими действиями заразить ваше устройство. Будьте внимательны, доверяя свое устройство в пользование третьим лицам.

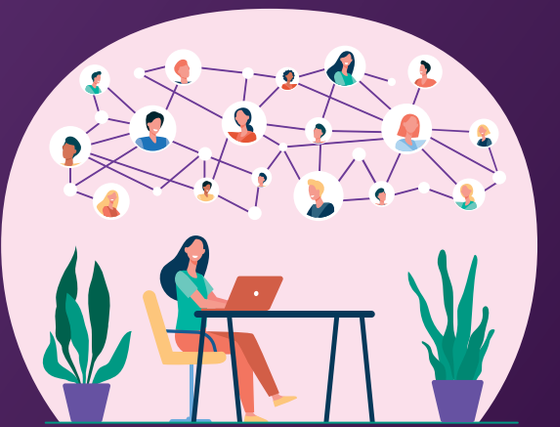
5. **Используйте внешние носители информации, такие как флеш-накопитель, CD-диск или файл из Интернета, только из проверенных источников.**
   Обязательно проверяйте все загруженное из Интернета и с флеш-носителя антивирусной программой.

6. **Не открывайте компьютерные файлы, полученные из ненадёжных источников.**
   Даже те файлы, которые прислал вас знакомый. Зачастую мошенники могут отправлять файлы могут от имени друзей.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно.

Пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.



Основные советы по безопасности в социальных сетях

1 **Ограничьте список друзей.**

У вас в друзьях не должно быть случайных и незнакомых людей. Часто добавляются в друзья мошенники, либо люди, которые хотят на вас заработать, предлагая решения контрольных работ, решения ЕГЭ и прочее, но зачастую после перевода денег, аккаунт становится недоступен.

2 **Защищайте свою частную жизнь.**

Не указывайте пароли, телефоны, адреса, дату вашего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести каникулы.

3 **Защищайте свою цифровую репутацию.**

Держите ее в чистоте и задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить, будь то личная фотография или репост из популярного сообщества.

4 **Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее.**

5 **Избегайте размещения фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше местоположение, удаляйте гео-метки из загружаемых фотографий.**

6 **При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством не менее 8 знаков.**

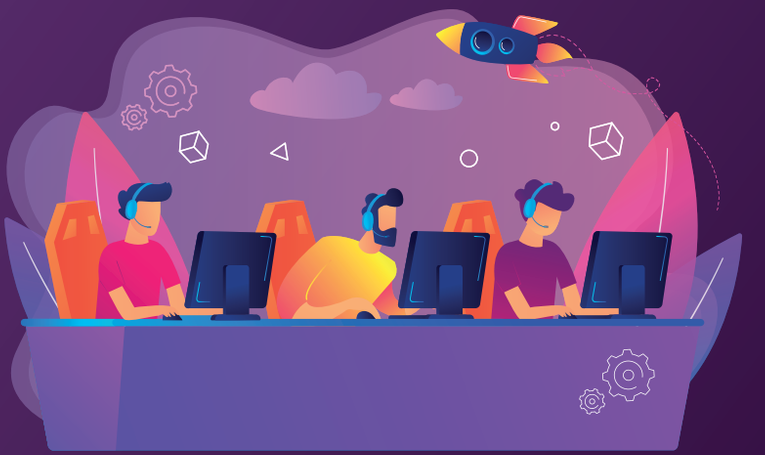
7 **Обязательно используйте двухфакторную аутентификацию.**

Даже если злоумышленник узнает ваш пароль, то при входе в аккаунт вам придет смс с кодом, который необходимо будет ввести, либо будет требоваться по-другому подтвердить действие входа, например через пуш-уведомление и прочее.

Онлайн игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру.

Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают голду, уникальные вещи или приобретают какие-то опции.



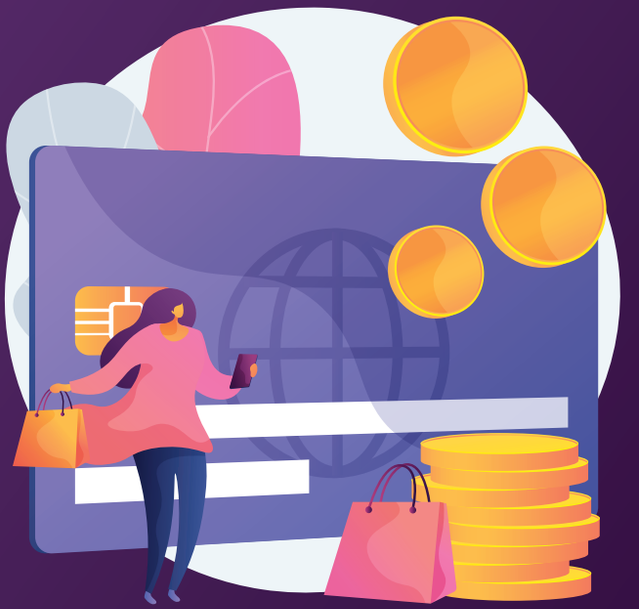
Основные советы по безопасности вашего игрового аккаунта

1. Если другой игрок ведет себя плохо или создает вам неприятности, заблокируйте его в списке игроков.
2. Пожалуйтесь администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скришотов.
3. Не переходите по внешним ссылкам и не загружайте присланные файлы от других игроков.
4. Не указывайте личную информацию в профайле игры.
5. Уважайте других участников по игре.
6. Не устанавливайте неофициальные патчи и моды.
7. Используйте сложные и разные пароли.
8. Даже во время игры не стоит отключать антивирус. Пока вы играете, ваш компьютер могут заразить.

Электронные деньги

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и неанонимные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.



Основные советы по безопасной работе с электронными деньгами

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.

2. **Используйте одноразовые пароли.**

   После перехода на усиленную авторизацию вам уже не будет угрожать опасность кражи или перехвата платежного пароля.

3. **Выберите сложный пароль и включите двухфакторную аутентификацию.**

   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, рубля, восклицательный знак и т.п.

   Например, $tR0ng!.

Фишинг

Фишинг – это вид интернет-мошенничества, используемого для получения логинов и паролей, а также другой информации пользователей.

Он применяется для кражи паролей, номеров карт, банковских счетов и другой конфиденциальной информации.

Как правило, фишинговая атака представляет собой выдачу фейковых сайтов, имитирующих интернет-страницы популярных компаний: соцсетей, интернет-магазинов, стриминговых сервисов и т.д. Злоумышленники рассчитывают на то, что пользователь не заметит подделки и укажет на странице личные данные: реквизиты карты, логин и пароль, номер телефона. Если человек сделает это, мошенники получат его данные.

Основные советы по борьбе с фишингом

1. **Следите за своим аккаунтом.**
   Если вы подозреваете, что ваш профиль был взломан, то необходимо заблокировать его и сообщить администраторам ресурса об этом как можно скорее.

2. **Используйте безопасные веб-сайты, в том числе интернет-магазины и поисковые системы.**

3. **Используйте сложные и разные пароли, а также двухфакторную аутентификацию.**
   Таким образом, если вас взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.

4. **Если вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у вас в друзьях, о том, что вас взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.**

5. **Установите надежный пароль на компьютер и смартфон.**

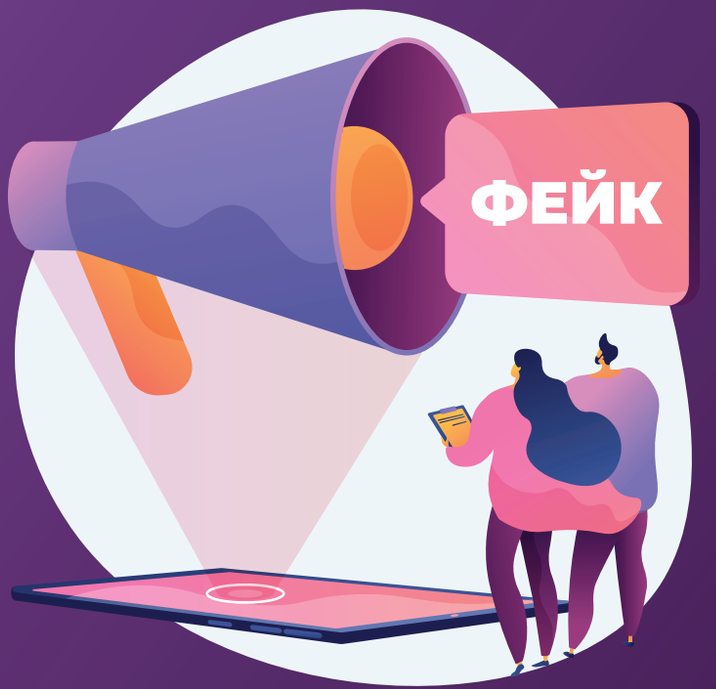
6. **Отключите сохранение пароля в браузере.**

7. **Не открывайте файлы, ссылки и другие вложения в письмах, даже если они пришли от ваших друзей.**
   Лучше уточните у них, отправляли ли они вам эти файлы.

Фейки в сети Интернет

В сети Интернет не всегда размещается только правдивая информация, наряду с ней часто можно встретить ложную, изменённую или так называемую фейковую информацию.

Она нацелена на изменение социальных норм и искажение реальности для дальнейшего воздействия на людей и манипуляцию их сознанием.



Методы защиты от ложной информации

Для защиты от такого вида «информационных вирусов», к сожалению, программных методов не существует. Вам необходимо всегда быть начеку и проверять поступающую информацию. В этом вам поможет фактчекинг.

Фактчекинг — это проверка информации на правдивость, точность и достоверность. Для этого существуют разные подходы и концепции.

Самой эффективной на текущий момент считается концепция «смерть автора». Идея данной концепции заключается в автономном существовании текста, в его независимости от личности автора.

Кто автор? Кем являлся? Насколько он был авторитетен?

Что за источник? Что там публиковалось до этого?

Совершенно не важно.

Прочитали, услышали что-то новое – изучите другие источники, послушайте, что говорят другие и после этого сделайте выбор – верить этому или нет.

ЦИФРОВЫЕ ВОЛОНТЕРЫ

Автономная некоммерческая организация по содействию развития цифровых компетенций молодёжи и профилактике негативных явлений в информационной среде «Цифровые волонтеры»

Методическое пособие подготовлено для проекта «Цифровой рост» в рамках конкурса грантов «Москва – добрый город» при поддержке Департамента труда и социальной защиты населения города Москвы.

127276, г. Москва, ул. Ботаническая, 14

Распространяется бесплатно

Москва – добрый город

ДЕПАРТАМЕНТ ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ ГОРОДА МОСКВЫ

ДЕПАРТАМЕНТ ДОБРЫХ ДЕЛ