Жизнь без интернет-рисков

Компьютерные вирусы

Использовать внешние носители информации (флеш, диск или файл из интернета, из непроверенных источников).
Открывать компьютерные файлы, полученные из ненадёжных источников.
Позволять физический доступ к ПК посторонним лицам.

Использовать современные операционные системы, имеющие серьёзный уровень защиты.
Работать на своем компьютере под правами Пользователя: это не позволит большинству вредоносных программ инсталлироваться на твоем ПК.
Постоянно устанавливать патчи и другие обновления своей операционной системы. Скачивать их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включить его.
Использовать антивирусные программные продукты известных производителей с автоматическим обновлением баз.

Фишинг (кража личных данных)

Открывать файлы и другие вложения в письмах от неизвестных отправителей.
Сохранять пароль в браузере.

Следить за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
Использовать безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.
Использовать сложные и разные пароли.
Если твой аккаунт взломан, предупредить об этом всех добавленных в «Друзья» и адресатов.
Установить надежный пароль (PIN) на мобильный телефон.

Online игры

Устанавливать неофициальные патчи и моды.
Указывать личную информацию в профайле игры.
Сразу соглашаться на приглашение переписываться, играть, обмениваться: проверь, нет ли подвоха.

Блокировать игрока в списке, если он нарушает правила игры или создает тебе неприятности.
Пожаловаться администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.
Использовать сложные и разные пароли.
Во время игры включать антивирус.

Сети Wi-Fi

Использовать публичный Wi-Fi для передачи личных данных.
Вводить пароли доступа, логины и какие-то номера телефонов, работая в Wi-Fi.
Допускать автоматическое подключение устройства к сетям Wi-Fi без твоего согласия.

При использовании Wi-Fi отключить функцию «Общий доступ к файлам и принтерам».
Использовать только защищенное соединение через «https://», а не «http».
Использовать и обновлять антивирусные программы и брандмауэр.
Отключить функцию «Подключение к Wi-Fi автоматически» в мобильном телефоне.

Мобильный телефон

Загружать приложения от неизвестного источника: они могут содержать вредоносное программное обеспечение.
Бездумно отправлять SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
Давать свой номер мобильного телефона случайным и малознакомым людям.

Быть осторожным, когда тебе предлагают бесплатный контент: в нем могут быть скрыты какие-то платные услуги.
Обновлять операционную систему твоего смартфона.
Использовать антивирусные программы для мобильных телефонов.
Зайти в настройки браузера и удалить cookies после выхода с сайта, где вводилась личная информация.
Периодически проверять, какие платные услуги активированы на твоем номере.
Выключать Bluetooth, когда ты им не пользуешься.

Социальные сети

Указывать пароли, телефоны, адреса, дату твоего рождения, место жительства, место учебы и другую личную информацию.
Размещать фотографии, где ты изображен на местности, по которой можно определить твое местоположение.
Размещать и указывать информацию, которая может кого-либо оскорблять или обижать.
Встречаться с Интернет-знакомыми в реальной жизни (необходимо посоветоваться со взрослым, которому доверяешь).

Ограничь список «друзей»: у тебя в «Друзьях» не должно быть случайных и незнакомых людей.
Использовать настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.
Прежде чем что-то опубликовать, написать и загрузить, подумать: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь?
Использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8 для социальной сети, почты и других сайтов.

Кибербуллинг

(форма травли,оскорбления, запугивания, хулиганства с помощью интернет-сервисов)

Бросаться в бой с обидчиком. Чем эмоциональнее ты реагируешь, тем активней травля: ведь она организована именно ради того, чтобы развлечься, наблюдая за твоей реакцией!
Выкладывать свои фото и видео, которые могут дать повод высмеять тебя.
Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно.

Сделать скриншот своей страницы, содержащей оскорбления и сохранить их для подтверждения факта травли.
Заблокировать агрессора.
Обратиться за помощью к взрослым (родителям или учителям, которым ты доверяешь): они могут тебя поддержать и обратиться в правоохранительные органы.
Изменить свои настройки в социальных сетях: внести обидчика в «Черный список», создать новые учетные записи; удалять из списка «Друзей» незнакомых и тех, кто тебе не нравится.
Обратиться в администрацию ресурса, указать дату и время кибербуллинга, приложить скриншот сообщения, сделать ссылку на профиль обидчика и на странице с сообщением.
Если ты стал свидетелем кибербуллинга, выступить против преследователя, поддержать жертву, сообщить взрослым о факте агрессивного поведения в сети.

Электронные платежи

Вводить свои личные данные на сайтах, которым не доверяешь.

Привязать к счету мобильный телефон: это поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.
Использовать одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехват платежного пароля.
Выбрать надежный пароль – не менее 8 знаков, включающий строчные и прописные буквы, цифры и несколько символов.

Электронная почта

Указывать в почте личную информацию.
Использовать при регистрации на форумах и сайтах адрес электронной почты, созданный для частной переписки.
Открывать письма и вложения в письмах, пришедших от неизвестных отправителей.

Выбирать надежный почтовый сервис.
Использовать двухэтапную авторизацию (когда помимо пароля нужно вводить код, присылаемый по SMS).
Использовать несколько почтовых ящиков. Создать сложный пароль для каждого почтового ящика.
Нажать на «Выйти» после окончания работы на почтовом сервисе перед закрытием вкладки с сайтом.

Проект "Безопасная школа Алтайского края"
Министерство образования и науки Алтайского края
КАУ ДПО «Алтайский институт развития образования имени А.М. Топорова»