«Безопасность в Интернет-пространстве»

Знаешь ли ты, кто такой Билл Гейтс?

Билл Гейтс

Это один из создателей операционной сети Windows, которая, скорее всего, стоит и на твоем компьютере. Можно сказать, что именно этот человек создал для нас те компьютеры, которыми мы пользуемся.

Как ты думаешь, сколько времени в день он разрешал своим детям проводить за компьютером?

Ответ тебя удивит:

45 минут в будни и 1 час, 45 минут в выходные. При этом он не разрешал детям пользоваться компьютером вечером перед сном, а до 14 лет и вовсе не давал им в руки гаджетов.

Другой известный человек, Стив Джобс,

основатель Apple и создатель знаменитого «Айфона», запрещал своим детям пользоваться гаджетами по ночам и в выходные дни, а также во время еды.

Почему так?

Да потому что эти люди больше других знают об опасности, которую несет Интернет-зависимость для здоровья и психики пользователей.

ПРИЗНАКИ:

1. Не ложишься спать, предварительно не посидев в смартфоне.
2. Каждый день ешь за компьютером или со смартфоном в руке.
3. Почти все выходные проводишь в Интернете, никуда не выходя.
4. Злишься или раздражаешься, когда приходится отложить смартфон или оторваться от Интернета.
5. Играешь в компьютерные игры два и более раз в неделю.
6. Сидишь в социальных сетях или «болталках» в ночное время.
7. Не высыпаешься, часто испытываешь головные боли или неприятные ощущения в глазах.

ОБЩАЙСЯ С ДРУЗЬЯМИ В РЕАЛЬНОЙ ЖИЗНИ,

А НЕ В ОНЛАЙНЕ!

ЕСЛИ ТЫ ХОЧЕШЬ ИЗБЕЖАТЬ ИНТЕРНЕТ-ЗАВИСИМОСТИ, ТО ПРИДЕРЖИВАЙСЯ ПРАВИЛ:

1. Сократи время использования гаджетов и компьютера.

2. Не бери в руки телефон минимум за час до того, как планируешь лечь спать. Интернет, социальные сети или игры могут вызвать яркие эмоции, которые помешают уснуть.

3. Не ешь за компьютером и не используй телефон во время еды. Отвлекись от них ненадолго, лучше пообщайся с родственниками или друзьями.

4. Старайся на выходных использовать компьютер и гаджеты как можно меньше. В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.

ПО ДАННЫМ ИССЛЕДОВАНИЙ В РОССИИ:

- 80% ШКОЛЬНИКОВ

не могут обойтись без смартфона

- 80% ШКОЛЬНИКОВ

страдают искривлением позвоночника

- 80% ШКОЛЬНИКОВ

страдают нарушением зрения

- 3-4% ВЫПУСНИКОВ

полностью здоровы

КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

1. Взлом аккаунтов в соцсетях и рассылка сообщений от друзей. Мошенники придумывают разные ситуации и просят срочно перевести деньги.

2. Сайты-подделки. Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-поделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.

3. Рассылка писем по электронной почте и в соцсетях с выигрышем. Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.

4. Звонки с поддельных номеров. Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.

5. Шантаж. Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях.

Проверяй адрес сайта!

Обрати внимание на настоящий адрес сайта! При наведении мыши реальный адрес отображается во всплывающей подсказке.

ЧЕМ ОПАСНЫСАЙТЫ-ПОДДЕЛКИ?

- Крадут пароли.
- Распространяют вредоносное ПО.
- Крадут персональные данные.
- Навязывают платные услуги.
- Крадут деньги.

Программы-ловушки

• Просят подтвердить логин/пароль

• Пугают блокировкой или заражением

• Просят прислать данные карты и CVV-код

1. Закрой страницу, блокировка пропала? Все в порядке!

2. Войди в сеть «как обычно» и убедись, что все в порядке!

3. Проверь систему своим антивирусом!

4. Удаляй письма с незнакомых адресов!

5. Игнорируй неизвестные ссылки!

6. Используй кнопки «Это спам»,

7. «Заблокировать отправителя».

Защита от мошенничества

1. Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию. При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.

2. Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили. Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номер у и с какой целью.

3. Проверяй адрес сайта. Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.

4. Обращай внимание на наполнение сайта. Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.

ЧТОБЫ НЕ ПОПАСТЬСЯ МОШЕННИКАМ – МЫСЛИ САМОСТОЯТЕЛЬНО!

- Не переходи по незнакомым ссылкам.
- Не открывай файлы из писем или сообщений, которые прислали незнакомые люди.
- Если же ты стал жертвой мошенников, то следует сразу же сообщить об этом родителям или классному руководителю.

ЧТО ОТНОСИТСЯ К ПЕРСОНАЛЬНЫМ ДАННЫМ?

Персональные данные

– это все данные о человеке, своего рода «паспорт его личности». Их раскрытие в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям.

Персональные данные

1. Фамилия, имя, отчество.

2. Все твои документы (паспорт, свидетельство о рождении, аттестат).

3. Банковские данные (номер счета, карты, пин-код, CVV-код).

4. Твоя контактная информация (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы).

5. Фотографии и видеозаписи с твоим изображением.

6. Данные о твоих родственниках.

7. Твои логины и пароли.

КАК ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

1. Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов. Пароль восстановить проще, чем вернуть украденные деньги.

2. Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.

3. Не отмечай местоположение своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.

МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

4. Не ставь в браузере «разрешить» всплывающим окнам. Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ исоглашаться на какое-либо действие.

5. Проверь, чтобы твои аккаунты не были доступны с чужих устройств. В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.

6. Закрой доступ к своим страницам в социальных сетях. Включи настройки конфиденциальности.

ТЕБЕ СЛЕДУЕТ ОСТЕРЕГАТЬСЯ НЕЗНАКОМЦЕВ В ИНТЕРНЕТЕ, КОТОРЫЕ:

1. Задают много вопросов о семье и личной жизни.
2. Просят об одолжениях в обмен на что-либо.
3. Убедительно просят никому о них не рассказывать и держать дружбу в тайне.
4. Задают вопросы о том, кто еще имеет доступ к твоему телефону, компьютеру или аккаунту.

ТЕБЕ СЛЕДУЕТ ОСТЕРЕГАТЬСЯ НЕЗНАКОМЦЕВ В ИНТЕРНЕТЕ, КОТОРЫЕ:

5. Настаивают на личной встрече.

6. Заставляют тебя чувствовать себя виноватым, шантажируют или даже угрожают.

7. Ведут с тобой такие разговоры, после которых ты ощущаешь печаль, тревогу, грусть, стыд, страх, одиночество, свою ненужность близким, разочарование в жизни или людях, безысходность, злость, ненависть, желание причинить кому-то боль (знай, что все это не твои чувства, а лишь умелая манипуляция твоим сознанием).

БУДЬ ОСТОРОЖЕН, ДОБАВЛЯЯ «ДРУЗЕЙ» ДЛЯ ОБЩЕНИЯ В СЕТИ!

ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

1. Страницы в социальных сетях лучше закрыть от посторонних. *Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои личные данные от попадания в руки преступников. Как правило, информацию о себе, своих увлечениях, хобби, фото с друзьями и многое другое мы публикуем в соцсетях. Очень часто информацию о нас злоумышленники берут в открытом доступе.*

2. Будь осторожен, когда добавляешь незнакомого человека в друзья, особенно того, кого ты не знаешь в реальной жизни. *Если же новый знакомый задает тебе много вопросов о семье или о том, где ты живешь и учишься, то никогда не рассказывай ему эту информацию. Сразу же сообщай о подозрительном незнакомце своим родителям.*

ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

3. Будь внимателен, если в переписке тебя призывают к действию и пытаются подловить. Об этом свидетельствуют такие фразы, как: «А ты сможешь или тебе слабо?» «Все мои знакомые уже это делали, в этом нет ничего такого» и аналогичные. Такие фразы должны тебя насторожить. Рекомендуем сразу блокировать подобные аккаунты.

4. Не соглашайся на встречу с людьми из Интернета. Под профилем твоего ровесника могут сидеть далеко не девочки и мальчики, а самые настоящие преступники. Всегда сообщай своим родителям о своих друзьях из Интернета, а также о том, куда ты направляешься, с кем собираешься встретиться во избежание опасности.

ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

5. Если человек, с которым ты общаешься в Интернете заставляет тебя испытывать негативные чувства и эмоции, о которых было написано ранее, поделись об этом с родителями или другими взрослыми людьми, которым ты доверяешь. Не стесняйся признаться в этом. Такие эмоции может испытывать любой человек, но только взрослый в состоянии помочь избавиться от них и защитить тебя от их воздействия.

Внимание!

НИКОГДА НЕ ДОБАВЛЯЙ В ДРУЗЬЯ ЧЕЛОВЕКА, С КОТОРЫМ ТЫ НЕ ВСТРЕЧАЛСЯ В РЕАЛЬНОЙ ЖИЗНИ!

Анонимность в сети

Анонимная информация – это информация, которая не имеет указания на автора.

Многим людям кажется, что Интернет – безопасное место, где каждый может тайно писать и делать все, что ему вздумается, поскольку пользователь скрыл своё настоящее имя. Но это не так. Всё, что однажды попало в Интернет, остается там навсегда. Автор всегда будет найден! Каждое твое действие в Интернете содержит информацию о том устройстве, с которого ты это делал – например, о телефоне или компьютере.

Внимание!

- Каждое действие или грубость в Интернете может иметь последствия.
- Клевета и оскорбление являются противоправными деяниями, за совершение которых предусмотрена уголовная и административная ответственность.
- Уважай других людей, относись с пониманием и состраданием к чужой беде.

Цифровой след

Невозможно пользоваться Интернетом и не оставлять след.

Даже если ты решишь ничего не публиковать, ничего никому не писать, в любом случае прочитанные и просмотренные посты, оставленные лайки будут формировать длинную историю твоей активности.

Будь острожен, по твоему следу могут идти преступники!

Внимание!

- В Интернете, как и в реальной жизни, нужно быть очень внимательным со своими словами и действиями, комментариями и лайками.
- Особенно осторожно следует относиться к личной информации, которую планируешь выложить в сеть. Ни в коем случае никому не отправляй фотографии интимного характера!
- Из Интернета, как мы уже знаем, ничего не удаляется. Всегда помни: чем меньше мы используем мобильный телефон или планшет, тем лучше!

Алгоритм защиты информации

1. Придумывай и используй разные сложные пароли для почтовых ящиков, социальных сетей и других сайтов.

2. Не размещай (выкладывай) в социальных сетях и не отправляй друзьям личные фото (видео) и фото (видео) своих родственников.

3. Не отмечай адрес и местоположение своего дома, учебы, дополнительных занятий.

4. Не описывай реальные маршруты своих прогулок и не указывай под фотографиями и видеозаписями названия твоего города, улиц и т.п.

5. Попроси родителей закрыть доступ к своим страницам в социальных сетях.

6. 80% информации о жертвах преступники находят именно в сети Интернет, и, увы, эту информацию ты можешь сообщить им сам.

Защити себя!