Путешествие в безопасный цифровой мир: Основные темы кибергигиены

Правила безопасности в интернете для детей — важная защита и интересное исследование.

Почему кибергигиена нужна каждому ребёнку?

Кибергигиена — это набор правил, которые помогают детям безопасно пользоваться интернетом, избегая мошенников, вирусов и защищая личные данные для спокойного общения и учёбы.

Персональные данные – ваша цифровая личность

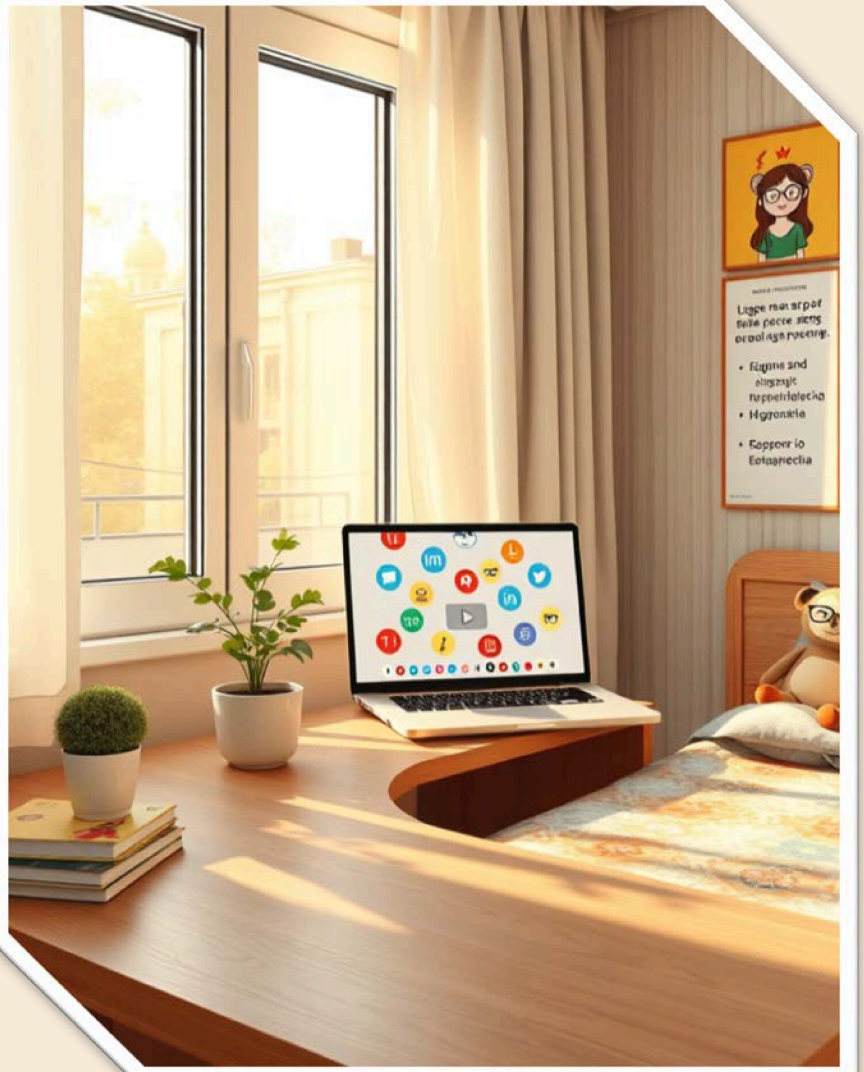
Ваша личная информация — имя, номер телефона, адрес и фотографии — формируют ваше цифровое «лицо». Она уникальна, как паспорт в реальном мире, и требует защиты.

Передавайте эти данные только тем, кому действительно доверяете, чтобы избежать мошенничества и сохранить безопасность в интернете для себя и близких.

Пароли – ключи от вашего цифрового дома

Создавайте сложные пароли, состоящие из заглавных и строчных букв, цифр и символов. Такие пароли надёжно защищают ваши аккаунты от взлома.

Регулярно меняйте пароли и не делитесь ими с другими. Это поможет сохранить ваши личные данные в безопасности и избежать неприятных ситуаций.



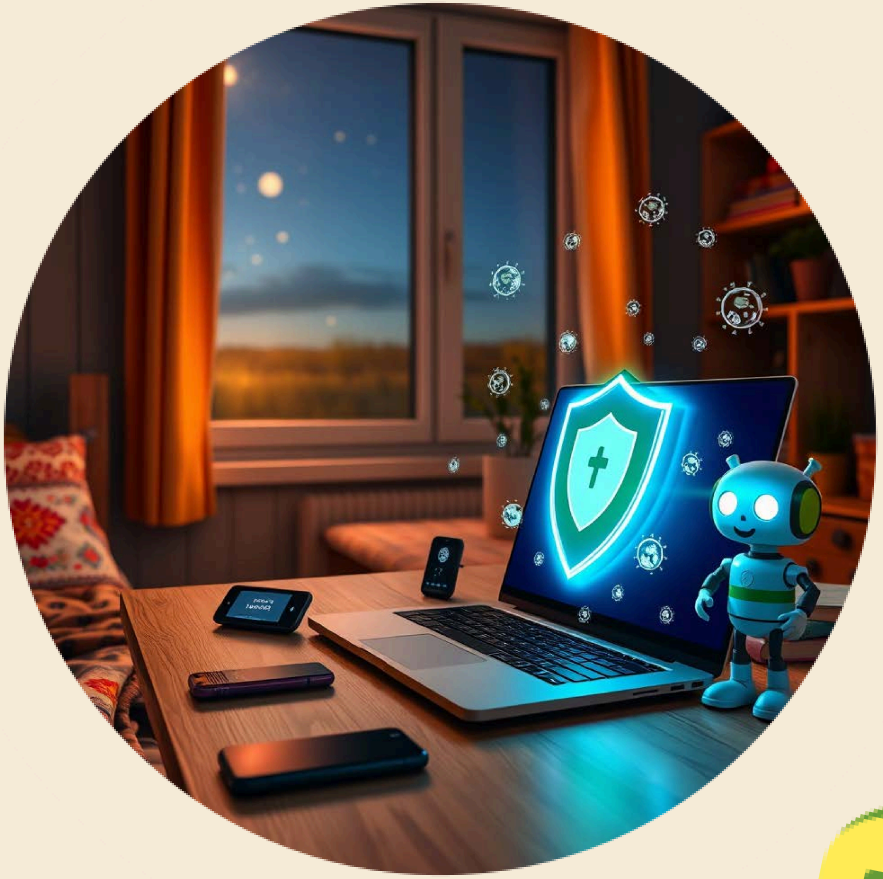
Правила общения в социальных сетях

Будьте внимательны с публикациями

Подумайте, что выкладываете в соцсетях, ведь ваши слова и фотографии остаются там навсегда и влияют на восприятие вас другими людьми.

Заботьтесь о своей репутации

Не делитесь личной информацией с незнакомцами и сохраняйте вежливость, чтобы избежать конфликтов и защитить себя от опасностей в сети.



Антивирус – ваш цифровой телохранитель

Антивирусные программы защищают ваш компьютер от вирусов, которые могут повредить файлы или украсть информацию. Обновляйте программы регулярно, чтобы быть под защитой.

Не открывайте подозрительные письма и ссылки, чтобы не заразить устройство вредоносными файлами. Антивирус помогает сохранить безопасность и работоспособность техники.

Примеры персональных данных и причины защиты

Имя и фамилия

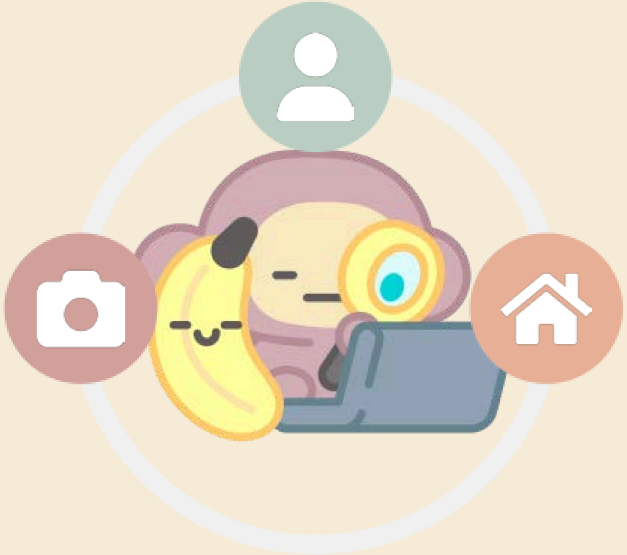
Ваше имя — это начало вашей цифровой личности, которую нельзя раскрывать посторонним, чтобы мошенники не смогли использовать её для обмана.

Адрес и школа

Эти данные важны для вашей безопасности. Злоумышленники могут использовать их, чтобы узнать о вашем местоположении и создать угрозу.

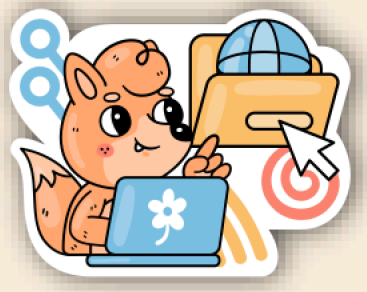
Фотографии

Фотографии могут раскрывать многое о вас. Не стоит выкладывать их в открытый доступ без необходимости, чтобы избежать нежелательного внимания.



Как создавать и запоминать сложные пароли?

Придумайте пароль из минимум 8 символов, комбинируйте буквы разных регистров и цифры, чтобы сделать его сложным для взлома.



Используйте запоминающиеся фразы или сочетания из слов и цифр, понятные только вам. Это облегчает хранение пароля без записей.

Не применяйте одинаковые пароли для разных аккаунтов. Это защитит вас, если где-то пароль злоумышленники узнают.

Безопасное поведение в социальных сетях

01

Не добавляйте в друзья незнакомцев, чтобы избежать общения с мошенниками и защитить личную информацию.

02

Не публикуйте ваш домашний адрес и номер телефона, чтобы сохранить личную безопасность и приватность.

03

Внимательно подумайте перед тем, как разместить фотографию или сообщение, чтобы не навредить своей репутации.

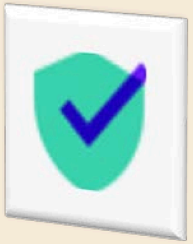
04

Помните, хорошие манеры и уважение в общении помогают сохранить друзей и доверие близких в интернете.

95%

обновлённый антивирус обеспечивает защиту от большинства современных угроз и предотвращает заражение устройства.

Исследование Касперского, 2023



Обновления антивируса помогают своевременно обнаруживать новые вирусы, предотвращая кражу данных и повреждение компьютера.

Как распознать интернет-угрозы?

Мошенники рассылают фальшивые письма и ссылки с вирусами. Они пытаются заставить вас перейти по ним или раскрыть личную информацию.

Перед тем как открывать сообщения или ссылки, убедитесь в надежности отправителя и адреса сайта. Это помогает избежать мошенничества.

Опасные ссылки и сообщения

Фишинг — ложные друзья

Проверяйте источники

Осторожность в сети

Фишинг — это когда кто-то притворяется знакомым или официальной службой, чтобы обмануть вас и получить доступ к вашим

Никогда не вводите пароли и личные данные на подозрительных сайтах. Настороженность и внимательность уменьшают риски

Примеры реальных случаев нарушения кибергигиены

01

Некоторые дети раскрывали свои имена и адреса в чатах, из-за чего мошенники пытались обмануть их семьи или получить доступ к аккаунтам.

02

Использование простых и одинаковых паролей среди детей приводило к взлому аккаунтов и утрате важных данных без возможности восстановления.

03

Публикация личных фотографий и информации о себе вызывала неприятности, такие как травля и недоброжелательное внимание от незнакомых пользователей.

Роль родителей и учителей в поддержке кибергигиены

Объяснение рисков

Родители и учителя помогают детям понять, какие опасности могут подстерегать в интернете и почему важно защищать свои данные.

Установка правил

Взрослые вместе с детьми договариваются о правилах пользования гаджетами, чтобы оградить их от ненужных рисков.

Поддержка и контроль

Постоянный диалог и совместный контроль помогают вовремя заметить проблемы и обучить детей правильному поведению в сети.

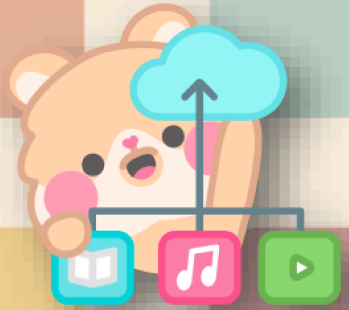
Как сделать цифровое путешествие безопасным и увлекательным

1

Создавайте надежные пароли, которые сложно угадать, сочетая буквы и цифры, и не используйте один пароль для разных аккаунтов.

2

Не делитесь личными данными или местом проживания с незнакомыми людьми, даже если они кажутся дружелюбными.



3

Будьте вежливы и внимательны при общении в социальных сетях, подумайте, прежде чем что-то публиковать или отправлять.

4

Регулярно обновляйте антивирусные программы, чтобы ваш компьютер и личные данные были под надежной защитой.

Кибергигиена – ключ к безопасному цифровому миру

Следуя правилам кибергигиены, каждый ребенок может уверенно и безопасно пользоваться интернетом, сохраняя личную информацию и устройства в безопасности, чтобы наслаждаться цифровыми возможностями без опасений.