2. **Интернет** — это огромная электронная сеть, которую часто называют «Всемирной паутиной», потому что она, словно невидимая нить, связывает людей и компьютеры по всей планете. В этом удивительном цифровом мире ты можешь **учиться, играть и находить ответы** на любые вопросы в огромном хранилище знаний. Это прекрасное место для общения и открытий, но в нём всегда нужно быть **внимательным и соблюдать правила безопасности.**

3. **Фишинг, смишинг и вишинг** — это разные хитрости мошенников, которые через письма, SMS или звонки притворяются важными службами, чтобы выманить твои секреты. Злоумышленники хотят украсть твои пароли или деньги, заманивая тебя на поддельные сайты или пугая поломкой компьютера. Чтобы не попасться, никогда не сообщай незнакомцам свои данные и не нажимай на ссылки в подозрительных сообщениях. Если тебе звонят или пишут «из банка» или «техподдержки» с просьбой что-то оплатить или переслать код, сразу положи трубку или удали письмо. Помни самое главное правило: если в интернете тебя что-то пугает или кажется странным, обязательно расскажи об этом взрослым.

4. **Социальная инженерия** — это когда интернет-обманщики используют хитрость и притворство, чтобы заставить тебя добровольно выдать им свои пароли или другие важные секреты. Злоумышленники могут выдавать себя за твоих друзей, помощников из техподдержки или людей в беде, чтобы втереться в доверие и обмануть тебя. Чтобы обезопасить себя, никогда не сообщай личные данные посторонним и **обязательно сразу рассказывай родителям**, если кто-то в сети просит тебя о чём-то странном или подозрительном.

5. **Ложная техподдержка** — это когда мошенники притворяются помощниками или работниками банка, чтобы напугать тебя поломкой аккаунта или потерей денег. Они могут уговаривать тебя перевести средства на якобы «безопасный счёт», но на самом деле это ловушка, чтобы украсть твои сбережения. Запомни: настоящие сотрудники никогда не спрашивают секретные пароли по телефону и не требуют срочно пересылать деньги незнакомцам. Если тебе пришло такое сообщение или кто-то позвонил с подобной просьбой, ничего не нажимай и **сразу позови взрослых**.

6. Твои имя, адрес и школа — это твои личные сокровища, которые называются персональными данными. Если они «утекут» в интернет, похититель может выдать себя за тебя и обидеть твоих друзей или семью. Чтобы защитить себя, никогда не сообщай незнакомцам свои секреты и не присылай им свои фотографии. Используй сложные пароли и общайся в сети только с теми людьми, которых ты знаешь в настоящей жизни. Если кто-то чужой просит тебя рассказать о себе или своей семье, сразу прекрати разговор и позови взрослых.

7. **Игровая валюта** — это цифровые деньги для покупок в играх, но злоумышленники часто используют твою жадность, предлагая горы золота «бесплатно» в обмен на номер телефона или SMS. Подобные обещания обычно оказываются обманом, из-за которого со счёта твоей семьи могут пропасть все настоящие деньги. Чтобы не попасться на удочку, **всегда советуйся со взрослыми** перед любой покупкой и никогда не верь слишком заманчивым подаркам в сети.

8. **Кибербуллинг** — это когда кто-то в интернете пытается тебя обидеть: пишет злые слова, дразнит в комментариях или выкладывает твои

фотографии без разрешения. Чтобы защитить себя, не отвечай на грубость и сразу **заблокируй обидчика**, чтобы он не мог больше тебе писать. Обязательно сохрани доказательства (сделай скриншот экрана) и **сразу расскажи родителям или учителю**, ведь взрослые всегда знают, как помочь. Будь вежлив с другими и помни, что ты имеешь право на доброе общение и безопасность в сети!

9. **Вредоносное ПО** — это «компьютерные простуды» или хитрые программы-червячки, которые могут пробраться в твой гаджет, чтобы поломать его или украсть твои данные. Такие «вирусы» часто прячутся в ссылках и файлах от незнакомцев, поэтому никогда ничего не скачивай и не открывай без разрешения взрослых. Чтобы защититься, обязательно используй **антивирус** — это надёжный щит и «прививка», которая не даст твоему устройству заболеть. Если экран стал вести себя странно или требует пароль, ничего не нажимай и **сразу расскажи об этом родителям или учителю**.

10. **DDoS-атака** — это когда хакеры отправляют на сайт так много запросов сразу, что он «устает» и перестает работать, словно в дверях образовалась огромная пробка. Если нужная страница не открывается, не нажимай на неё много раз подряд, а просто подожди или обратись за помощью к родителям. **Бесплатный Wi-Fi** в кафе или парке может быть ловушкой: через такую сеть мошенники умеют «подсматривать» твои пароли и личную переписку. Чтобы защитить свои секреты, старайся пользоваться только проверенным домашним интернетом и никогда не вводи важные данные в незнакомых сетях.

11. **Дипфейки** — это хитрые подделки, созданные специальными программами, которые могут «подменить» лицо или голос человека на видео, заставляя его говорить то, чего он никогда не произносил. Чтобы не попасться на такой обман, всегда внимательно присматривайся к деталям на экране и не верь всему, что видишь, если поведение человека кажется тебе необычным. Если «знакомый» в видеозвонке или ролике просит тебя выдать секрет или совершить покупку, **ничего не делай сам и сразу расскажи об этом родителям**.

12. **Пароль** — это твой самый важный цифровой секрет, который должен быть длинным и сложным, чтобы его не смогли разгадать посторонние. **Двухфакторная защита** работает как второй замок на двери: для входа в аккаунт тебе понадобится не только пароль, но и специальный код из SMS или твой отпечаток пальца. Никогда не сообщай свои пароли незнакомцам и попроси родителей настроить двойную защиту, чтобы твои игры и переписка всегда были в безопасности.

13. **Антивирус** — это твой цифровой защитник, который, как крепкий щит, охраняет гаджет от вредных программ. Регулярные **обновления** очень важны, так как они закрывают лазейки для мошенников и делают твою защиту ещё надёжнее. Всегда проверяй со взрослыми защиту гаджетов, чтобы твои игры и файлы всегда оставались в безопасности.

14. Твоя суперсила — критическое мышление! СТОП, СМОТРИ, СПРОСИ!