1. **Интернет** — это не просто «сеть», а глобальная цифровая экосистема, в которой мы живём: учёба, работа, финансы, контент, коммуникации — всё онлайн. Это пространство возможностей: можно запускать проекты, строить личный бренд, зарабатывать и прокачивать навыки. Но вместе с этим растёт и количество киберугроз — от банального скама до серьёзных атак. Каждый пользователь оставляет цифровой след, который может работать как на вас, так и против вас. Поэтому цифровая грамотность сегодня — это такой же базовый скилл, как умение читать и писать.

2. **Персональные данные** — это всё, что позволяет вас идентифицировать: ФИО, номер телефона, почта, фото, геолокация, данные карты и даже привычки. Утечка этой информации может привести к оформлению кредитов, взлому аккаунтов и репутационным проблемам. Всё, что вы публикуете, формирует ваш цифровой профиль — его видят не только друзья, но и алгоритмы, работодатели и мошенники. Используйте разные сложные пароли и не выкладывайте лишнего в открытый доступ. Чем меньше приватной информации в паблике, тем сложнее вас «развести».

3. **Социальная инженерия** — это взлом без взлома, когда атакуют не систему, а человека. Мошенники играют на доверии, страхе, срочности или эмпатии, чтобы вы сами отдали нужные данные. Они могут притворяться одногруппниками, сотрудниками банка, службой безопасности или знакомыми. Перед атакой они часто изучают ваши соцсети, чтобы звучать максимально правдоподобно. Лучший антидот — холодная голова и правило: никакие коды, пароли и доступы никому не передаются.

4. **Фишинг, смишинг и вишинг** — это разные форматы цифрового скама. Фишинг — через фейковые сайты и email, смишинг — через SMS и мессенджеры, вишинг — через звонки. Сценарий почти всегда один: создать панику или срочность и заставить вас слить код подтверждения или данные карты. Сообщения могут выглядеть как официальные — с логотипами, подменой номера и «службой безопасности». Любой кипиш с требованием «срочно перевести деньги» — повод поставить на паузу и проверить информацию через официальный канал.

5. **Дипфейки** — это фейковые видео и аудио, созданные с помощью ИИ. Технологии позволяют подделывать голос и лицо так, что отличить от оригинала становится сложно. Это используют для дезинформации, манипуляций и финансовых разводов. Если «знакомый» на видео просит срочно перевести деньги — это повод усомниться. Любую нестандартную просьбу нужно перепроверять через альтернативный канал связи.

6. **Финансовые ловушки** часто маскируются под «лёгкие деньги», быстрые инвестиции или срочное спасение средств на так называемом «безопасном счёте». Мошенники убеждают перевести деньги якобы для защиты от взлома или предлагают вложиться в «гарантированно прибыльный» проект с высокой доходностью и минимальными рисками. Отдельный тревожный сигнал — требование срочно снять наличные и передать их курьеру или «представителю службы безопасности». Ни банки, ни правоохранительные органы никогда не просят переводить деньги на сторонние счета или передавать наличные незнакомым людям — любые такие инструкции являются признаком мошенничества.

7. **Мошенничество в соцсетях** часто начинается со взлома аккаунта знакомого. От его имени рассылаются сообщения с просьбой срочно занять денег или скинуть код из SMS. Параллельно создаются фейковые профили, копирующие реальные страницы для втирания в доверие. Если сообщение выглядит странно — напишите человеку в другом мессенджере или позвоните лично. Сложные пароли и двухфакторная аутентификация серьёзно снижают риск таких ситуаций. **Ложная техподдержка** — классика жанра цифрового мошенничества. Вам сообщают о «взломе», «подозрительной операции» или

«угрозе блокировки» и требуют срочных действий. Часто предлагают установить программу удалённого доступа или перевести деньги на «безопасный счёт». Всё строится на давлении и тайминге: чем быстрее вы реагируете, тем меньше думаете. Реальные банки и сервисы не просят коды, пароли и переводы по телефону — любые такие требования это красный флаг.

8. **Вредоносное ПО** — это вирусы, трояны, шпионские программы и другой софт, который работает против вас. Его можно подхватить через пиратские файлы, подозрительные вложения, «кряки» и странные ссылки. Некоторые программы тихо собирают ваши пароли и банковские данные в фоновом режиме. Регулярные обновления системы закрывают уязвимости, которыми пользуются хакеры. Лицензионный софт и базовая кибергигиена — это не занудство, а нормальный уровень самозащиты.

9. **DDoS-атака** — это перегруз сервера огромным количеством запросов, из-за чего сайт «падает». Вы как пользователь повлиять на это не можете, сколько бы ни жали F5. Если сервис временно недоступен, проблема на стороне инфраструктуры, а не у вас. Главное — не искать «зеркала» на сомнительных сайтах, которые могут оказаться ловушкой. Иногда ожидание безопаснее, чем попытка обойти ограничение. **Публичный Wi-Fi** в кафе, ТЦ или транспорте — это потенциальная зона риска. В открытых сетях трафик может перехватываться, особенно если соединение не защищено. Через такие точки злоумышленники получают доступ к логинам, паролям и сессионным данным. В общественных сетях не стоит заходить в мобильный банк или вводить платёжные реквизиты. Если нет альтернативы, используйте дополнительные инструменты защиты и двухфакторную аутентификацию.

10. **Кибербуллинг** — это системная травля в онлайне: хейт, угрозы, слив личной информации или фото без согласия. В отличие от обычного конфликта, это целенаправленное давление. Такое может происходить в соцсетях, чатах, на форумах и игровых платформах. Вступать в перепалку — значит подливать масла в огонь. Скриншоты, блокировка и обращение к администрации платформы — более эффективная стратегия.

11. **Пароли и двухфакторная аутентификация** — это база цифровой безопасности. Один и тот же пароль на всех сервисах — подарок для злоумышленника. Надёжный пароль должен быть длинным и уникальным, а хранить его лучше в менеджере паролей. Двухфакторная аутентификация добавляет ещё один уровень защиты — код из приложения или биометрию. Даже если пароль утечёт, второй фактор может спасти аккаунт.

12. **Антивирусное программное обеспечение** — это базовый элемент цифровой безопасности, который помогает выявлять и блокировать вредоносные программы, фишинговые сайты и подозрительную активность. Решения, такие как PRO32, Kaspersky и Dr.Web, предлагают комплексную защиту устройств от современных киберугроз. Однако даже самый надёжный антивирус неэффективен без регулярных обновлений баз и операционной системы, поскольку именно обновления закрывают обнаруженные уязвимости. Своевременный апдейт системы и защитного ПО — это простая, но критически важная мера для снижения риска взлома и утечки данных.

13. **Критическое мышление** — главный софт, который нельзя скачать, но можно прокачать. В онлайне вас постоянно пытаются зацепить на эмоции: страх, жадность, срочность, хайп. Любое давление — сигнал поставить паузу. Перед тем как переводить деньги или отправлять данные, задайте себе вопрос: кто выигрывает от того, что я сейчас это сделаю? Правило простое: Стоп — Думай — Проверяй.