1. **Интернет** — это глобальная цифровая инфраструктура, объединяющая миллиарды устройств и пользователей по всему миру. Его часто называют «Всемирной паутиной», потому что он связывает людей, сервисы, базы данных и платформы в единую систему. Через интернет можно учиться, работать, управлять финансами, создавать проекты и строить профессиональные связи. Однако вместе с возможностями растут и риски: мошенничество, утечки данных, кибератаки. Поэтому цифровая грамотность сегодня — это не дополнительный навык, а базовая необходимость.

2. **Персональные данные** — это любая информация, позволяющая идентифицировать человека: ФИО, номер телефона, адрес, документы, данные банковских карт и даже фотографии. Утечка таких сведений может привести к финансовым потерям, мошенническим займам и репутационному ущербу. Важно осознавать, что всё опубликованное в сети формирует цифровой след. Используйте уникальные пароли для разных сервисов и настраивайте параметры конфиденциальности в социальных сетях. Чем меньше лишней информации доступно публично, тем ниже риск её злоупотребления.

3. **Социальная инженерия** — это метод психологического воздействия, при котором человек сам раскрывает доступ к своим данным. В отличие от технического взлома, здесь основным инструментом является манипуляция доверием, страхом или сочувствием. Мошенники могут представляться коллегами, сотрудниками банка, представителями службы безопасности или даже знакомыми людьми. Они тщательно изучают информацию в социальных сетях, чтобы сделать общение максимально убедительным. Главная защита — сохранять холодный анализ ситуации и не передавать личные данные без проверки личности собеседника.

4. **Фишинг, смишинг и вишинг** — это формы цифрового мошенничества, направленные на получение конфиденциальных данных пользователя. Фишинг реализуется через поддельные письма и сайты, смишинг — через SMS и сообщения в мессенджерах, а вишинг — через телефонные звонки. Злоумышленники создают ощущение срочности или угрозы, чтобы человек действовал импульсивно и передал пароли, коды подтверждения или реквизиты карты. Часто они копируют стиль официальных организаций и используют подмену номеров. Любое сообщение с давлением, требованием немедленного перевода средств или передачи кода нужно воспринимать критически и проверять через официальный сайт или приложение компании.

5. **Вредоносное программное обеспечение** — это программы, созданные для кражи данных, слежки или вывода устройств из строя. Оно может распространяться через заражённые файлы, пиратский контент, вложения в письмах и подозрительные ссылки. Некоторые виды вредоносного ПО незаметно собирают пароли и банковские данные. Регулярные обновления операционной системы закрывают уязвимости, которыми пользуются злоумышленники.

Использование лицензированного антивируса и внимательность при установке программ значительно снижают риски заражения.

6. **DDoS-атака** представляет собой перегрузку сервера большим количеством запросов, из-за чего сайт становится временно недоступным. Пользователь в такой ситуации не может повлиять на восстановление работы ресурса, поэтому не стоит многократно обновлять страницу.

7. Серьёзную угрозу представляют открытые сети Wi-Fi в общественных местах. Через незащищённое соединение злоумышленники могут перехватывать передаваемые данные. При использовании публичного интернета не рекомендуется вводить банковские реквизиты и конфиденциальную информацию без дополнительной защиты.

8. **Ложная техподдержка** — распространённая схема, при которой злоумышленники сообщают о «взломе аккаунта» или «подозрительной операции». Они могут предлагать установить программу удалённого доступа или перевести деньги на так называемый «безопасный счёт». Часто разговор сопровождается давлением и утверждением, что счёт будет заблокирован в течение нескольких минут. Настоящие сотрудники банков и IT-сервисов не запрашивают пароли, коды подтверждения и переводы средств по телефону. Если возникает подобная ситуация, необходимо самостоятельно связаться с организацией через официальный номер или сайт.

9. **Игровая валюта, инвестиции, фейковые конкурсы** нередко становятся инструментом мошенничества. Предложения «бесплатных бонусов» или «эксклюзивных скинов» за ввод номера телефона или пароля обычно ведут к потере аккаунта или списанию реальных средств. Поддельные сайты могут визуально копировать официальные игровые платформы. Перед вводом данных необходимо проверять адрес сайта и его подлинность. Любые финансовые операции в цифровой среде должны быть осознанными и подтверждёнными через официальные сервисы. Помни, бесплатный сыр только в мышеловке!

10. Мошенничество в социальных сетях часто связано со взломом аккаунта: злоумышленник от имени вашего знакомого просит срочно перевести деньги или сообщить код подтверждения. Распространены и фейковые профили, которые копируют реальные страницы или создаются специально для обмана и втирания в доверие. Если друг неожиданно обращается с финансовой просьбой или требует передать данные, важно проверить информацию — связаться с ним другим способом или задать уточняющий вопрос. Для защиты используйте сложные пароли, включите двухфакторную аутентификацию и не реагируйте на сообщения под давлением или с ощущением срочности.

11. **Кибербуллинг** — это систематическая травля в онлайн-пространстве, включающая оскорбления, угрозы и распространение личной информации без согласия. В отличие от разового конфликта, кибербуллинг носит повторяющийся и целенаправленный характер. Он может происходить в социальных сетях, мессенджерах, на форумах и игровых платформах. Важно не вступать в эскалацию и не отвечать агрессией на агрессию. Следует сохранять доказательства нарушений, использовать функции блокировки и при

необходимости обращаться к администрации платформы или взрослым наставникам.

12. **Дипфейки** — это цифровые подделки аудио и видео, созданные с применением технологий искусственного интеллекта. Они позволяют имитировать голос и внешность человека, создавая реалистичную, но ложную запись. Такие материалы могут использоваться для дезинформации, шантажа или финансовых мошенничеств. Особенно опасны ситуации, когда «знакомый» человек на видео просит срочно перевести деньги или сообщить код доступа. Любую подобную информацию необходимо проверять через альтернативные каналы связи.

13. **Пароль и двухфакторная аутентификация** являются базовыми инструментами защиты цифровых аккаунтов. Надёжный пароль должен быть длинным, содержать разные типы символов и не использоваться повторно на других платформах. Хранение паролей в менеджерах паролей повышает уровень безопасности. Двухфакторная аутентификация добавляет дополнительный этап проверки личности — код из приложения, SMS или биометрическое подтверждение. Даже если пароль будет скомпрометирован, второй фактор существенно усложнит несанкционированный доступ.

14. Ключевой навык современного пользователя — **критическое мышление**. В цифровой среде важно не поддаваться эмоциям и не реагировать импульсивно на провокации. Любая срочность, запугивание или чрезмерно выгодное предложение требуют дополнительной проверки. Перед передачей данных или переводом средств стоит задать себе вопрос о достоверности источника. Принцип «Стоп – Думай – Смотри – Проверяй» остаётся универсальным правилом информационной безопасности.