**Слайд 1: Пароли и двухфакторная аутентификация**

**Текст на слайде:**  
*Пароли и двухфакторная аутентификация*

**Речь:**  
*"Сегодня мы поговорим о двух ключевых инструментах безопасности: паролях и двухфакторной аутентификации. Вы узнаете, как создавать надёжные пароли, зачем нужны менеджеры паролей и почему 2FA — это обязательный уровень защиты."*

**Слайд 2: Почему пароли важны?**

**Текст на слайде:** **Почему пароли важны?**

***Пароли важны, потому что они защищают аккаунты, данные и ресурсы от несанкционированного доступа злоумышленников****.*

*-80% взломов происходят из-за слабых паролей.*

*-123456, qwerty, password – самые популярные пароли.*

*-Утечки данных случаются даже у крупных компаний.*

**Речь:**  
\*"Пароль — это как ключ от вашей цифровой жизни. Если он простой, злоумышленники могут легко его подобрать. Например, пароли вроде '123456' или 'password' взламываются мгновенно. В 2024 году из-за утечек пострадали миллионы пользователей."\*

**Слайд 3: Как создать надежный пароль?**

**Текст на слайде: Как создать надежный пароль?**  
Для создания надежного пароля, необходимо нужно:

-12+ символов -Буквы (A-Z, a-z), цифры (0-9), спецсимволы (!, #, $) -Не используйте личную информацию

Примеры надежного пароля: MaMaMidLalamy2046, J8#kL3$pQ9!mN2 **Примеры ненадежного пароля: qewrty123, dima228**

**Речь:**  
*"Хороший пароль — длинный и сложный. Вместо одного слова используйте фразу и заменяйте буквы на символы. Например, 'Я люблю кофе' можно превратить в 'Y@lybljuK0f3!'. И никогда не используйте один пароль для всех сервисов!"*

**Слайд 4: Менеджеры паролей**

**Текст на слайде:**  
*Менеджеры паролей*

Что они делают?

* Генерация сложных паролей.
* Автозаполнение на сайтах.
* Хранят пароли в зашифрованном виде.

**Лучшие менеджеры:** Bitwarden, 1Password, Kaspersky Password Manager.

**Речь:**  
*"Запоминать десятки паролей сложно. Менеджеры паролей делают это за вас: они хранят данные в зашифрованном виде и даже предупреждают об утечках. Вам нужно запомнить только один мастер-пароль."*

**Слайд 5: Двухфакторная аутентификация (2FA)**

* **Текст на слайде:**  
  *Двухфакторная аутентификация (2FA)*  
   это метод защиты онлайн-аккаунтов, который требует подтверждения личности не только с помощью пароля, но и второго фактора, который только может предоставить пользователь. Это дополнительный уровень безопасности, который усложняет взлом аккаунта даже если злоумышленник получит пароль.

Некоторые способы 2FA:

**-SMS-коды**

**-Аутентификационные приложения**

**-Биометрическая аутентификация**

**Речь:**  
*"Даже если хакер узнает ваш пароль, без второго фактора (например, кода из приложения) он не войдёт в аккаунт. Всегда включайте 2FA в важных сервисах: почте, соцсетях, банках."*

**Слайд 6: Итоги**

**Текст на слайде:**  
*Итоги*

* Создавайте длинные и сложные пароли.

(12+ символов)

* Храните их в менеджере паролей.

 (не в браузере!)

* Всегда включайте двухфакторную аутентификацию.

(для важных аккаунтов)

**Речь:**  
*"Запомните эти три правила — и ваши данные будут под надёжной защитой. Безопасность начинается с простых действий!"*

**Слайд 7: Вопросы?**

**Текст на слайде:**  
*Спасибо за внимание! Есть вопросы?*

**Речь:**  
*"Если что-то осталось неясно или хотите узнать больше — спрашивайте! Также рекомендую проверить свои пароли на haveibeenpwned.com."*