**Сценарий для презентации: Пароли и двухфакторная аутентификация**

**Слайд 1: Приветствие**

* **Текст на слайде:** "Добро пожаловать на презентацию о паролях и двухфакторной аутентификации!"
* **Говорить:** "Здравствуйте! Меня зовут Янова Анна, и сегодня мы обсудим важные аспекты безопасности в интернете, такие как создание сложных паролей, использование менеджеров паролей и значимость двухфакторной аутентификации. Эти меры помогут защитить ваши данные от киберугроз."

**Слайд 2: Цели и задачи**

* **Текст на слайде:** "Цели и задачи"
  + Понять, как создавать сложные пароли
  + Узнать о менеджерах паролей
  + Осознать важность двухфакторной аутентификации
* **Говорить:** "Цели и задачи мероприятия: понять, как создавать сложные пароли, узнать о менеджерах паролей и осознать важность двухфакторной аутентификации. Эти аспекты помогут нам защитить личные и корпоративные данные."

**Слайд 3: Правила создания сложных паролей**

* **Текст на слайде:** "Правила создания сложных паролей"
* Должен включать:
  + Не менее 8-ми символов
  + Использование букв двух регистров (строчные и заглавные)
  + Не только буквы, но и цифры
  + Использование символов, например: ! № $ ? & \* ()
* Должен исключать:
  + Имена и фамилии
  + Какие-либо даты, например, дату рождения
  + Цифры и буквы расположенные подряд на клавиатуре
  + Одинаковые символы повторяющиеся несколько раз
* **Говорить:** "Первое правило — создание сложных паролей. Рекомендуется использовать пароли длиной не менее 8-ми символов, включающих заглавные и строчные буквы, цифры и специальные символы. Избегайте использования личной информации, такой как имена или даты рождения. Цифры и буквы, расположенные подряд на клавиатуре. Также символы повторяющиеся несколько раз. Например, пароли вроде '123456' или 'password' легко подбираются хакерами."

**Слайд 4: Как создать надежный пароль**

* **Текст на слайде:** "Как создать надежный пароль"
* **Говорить:**

1. **Используйте фразы**: вместо одного слова попробуйте создать фразу из нескольких слов. Например, "Собака\_бегает\_по\_парку!" — это длинный и сложный пароль, который легко запомнить.
2. **Заменяйте буквы на символы**: вы можете взять фразу и заменить некоторые буквы на похожие по форме символы. Например, "Собака\_бегает\_по\_парку!" можно преобразовать в "S0b@k@\_b3g@eT\_по\_парку!". Это добавляет сложности, но при этом фраза остаётся запоминающейся.
3. **Используйте рифмы или ассоциации**: создайте пароль, который будет рифмоваться или ассоциироваться с чем-то знакомым. Например, "Мама\_мыла\_ламу!57" — это не только легко запоминается, но и содержит разнообразные символы.
4. **Создайте акроним**: придумайте фразу, которая имеет для вас значение, и используйте первые буквы каждого слова. Например, фраза "Я люблю пить кофе по утрам" может стать "ЯлпкпУ!". Добавьте к этому несколько цифр или символов для надёжности, например, "ЯлпкпУ!2025".
5. **Смешивайте языки**: если вы говорите на нескольких языках, попробуйте смешивать слова из разных языков. Например, "Cat\_собака\_123!" — это комбинация английского и русского, что делает пароль уникальным и запоминающимся.

**Слайд 5: Использование менеджеров паролей**

* **Текст на слайде:** "Менеджеры паролей"
* **Централизованное хранение паролей**
* **Безопасность**
* **Автоматизация ввода паролей**
* **Синхронизация между устройствами**
* **Удобство использования**
* **Защита от фишинга**

**Пример:** Dashlane, BitWarden, Kaspersky Password Manager

**Говорить:**

1. **Централизованное хранение паролей**: все ваши пароли хранятся в одном месте — цифровом хранилище. Для доступа к этому хранилищу используется **мастер-пароль**, который является единственным паролем, который вам нужно запомнить.
2. **Безопасность**: менеджеры паролей обеспечивают высокий уровень безопасности. Они используют шифрование с нулевым разглашением, что означает, что даже разработчики не могут получить доступ к вашим паролям. Многие из них поддерживают двухфакторную аутентификацию для дополнительной защиты.
3. **Автоматизация ввода паролей**: менеджеры паролей могут автоматически заполнять формы входа на сайтах, что упрощает процесс авторизации. Это также помогает избежать использования одинаковых паролей для разных аккаунтов, что повышает безопасность.
4. **Синхронизация между устройствами**: многие менеджеры паролей предлагают возможность синхронизации данных между различными устройствами. Это означает, что, если вы сохраните пароль на одном устройстве, он будет доступен и на других.
5. **Удобство использования**: хороший менеджер паролей должен иметь интуитивно понятный интерфейс, что делает его использование комфортным. Это особенно важно, если у вас много аккаунтов и паролей.
6. **Защита от фишинга**: менеджеры паролей могут помочь вам избежать фишинга, так как они не подставляют логин и пароль на подозрительных сайтах, что позволяет вам заметить, если вы попали на подделку.

**Слайд 6: Важность двухфакторной аутентификации**

* **Текст на слайде:** "Двухфакторная аутентификация (2FA)"
* **Дополнительный уровень защиты**
* **Защита от фишинга**
* **Уменьшение вероятности взлома**
* **Удобство и доступность**

**Говорить:**

1. **Дополнительный уровень защиты**: 2FA требует от пользователя подтверждения своей личности с помощью двух различных факторов. Обычно это что-то, что вы знаете (например, пароль) и что-то, что у вас есть (например, код, отправленный на телефон или сгенерированный приложением). Это делает доступ к вашему аккаунту гораздо более сложным для злоумышленников, даже если они узнали ваш пароль.
2. **Защита от фишинга**: даже если злоумышленник получит ваш пароль через фишинг или другие методы, ему всё равно потребуется второй фактор для доступа к вашему аккаунту. Это значительно снижает риск несанкционированного доступа.
3. **Уменьшение вероятности взлома**: статистически, аккаунты с двухфакторной аутентификацией менее подвержены взломам. Это связано с тем, что злоумышленникам необходимо преодолеть два уровня защиты, что требует больше времени и усилий.
4. **Удобство и доступность**: многие сервисы предлагают простые и удобные методы двухфакторной аутентификации, такие как SMS-коды или приложения для аутентификации. Это делает процесс подтверждения личности быстрым и доступным для большинства пользователей.

**Слайд 7: Заключение**

* **Текст на слайде:** "Заключение"
  + Создание сложных паролей
  + Использование менеджеров паролей
  + Внедрение двухфакторной аутентификации
* **Говорить:** "В заключение, создание сложных паролей, использование менеджеров паролей и внедрение двухфакторной аутентификации — это ключевые шаги для защиты ваших данных. Не забывайте об этих мерах безопасности!"

**Слайд 8: Вопросы и ответы**

* **Говорить:** "Спасибо за внимание!