Guidelines for creating a strong password

Guidelines for creating a strong password

To ensure the security of your account, follow these best practices when creating a password:

1. Length

- Your password must be at least 8 characters long.
- Longer passwords (12+ characters) are even more secure.

2. Complexity

A strong password should include a mix of the following:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (e.g., !, @, #, $, %, ^, &, *)

3. Uncompromised Password

- Avoid using passwords that have been previously exposed in data breaches.
- Use a unique password for each account to prevent security risks.
- You can check if a password has been compromised using publicly available services.

Examples of Strong Passwords

Good Examples:

- P@ssw0rd!23
- G#t3kS!9z@l
- Zy8$Tp&vL3

Weak Examples (Avoid These):

- Password123 (Too common and predictable)
- JohnDoe2024 (Contains personal information)
- abcdefg1 (Lacks complexity)

Additional Security Tips

- Do not reuse passwords across multiple accounts.
- Use a password manager to generate and store complex passwords securely.

By following these guidelines, you can significantly improve the security of your account and protect your personal data.

If you forgot your password

If you forgot your password to your Eskimi DSP account, you can recover it using Forgot password? option in the login page.

Revision #2
Created 11 April 2025 10:50:18
Updated 11 July 2025 14:16:23