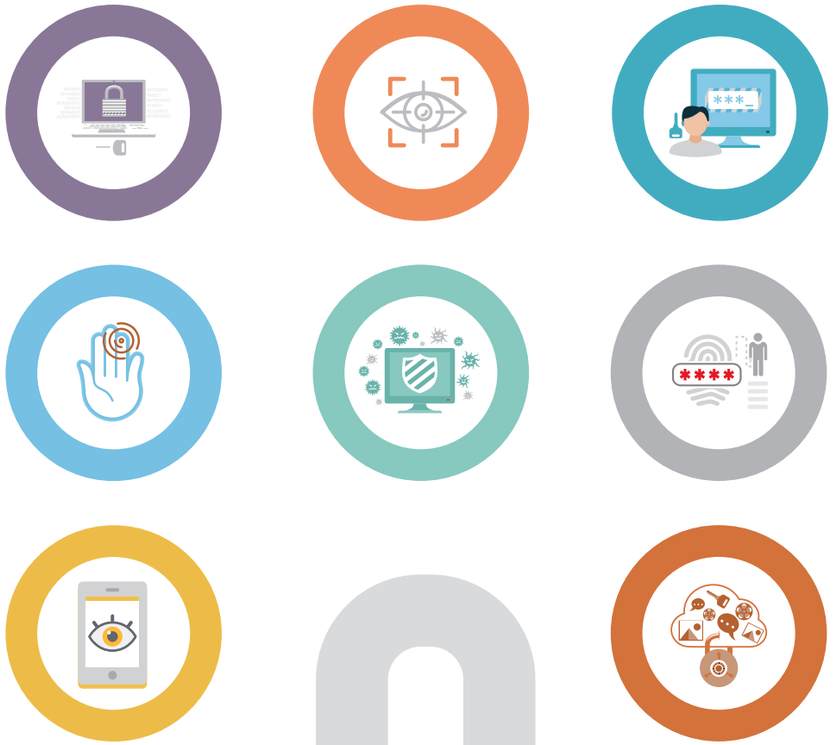
KISA-GD-2018-0033

패스워드 선택 및 이용 안내서



패스워드 선택 및 이용
안내서

과학기술정보통신부
Ministry of Science and ICT

(13809) 경기도 과천시 관문로 47, 5동 과학기술정보통신부
대표전화 : 국번없이 1335 www.msit.go.kr

KISA 한국인터넷진흥원

(58324) 전라남도 나주시 진흥길 9(빛가람동 301-2)
대표전화 : 1544-5118 www.kisa.or.kr

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원

패스워드 선택 및 이용 안내서

Contents

제1장 안전한 패스워드
제2장 이러한 패스워드 사용하지 마세요
제3장 안전한 패스워드 생성 Tip
제4장 패스워드 보안 지침(이용자 측면)
제5장 패스워드 보안 지침(관리자 측면)

01

제 1 장 안전한 패스워드

패스워드란?

이용자가 인터넷 사이트에 로그인 할 때, 허가된 이용자임을 확인하는데 이용되는 문자열입니다. 이용자의 패스워드가 노출되면, 이용자의 개인 메일 정보, 금융정보 등이 타인에게 유출될 수 있습니다. 따라서 이용자는 안전한 패스워드를 설정하고 이용하여야 하며, 또한 안전하게 관리해야 합니다.

안전한 패스워드란?

제3자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 이용자 정보 또는 인터넷을 통해 전송되는 정보를 해킹하여 이용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 말합니다.

두 종류 이상의 문자구성과 8자리 이상의 길이로 구성된 문자열

※ 문자종류는 알파벳 대문자와 소문자, 특수문자, 숫자의 4가지임

또는

10자리 이상의 길이로 구성된 문자열

※ 숫자로만 구성할 경우 취약할 수 있음

02

제 2 장 이러한 패스워드는 사용하지 마세요

패스워드 안전성 체크 리스트

- ✔ **특정 패턴을 갖는 패스워드**
  동일한 문자의 반복
  예) 'aaabbb', '123123'
  키보드 상에서 연속한 위치에 존재하는 문자들의 집합
  예) 'qwerty', 'asdfgh'
  숫자가 제일 앞이나 제일 뒤에 오는 구성의 패스워드
  예) 'security1', '1security'

- ✔ **제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드**
  가족이름, 생일, 주소, 휴대전화번호 등을 포함하는 패스워드

- ✔ **이용자 ID를 이용한 패스워드**
  예) 이용자의 ID가 'KDHong'인 경우, 패스워드를 'KDHong12' 또는 'HongKD'로 설정

- ✔ **한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드**
  예) '바다나라', '천사10', 'love12'

- ✔ **특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드**
  컴퓨터 용어, 사이트, 기업 등의 특정 명칭을 포함하는 패스워드
  유명인, 연예인 등의 이름을 포함하는 패스워드

- ✔ **숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드**
  예) 영문자 'O'를 숫자 '0'으로, 영문자 'I'를 숫자 '1'로 치환

- ✔ **기타**
  시스템에서 초기에 설정되어 있거나 예제로 제시되고 있는 패스워드 한글의 발음을 영문으로, 영문단어의 발음을 한글로 변형한 형태의 패스워드
  예) 한글의 '사랑'을 영어 'SaRang'으로 표기, 영문자 'LOVE'의 발음을 한글 '러브'로 표기

03

제 3 장 안전한 패스워드 생성 Tip

기억하기 쉬운 패스워드 설정방법

✔ 특정명칭을 선택하여 예측이 어렵도록 가공하여 패스워드 설정

특정명칭의 홀·짝수 번째의 문자를 구분하는 등의 가공방법을 통해 설정
국내 이용자는 한글 자판을 기준으로 특정명칭을 선택하고 가공하여 설정

예) '한국인터넷진흥원'의 경우, 홀수 번째 '한인넷흥'이 'gksdlssptgmd'로, 짝수 번째 '국터진원'이 'rnrxjwlsdnjs'로 사용

✔ 노래 제목이나 명언, 속담, 가훈 등을 이용·가공하여 패스워드 설정

※ 영문사용의 경우, 'This May Be One Way To Remember'를 'TmB1w2R'이나 'Tmb1w>r~'로 활용

※ 한글사용의 경우, '백설공주와 일곱 난쟁이'를 '백설+7난장'로 구성하고 'QorTjf+7SksWkd'등으로 활용

예측이 어려운 문자구성의 패스워드 설정방법

✔ 영문자(대·소문자), 숫자, 특수문자들을 혼합한 구성으로 패스워드 설정

예) '10H+20Min', 'I!Can&9it' 등과 같은 구성

✔ 패스워드의 길이를 증가시키기 위해서는 알파벳 문자 앞뒤가 아닌 위치에 특수문자 및 숫자 등을 삽입하여 설정

예) 'Security1'이 아니라 'Securi2t&&y'와 같은 형태로 패스워드의 길이를 늘림

✔ 알파벳 대·소문자를 구별할 수 있을 경우, 대·소문자를 혼합하여 설정

특정위치의 문자를 대문자로 변경하거나, 모음만을 대문자로 변경

예) 'gkswjdqhwlsdnjs'→'gKsWjDqHwLsDnJs', 'rnrqhghgmd'→'rNrQhGhGmD'

사이트별 상이한 패스워드 설정을 위한 방법

✔ 자신의 기본 패스워드 문자열을 설정하고 사이트별로 특정 규칙을 적용하여 패스워드 설정

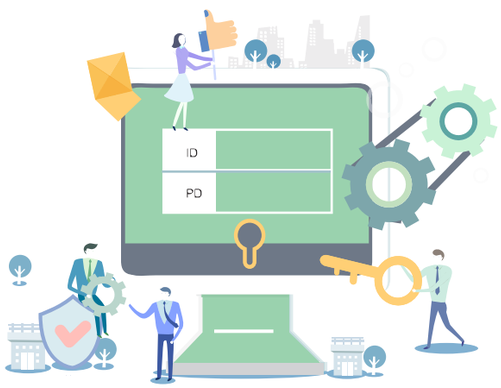
예) 패스워드 문자열을 '486*+'로 설정하고, 사이트 이름의 짝수 번째 문자 추가를 규칙으로 yahoo.com는 '486*+ao.o', google.co.kr는 '486*+ogec.r'등으로 활용

04

제 4 장 패스워드 보안 지침

(이용자 측면)

- 이용자는 제 3 장을 참고하여 안전한 패스워드를 설정하여 사용해야 합니다
- 초기 패스워드가 시스템에 의해 할당되는 경우, 이용자는 빠른 시간 내에 해당 패스워드를 새로운 패스워드로 변경해야 합니다
- 패스워드 변경 시, 이전에 사용하지 않은 새로운 패스워드를 사용하고 변경된 패스워드는 이전 패스워드와 연관성이 없어야 합니다
- 자신의 패스워드가 제3자에게 노출되지 않도록 해야 합니다
- 자신의 패스워드가 제3자에게 노출되었을 경우, 즉시 새로운 패스워드로 변경해야 합니다
- 여러 계정이나 시스템에서 동일한 패스워드를 사용하지 않도록 해야 합니다



05

제 5 장 패스워드 보안 지침

(관리자 측면)

- 이용자가 안전한 패스워드를 선택할 수 있도록 제 3 장을 참고하여 패스워드 선택 기준을 안내해야 합니다
- 초기 패스워드, 패스워드 분실 등의 이유로 이용자에게 제공하기 위해 생성된 패스워드는 최소 6자 이상이어야 하며 안전하게 생성된 난수여야 합니다
- 패스워드를 최소 8자 이상으로 요구해야 하며, 영문, 숫자, 특수 기호를 조합하여 사용할 수 있도록 허용해야 합니다
- 반복적으로 잘못된 패스워드를 입력할 경우, 입력 횟수를 제한하는 시스템을 구현해야 합니다
- 이용자가 패스워드를 변경하고자 할 때 관리자는 패스워드가 안전한지 확인하여 이용자에게 알리고 안전하지 않을 경우 다른 값을 요구하는 시스템을 구현해야 합니다
- 패스워드는 여러 번의 일방향 해시함수를 사용하고 패스워드와 함께 사용하는 솔트(Salt)는 안전하게 저장하여야 합니다