**[패스워드 관리 안내]**

1. **안전한 패스워드란?** 제 3 자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 사용자 정보 또는 인터넷을 통해 전송되는 정보를 해킹하여 사용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 말합니다.
   가. 세가지 종류 이상의 문자 구성으로 10 자리 이상의 길이로 구성된 문자열
   ※ 문자 종류는 알파벳 대문자와 소문자, 특수문자, 숫자의 4 가지임

**2. 패스워드 안전성 체크 리스트 – ,이러한 패스워드는 사용하지 마세요‘**

   가. 7 자리 이하 또는 두가지 종류 이하의 문자구성으로 8 자리 이하 패스워드
   나. 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‘

   다. 제 3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드
   라. 가족 이름, 생일, 주소, 휴대전화번호 등을 포함하는 패스워드
   마. 사용자 ID를 이용한 패스워드
   - 예) 사용자의 ID가‘KDHong‘인 경우, 패스워드를‘KDHong12‘또는‘HongKD‘로 설정

   바. 한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드
   - 예)‘ 바다나라‘,‘ 천사10‘,‘ love12‘

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

**3. 안전한 패스워드 생성 TIPS**

   가. 특정 명칭을 선택하여 예측이 어렵도록 가공하여 패스워드 설정
   - 특정 명칭의 홀·짝수 번째의 문자를 구분하는 등의 가공방법을 통해 설정
   - 국내 사용자는 한글 자판을 기준으로 특정 명칭을 선택하고 가공하여 설정

   ※ 예) ‘한국정보보호진흥원‘의 경우, 홀수 번째‘한정보진원‘이‘gkswjdqhwlsdnjs‘로, 짝수 번째‘국보호흥‘이 ‘rnrqhghgmd‘로 사용

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

   ※ 영문 사용의 경우,‘ This May Be One Way To Remember‘를‘TmB1w2R‘이나‘Tmb1w>r~‘로 활용
   ※ 한글 사용의 경우,‘ 백설공주와 일곱 난쟁이‘를‘백설+7 난장‘로 구성하고‘QorTjf+7SksWkd‘등으로 활용

**4. 패스워드 보안 지침**

   가. 사용자는 안전한 패스워드를 설정하여 사용해야 합니다.
   나. 초기 패스워드가 시스템에 의해 할당되는 경우, 사용자는 빠른 시간 내에 해당 패스워드를 새로운 패스워드로 변경해야 합니다.
   다. 사용자는 패스워드를 주기적으로 변경해야 하며, 권장하는 패스워드 변경 주기는 3 개월입니다.
   라. 패스워드 변경 시, 이전에 사용하지 않은 새로운 패스워드를 사용하고 변경된 패스워드는 이전 패스워드와 연관성이 없어야 합니다.
   마. 자신의 패스워드가 제 3 자에게 노출되지 않도록 해야 합니다.
   바. 패스워드를 메모지 등에 기록할 경우, 메모지는 항상 자신이 소유하고 있거나 안전한 장소에 보관함으로써 외부로 노출되지 않도록 해야 합니다.
   사. 제 3 자에게 자신의 패스워드와 관련된 정보 및 힌트를 제공하지 않아야 합니다.
   아. 자신의 패스워드가 제 3 자에게 노출되었을 경우, 즉시 새로운 패스워드로 변경해야 합니다.

   ※ 출처: KISA, 패스워드 선택 및 이용 가이드

**[해킹방지 안내]**

1. **피싱이란?** 인터넷을 통해 국내의 유명 기관을 사칭하여 개인정보나 금융정보를 수집한 뒤 이를 악용하여 금전적인 이익을 노리는 신종 사기의 일종 입니다.

**2. 피싱의 위험성**

가. 피싱은 금전적 이익을 주목적으로 하기 때문에, 직접적으로 의도하지 않은 계약 신청 등의 피해가 발생할 수 있습니다.

나. 간접적인 피해로는 광고성 전화 및 스팸메일 수신, 명의 도용 등이 있습니다.

**3. 피싱 유형**

가. 유명 기관을 사칭하여 메일을 발송하고, 메일 본문의 인터넷 주소로 접속해 개인정보를 입력하도록 하는 방법

나. 경품 이벤트나 신용 대출, 게임 아이템 충전 등을 미끼로 대형 포탈 게시판에 광고 글을 게시하거나 쪽지를 보내는 방법 등

**4. 피싱 예방법**

가. 이용자 개인이 피싱 메일이나 사기성 이벤트 등에 현혹되어 개인 정보를 제공하는 일이 없도록 주의해야 합니다.

- 메일이나 게시판에 연결된 사이트에 개인정보 입력 주의
- 무분별한 인터넷 이벤트 참여 금지
- 금융거래 사이트는 인터넷 주소를 직접 입력하여 접속 또는 검색엔진(네이버, 다음)으로 조회하여 사용
- 비밀번호를 주기적으로 변경

나. 이용자 PC 의 윈도우 업데이트와 백신 프로그램이 필수이며, 안전한 인터넷 이용 습관을 생활화 해야 합니다.

- 윈도우 자동 보안 업데이트 설정
- PC 보안상태 점검: 정보보호 포털사이트 ‚보호나라‘ 홈페이지 방문 후 PC 원격 점검 서비스 이용
- 백신 프로그램 실시간 구동 및 주기적인 점검
- 신뢰할 수 있는 사이트에서만 파일 다운로드 (e.g. 메일 첨부파일, 인터넷 공개자료실, 파일공유 등을 통한 자료 다운로드 금지)

다. 피싱 등 해킹 사고 의심 시 관련 기관으로 신고해 주세요.

- 폭스바겐파이낸셜서비스코리아: 02-513-3100
- 경찰청 사이버테러 대응센터: 경찰민원 콜센터 182, https://www.cyberbureau.police.go.kr
- 금융감독원 전자 민원 창구: 1332 (국번없이), https://www.fcsr.kr

출처: KISA, 개인 사용자를 위한 피싱 예방 가이드