



중소기업 기술 유출 방지
IT 보안

가이드라인

임직원 편



국가정보원



중소벤처기업부

중소기업 기술 유출 방지 IT 보안 가이드라인



2023.12

들어가며

2023년 기준, 대한민국의 중소기업은 국내 전체 기업의 99.9%를 차지하며 우리 경제 전반을 책임지고 있습니다. 하지만 많은 중소기업이 정보보호에 투자할 재정적 여유가 부족해 보안 시스템을 갖추지 못하고 있거나, 보안 책임자가 부재한 상황에 놓여 있습니다.

「중소기업 기술 유출 방지 IT 보안 가이드라인」은 이처럼 보안 사각지대에 있는 중소기업을 위해 작성되었습니다. 정보보호 전문가가 부족한 중소기업의 현실을 고려하여 업무상 많이 활용되는 IT장비의 보안 설정에 대해 쉽고 자세히 설명하고자 노력하였습니다. 중소기업에서 많이 사용하는 제품을 위주로 작성하였고, 추가 비용 없이 따라할 수 있는 기본적인 내용을 담았습니다.

해킹에 의한 기술 유출은 매년 증가하고 있습니다. 중소기업도 예외는 아니며, 그렇기 때문에 이제 보안은 선택이 아닌 필수라고 할 수 있습니다. 앞으로 중소기업은 임직원들에게 안전한 근무 환경을 제공하면서 해킹을 통한 기술 유출을 예방해야 할 것입니다.

본 가이드라인을 통해 모든 중소기업의 정보보안 역량이 향상되기를 희망합니다.



목차

제1장	가이드라인 개요	
Ⅰ.	가이드라인 작성 배경	05
Ⅱ.	가이드라인 구성	06
Ⅲ.	가이드라인의 기대 효과	09

제2장	임직원 보안수칙	
Ⅰ.	PC	11
	1. 시스템	13
	2. 웹 브라우저	25
	3. 이메일	61
	4. 오피스	78
	5. 메신저	93
Ⅱ.	저장매체	98
	1. 시스템	100
	2. 시중 소프트웨어	106
Ⅲ.	모바일	112
	1. 운영체제	116

제3장	침해사고 발생 시 대처 방법	
Ⅰ.	침해사고 대응하기	122
Ⅱ.	유관기관 알라두기	126



1

가이드라인 개요

제1장은 「가이드라인 개요」로 본 가이드라인에 대하여 전체적으로 소개합니다. 가이드라인의 작성 배경과 이를 통해 얻고자 하는 기대 효과에 대하여 서술하며, 가이드라인의 구성을 설명하여 이를 어떻게 활용하면 좋을지 안내합니다.

가이드라인 작성 배경

한국인터넷진흥원에 따르면 민간 분야에 대한 사이버 침해 신고는 최근 5년간 계속 증가하고 있습니다. 2019년 418건이었던 신고건수는 매년 증가하여 2022년에는 1,142건이 집계되었고, 올해 2023년에는 상반기에만 890건이 집계되어 관련 피해가 상당할 것으로 예상됩니다.

기업을 향한 해킹 공격은 대부분 산업기술을 탈취하려는 목적으로 일어나고 있습니다. 21세기 글로벌 경쟁시대에 산업기술은 기업과 국가 경쟁력을 좌우하는 핵심 요소로 작용하고 있으며, 산업기술 유출은 피해 기업은 물론 국가경쟁력까지 훼손할 수 있습니다.

현재 사이버 침해사고로 인한 피해는 대부분 중소기업에 집중되어 있습니다. 그 이유는 다수의 중소기업이 정보보안 전문 인력과 관련 예산을 갖추지 못한 경우가 많기 때문입니다. 이는 우리 중소기업이 해킹을 통한 산업기술 유출에 매우 취약한 상태임을 의미합니다.

해킹에 의한 산업기술 유출 위협으로부터 우리 중소기업을 지키고, 국내산업의 경쟁력을 강화하기 위해서는 기술 보호에 대한 국가적·국민적 관심이 절실히 필요합니다. 본 가이드라인은 이러한 문제의식 속에서 작성되었습니다. 중소기업이 보안에 투자할 재정적 여력이 부족하다는 점에 중점을 두어, 별도의 비용 없이 기존에 사용하고 있는 IT 장비에 대한 보안 설정 방법에 대하여 안내합니다. 본 가이드라인을 통해 중소기업 내 IT 인프라 보안 역량이 향상되기를 기원합니다.

2023년 12월
산업기밀보호센터

가이드라인 구성

01. 내용 구성

행동 수칙

「행동 수칙」은 업무 중 IT 장비를 다룸에 있어서 알아 두어야 할 일반적인 행동 지침을 포스터로 설명하고 있습니다. 기술적인 내용보다는 사용자의 행동에 초점을 두어, 업무를 수행하면서 기억하면 좋을 기본적인 보안 수칙 위주로 작성되었습니다. 이를 출력하여 배부하거나, 보기 좋은 곳에 게시하여 기업 임직원에게 지속적으로 노출한다면 모든 구성원의 보안 인식 향상에 도움이 될 것입니다.



가이드라인 구성

설정 방안

「설정 방안」은 IT 제품에 대한 설명과 함께, 개별적인 장비에서 할 수 있는 보안 설정 방법을 상세하게 안내합니다. 해당 제품에 대한 기술적인 지식이 없는 사람도 바로 따라 할 수 있도록 실제 화면을 담았고, 설정 방법 또한 자세하게 서술하였습니다.

우선 목차를 통해 기업 내에서 사용하고 있는 IT 장비를 찾아, 해당 부분에서 다루는 설정을 모두 적용하기를 권장합니다. 설정 방안에서 제시하는 보안 설정은 필수적이고 기본적인 조치입니다. 제품이 기본적으로 제공하는 보안 기능을 최대한 활용하여 발생할 수 있는 보안 문제를 기술적으로 예방할 수 있게 하고자 하였습니다.



가이드라인 구성

가이드라인 구성 예시

중분류명
제품군명

대분류
I II III IV
제품군명

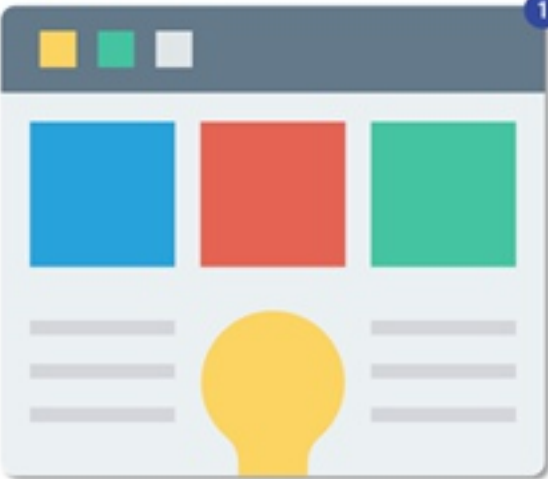
제품명

1. 해당 제품에서 할 수 있는 보안 설정

각 보안 설정의 구체적인 설정 방법을 안내하기 전, 해당 설정의 개념과 필요성에 대하여 설명합니다.

세부적인 보안 설정 방법

1 [●●●● 검색 및 실행] > [●●●● 설정 또는 해제] > [●●●● 사용 확인]
※ 세부 설정 절차를 자세하게 설명합니다.



※ 실제 화면을 담은 사진을 제시하여 쉽게 따라할 수 있도록 구성했습니다.

TIP
이 '상자'를 통해서 추가적인 보안 설정 방법이나 알아두면 좋은 IT 또는 보안 지식을 안내합니다.

사람들은 일반적으로 해킹 사고를 막기 위해 고가의 장비나 전문적인 도움이 필요하다고 인식하며, 정보보호는 나와 관련 없는 일이라 생각합니다. 하지만 알려진 것 이상으로 침해사고는 주변에서 빈번하게 일어나고 있으며, 이는 기본적인 보안조치 만으로도 충분히 예방이 가능합니다.

본 가이드라인은 별도의 보안 장비나 전문 인력 없이 누구나 따라할 수 있는 내용들로 구성되어 있습니다. 가이드라인을 통해 기업의 보안 수준을 빠르게 끌어올릴 수 있기를 희망하며, 정보보호의 중요성에 대한 인식이 널리 퍼지기를 기대합니다.



2

임직원 보안수칙

제2장은 「임직원 보안수칙」으로 기업 내 직책과 상관없이 모든 임직원이 수행해야 할 사항에 대해 다룹니다. PC, 저장매체, 모바일과 같이 업무상 일반적으로 사용하는 IT 제품에 대한 보안수칙과 설정방법에 대하여 설명합니다. 본 장에서 권장하는 사항을 준수해 기업 사무환경의 전체적인 보안수준을 높여야 합니다

제2장 임직원 보안수칙

I. PC



i. 시스템 ... 12

1. Windows 10/11 ... 14

ii. 웹 브라우저 ... 25

1. 구글 크롬 ... 27
2. 마이크로소프트 엣지 ... 40
3. 네이버 웨일 ... 51

iii. 이메일 ... 61

iv. 오피스 ... 78

1. Word 2021 ... 80
2. Excel 2021 ... 81
3. PowerPoint 2021 ... 84
4. 한글 2022 ... 88
5. 한셀 2022 ... 90
6. 한쇼 2022 ... 92

v. 메신저 ... 93

1. 카카오톡 ... 94



이것만은 지키자!

행동수칙

공통 편

1



비밀번호를 주기적으로 변경해요!

공격자의 공격(무차별 대입 공격, 사전 공격 등)에 의해 비밀번호가 노출될 수 있으므로, 비밀번호를 주기적으로 변경하여 사이버 침해사고를 예방하여야 합니다.

2



소프트웨어를 주기적으로 업데이트해요!

매체를 막론하고 업데이트는 벤더사가 제공하는 가장 저렴하고 효과적인 보안 수단입니다. 서버의 부하가 적은 시간대를 활용하여 정기적인 업데이트 일정을 설정하여 업데이트를 진행해야 합니다.

이번 편에서는 PC 사용의 기반이 되는 운영체제의 시스템 보안 설정에 대해 안내합니다. 대표적으로 가장 많이 이용하는 PC 운영 체제인 'Windows 10/11' 의 시스템 보안 설정을 자세하게 다룹니다.



☑ 시스템이란 무엇인가요?

시스템이란 목표를 달성하기 위해 서로 영향을 주고받는 구성 요소들의 모임입니다. 특히 컴퓨터에서 '시스템'은 사용자와 컴퓨터 사이에서 서로의 말을 번역해주는 통역사의 역할을 합니다.

☑ 시스템 보안을 왜 해야 할까요?

회사 PC에서는 회사 영업 정보나 고객 개인 정보와 같은 중요한 영업 데이터를 다룹니다. 그렇기 때문에 이를 노리는 불법적인 외부 침입자, 바이러스, 악의적인 내부자 등 다양한 위협으로부터 시스템을 보호해야 합니다.

가이드라인에서 다루는 제품 확인하기



Windows 10

▲ Windows 10



Windows 11

▲ Windows 11

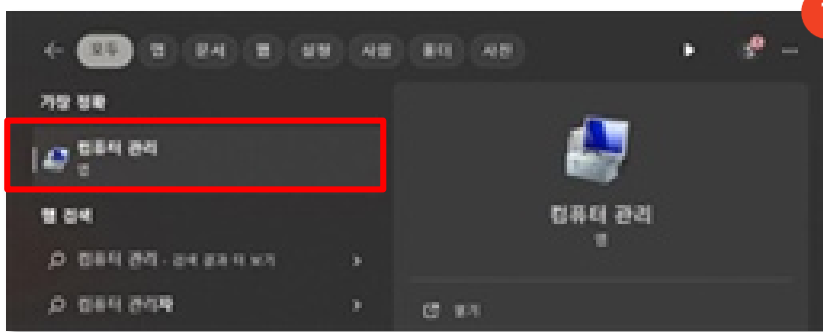
Windows 10/11

1. 안전한 비밀번호 정책 설정하기

안전하지 않은 비밀번호를 사용하면 공격자가 PC에 침입할 확률이 높아집니다. 잘못된 비밀번호 사용의 예시로는 패스워드를 변경하지 않고 오랫동안 사용하거나, 이전에 사용하던 패스워드를 재사용하거나, 복잡하지 않은 패스워드를 사용하는 것이 있습니다. 안전한 비밀번호를 사용하도록 정책을 설정하여 시스템의 보안을 강화할 수 있습니다.

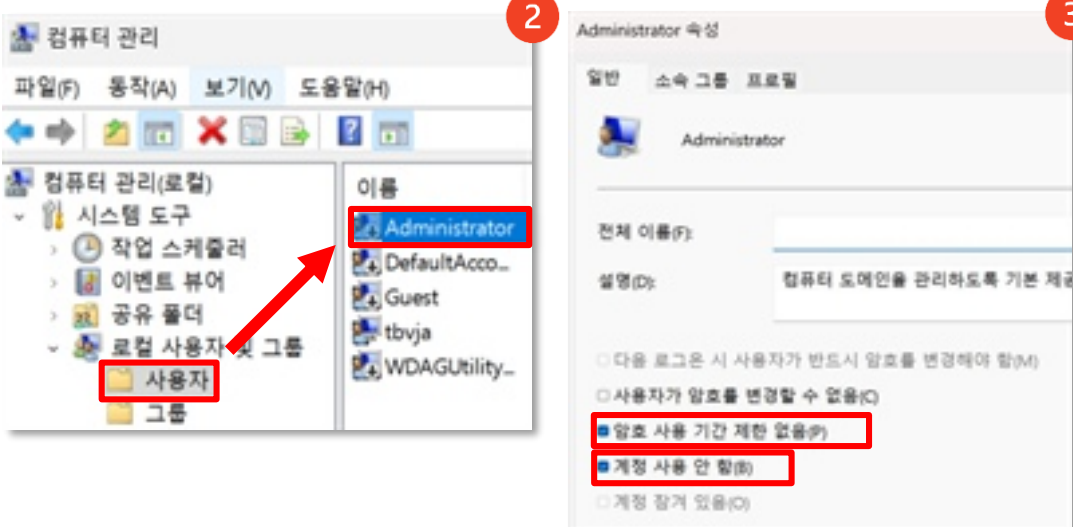
계정 환경 설정하기

1. ['컴퓨터 관리' 검색 및 클릭]



2. [로컬 사용자 및 그룹] > [사용자] > ['Administrator' 클릭]

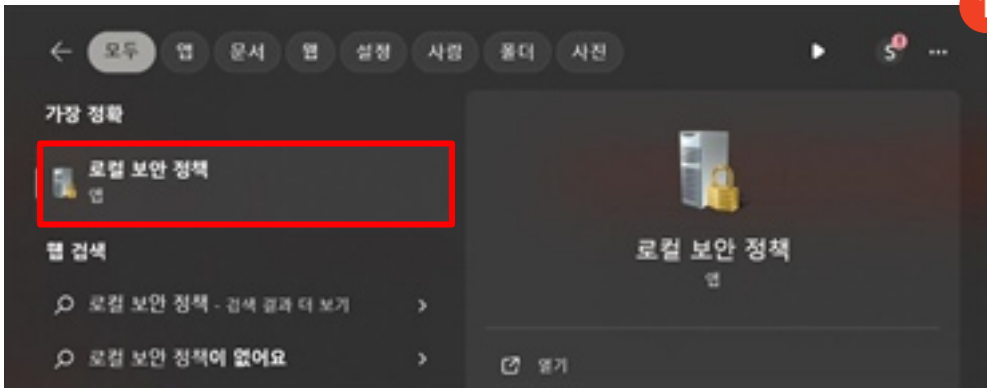
3. [Administrator 속성] > [일반] > ['암호 사용 기간 제한 없음/계정 사용 안 함' 체크 박스 선택 해제]



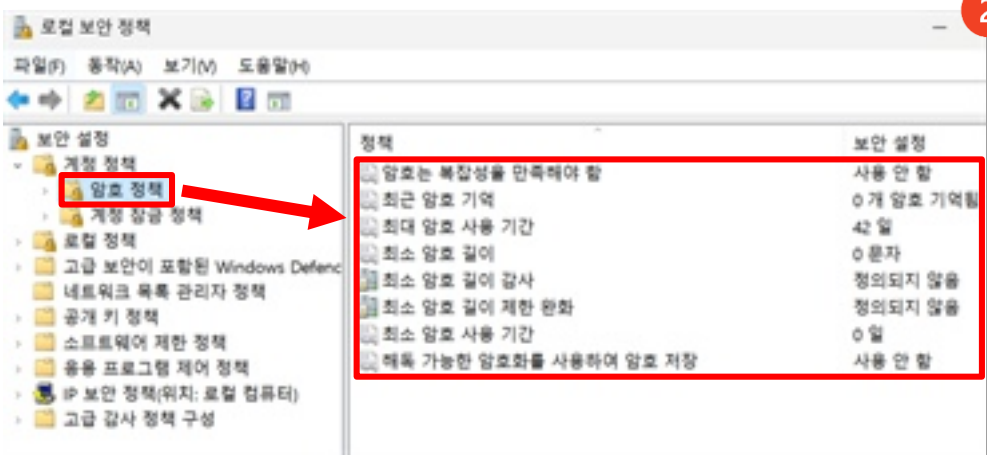
Windows 10/11

계정 비밀번호 정책 설정하기

1 ['로컬 보안 정책' 검색 및 클릭]



2 [보안 설정] > [계정 정책] > [암호 정책] > [하단 표 참고해 암호 정책 설정]



권장하는 규칙

설정 항목	안전한 값	상세 설명
암호 복잡성 설정	활성화	영문, 숫자, 특수문자 중 2종류와 10자리 이상 조합, 또는 3종류 이상 최소 8자리 이상 조합을 사용하게 하는 설정
최근 암호 기억 속성	24개 이상	기존에 사용했던 비밀번호를 재사용하지 못하게 하는 설정
최대 암호 사용 기간	90일 미만	같은 비밀번호를 변경없이 사용할 수 있는 최대 기간 설정
최소 암호 사용 기간	1일 이상	비밀번호 변경 후 다시 변경할 수 있는 간격을 두게 하는 설정
최소 암호 길이 설정	8자 이상	비밀번호의 최소 길이 조건을 두는 설정

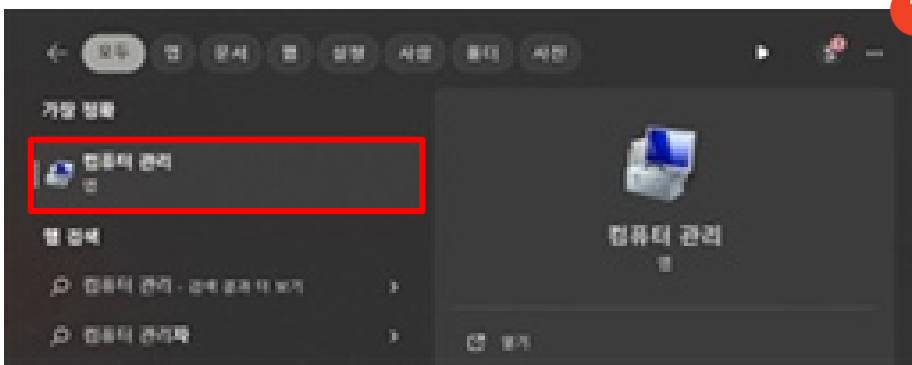
Windows 10/11

2. 공유 폴더 관리하기

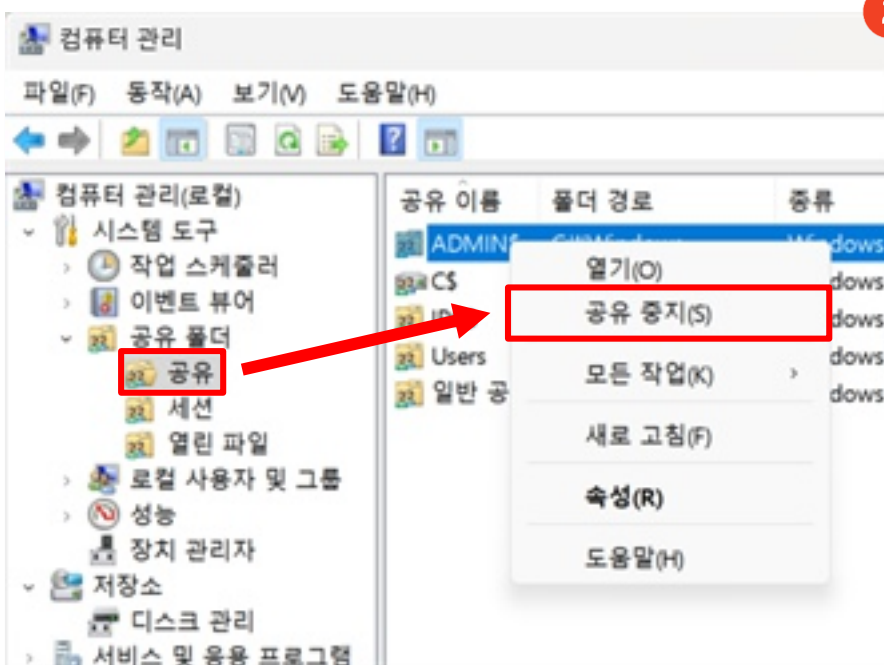
공유 폴더를 통해 다른 사람이 내 PC에 접근할 수 있기 때문에 사용하지 않는 공유 폴더는 해제하여야 하며, 불가피하게 공유폴더를 사용하고 있다면 허가 받은 사용자만이 접근할 수 있도록 암호를 설정하여야 합니다. 이렇게 함으로써 PC에 대한 무단 접근과 데이터 유출의 위험을 줄일 수 있습니다.

1. C\$, D\$, Admin\$ 등의 기본 공유 폴더 및 불필요한 공유 폴더 공유 중지하기

1. ['컴퓨터 관리'] 검색 및 클릭



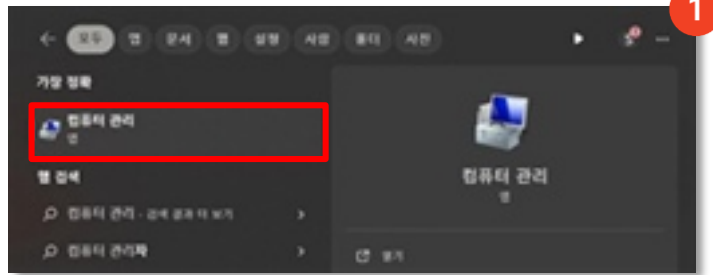
2. [시스템 도구] > [공유 폴더] > [공유] > ['공유 중지할 폴더' 우클릭] > ['공유 중지' 클릭]



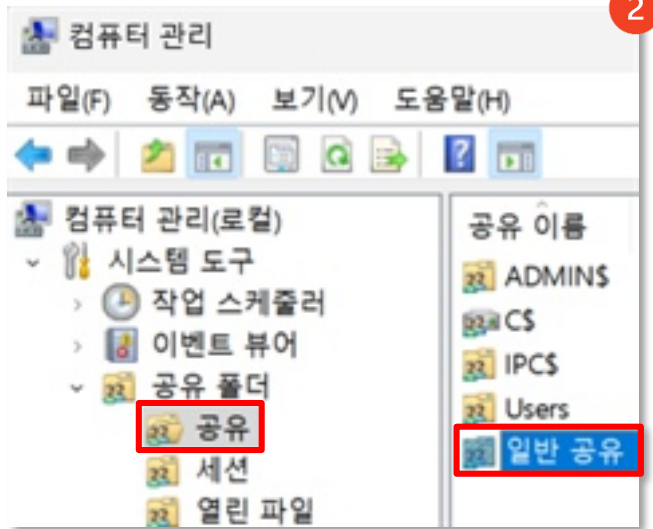
Windows 10/11

일반 공유 폴더 권한 설정하기

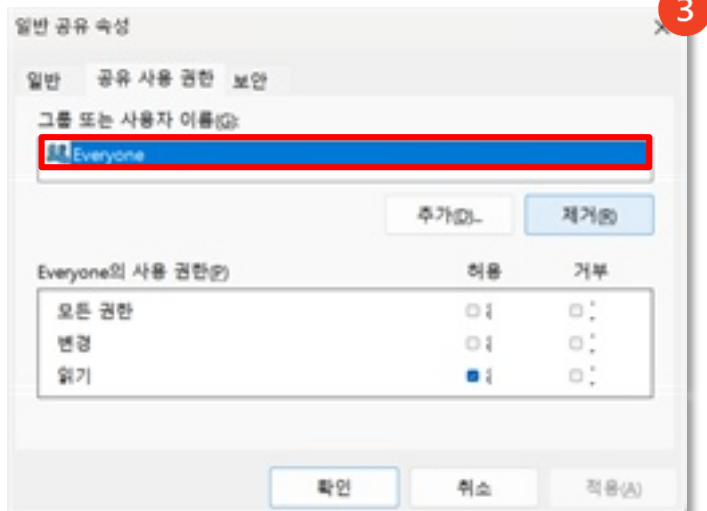
- 1 [컴퓨터 관리] 검색 및 클릭



- 2 [시스템 도구] > [공유 폴더] > [공유] > [권한 설정이 필요한 공유 폴더 우클릭 후 '속성' 클릭]



- 3 [공유 사용 권한] > [Everyone 제거]



Windows 10/11

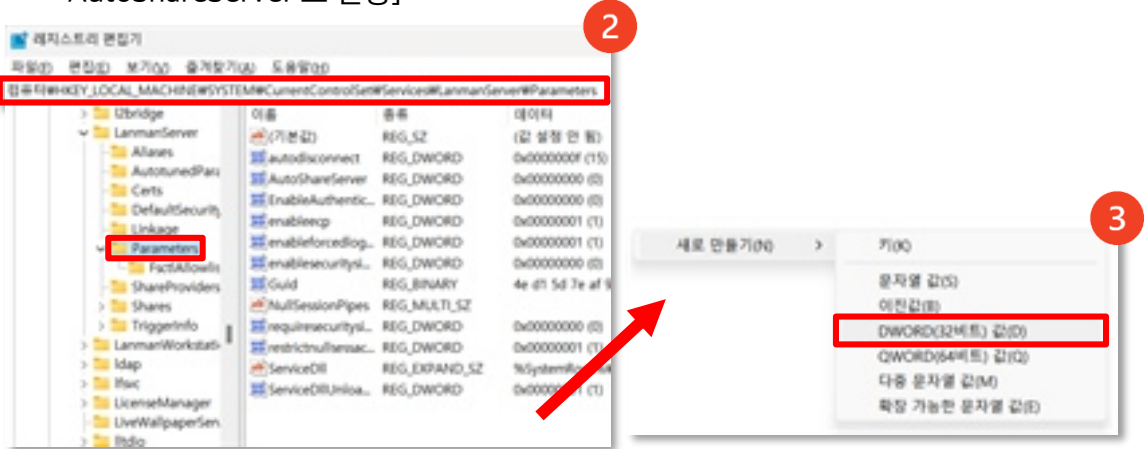
기본 공유 폴더가 자동으로 공유되는 것을 방지하기

- 1 [레지스트리 편집기] 검색 및 클릭

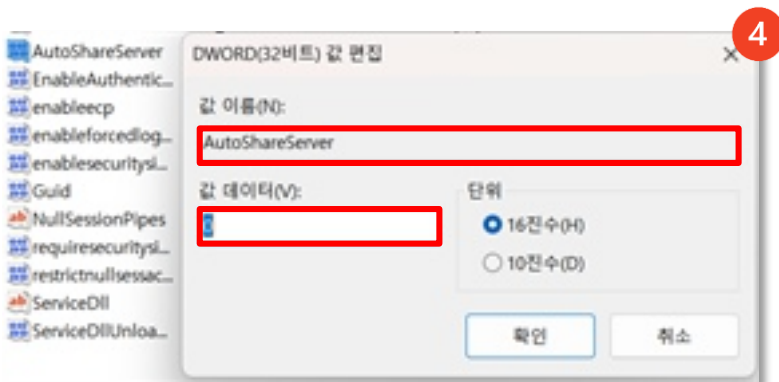


- 2 [컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters] 이동

- 3 [마우스 우클릭 후 '새로 만들기'] > ['DWORD(32비트) 값'] 클릭 > [새 파일 이름 'AutoShareServer'로 변경]



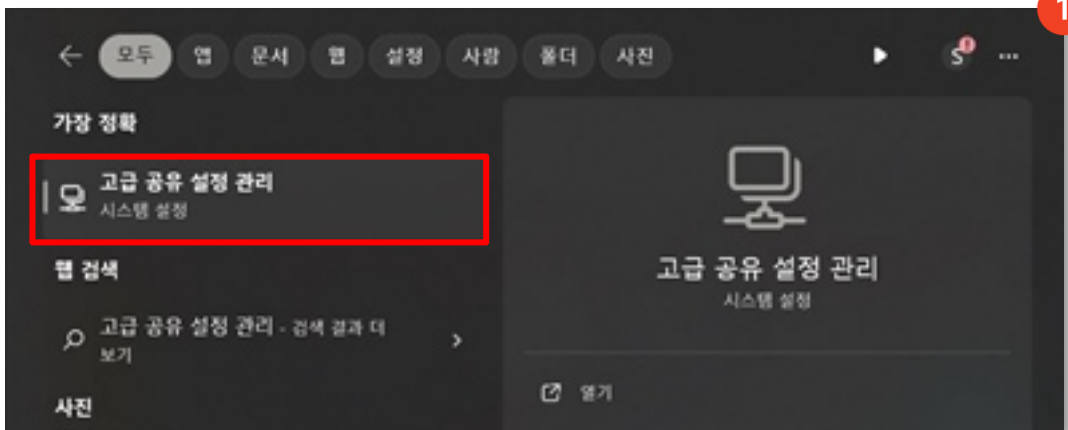
- 4 ['AutoShareServer'] 파일 값을 '0'으로 변경



Windows 10/11

공유 폴더 접근 시 비밀번호 설정하기

- 1 ['고급 공유 설정 관리' 검색 및 클릭]



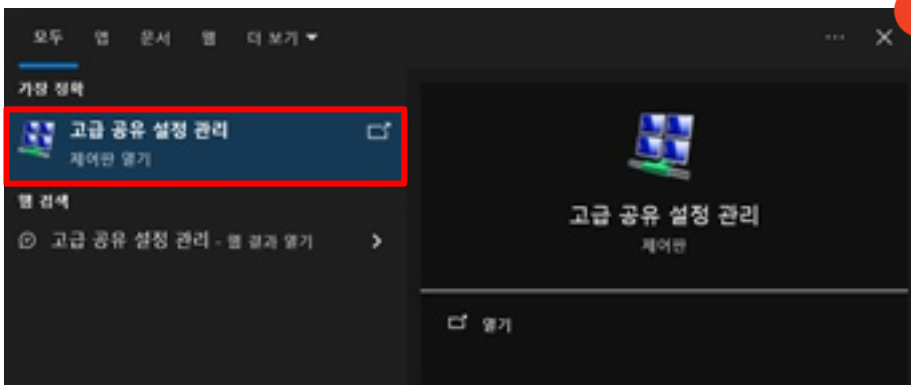
- 2 ['암호로 보호된 공유' 활성화]



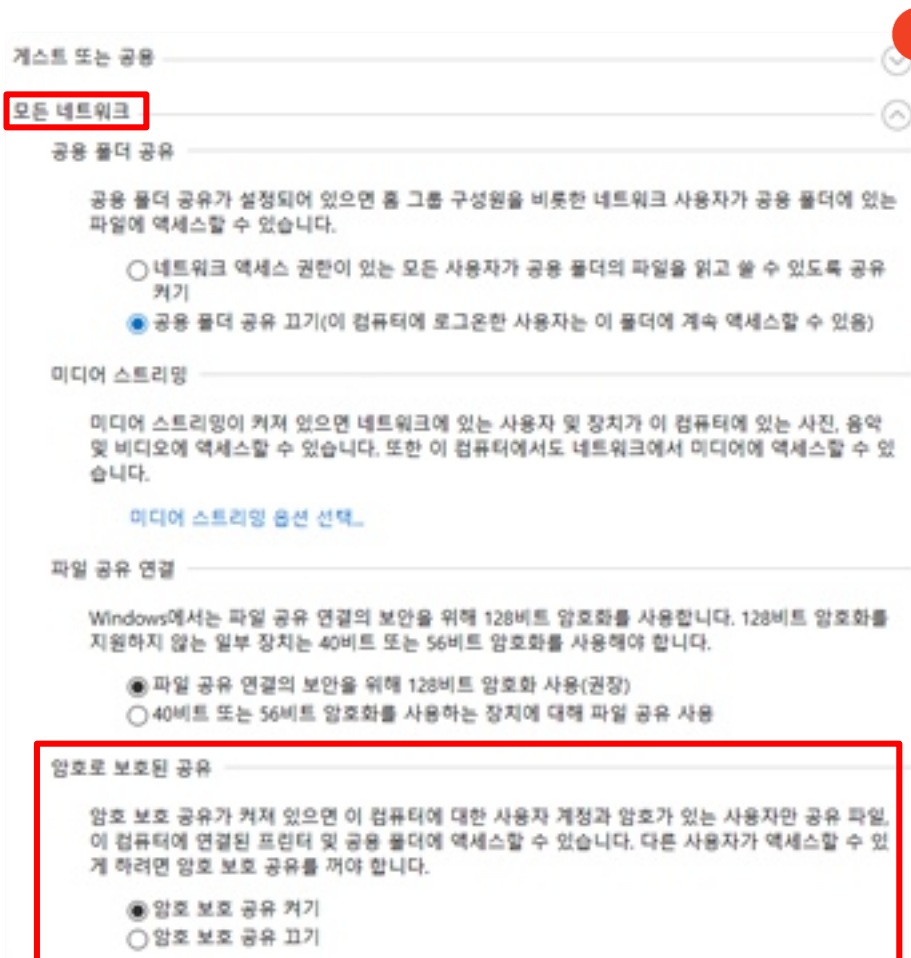
Windows 10/11

공유 폴더 접근 시 비밀번호 설정하기 (Windows 10 Ver.)

1 ['고급 공유 설정 관리' 검색 및 클릭]



2 ['암호로 보호된 공유 켜기' 선택]



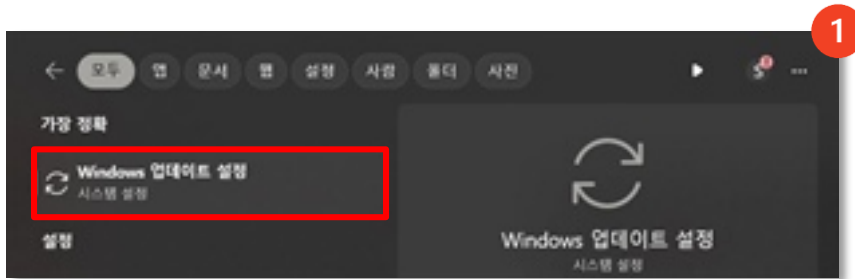
Windows 10/11

3. 최신 보안 업데이트 적용하기

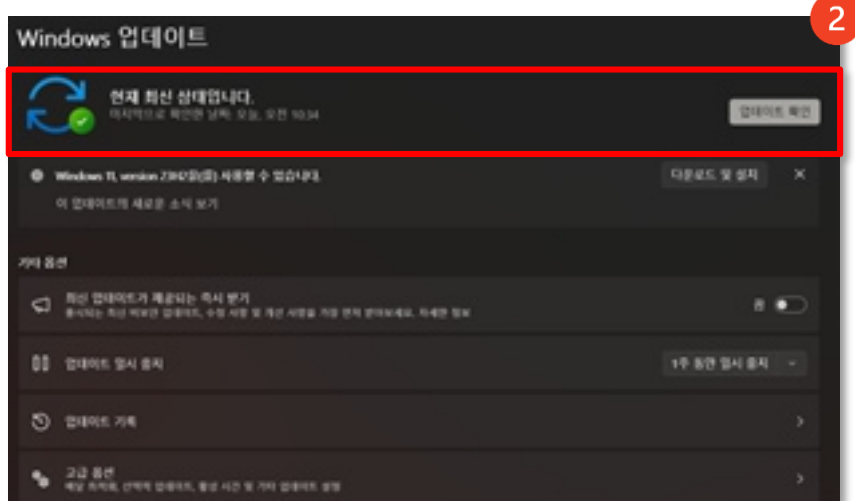
최신 보안 업데이트를 적용하지 않으면 시스템이 알려진 취약점에 대응할 수 없기 때문에, 공격자가 쉽게 침투해 데이터를 유출할 수 있습니다. 이를 막기 위해 윈도우 운영체제는 항상 최신 버전으로 유지하여야 합니다.

최신 보안 업데이트 적용하기

- 1 ['Windows 업데이트 설정' 검색 및 클릭]



- 2 [최신 업데이트 존재 여부 확인] > [다운로드 및 업데이트 적용]



보안 업데이트의 필요성

최신 보안 업데이트를 적용하지 않아 발생하는 침해사고들이 계속 증가하고 있습니다. 대표적인 예시로, 2014년에 발생한 '하트블리드' 사태와, 2017년에 발생한 '워너크라이' 사태가 있습니다. 이는 모두 배포된 보안 업데이트를 적용하지 않아 피해가 발생한 사례들입니다.

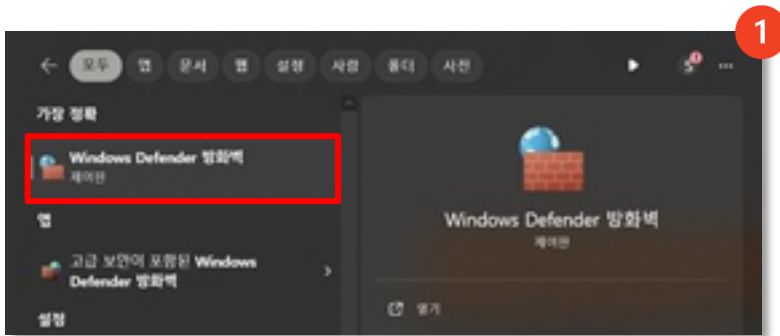
Windows 10/11

4. 침입 차단 기능 활성화하기

Windows 방화벽은 데이터를 지키고 악성 코드 감염을 막는 핵심적인 역할을 합니다. 이 기능을 사용하지 않으면 PC에 저장된 회사의 데이터가 위험에 노출될 수 있고, 악성 코드로 인한 시스템 성능 저하 및 서비스 중단 등의 문제가 발생할 수 있습니다. 따라서 방화벽의 침입 차단 기능은 항상 활성화되어 있어야 합니다.

Windows 방화벽 기능 활성화하기

- 1 ['Windows Defender 방화벽' 검색 및 클릭]



- 2 ['Windows Defender 방화벽 설정 또는 해제' 클릭]

- 3 [Windows Defender 방화벽 사용 확인]



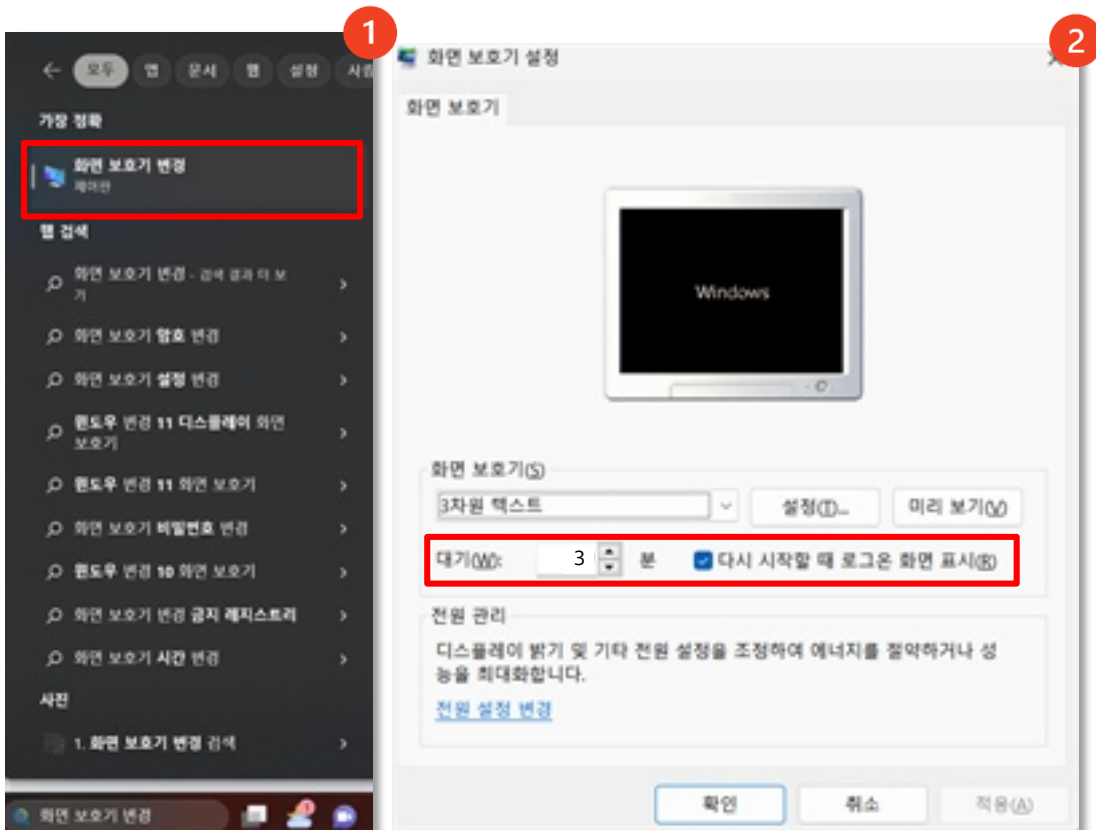
Windows 10/11

5. 화면보호기 설정하기

PC 화면을 그대로 켜 둔 채 자리를 비우면 누군가가 내 PC에 접근하여 회사 기밀정보를 빼가거나 악성프로그램을 설치할 수 있습니다. 이때 화면보호기 기능을 사용하면 이러한 위험을 막을 수 있습니다. 화면보호기는 일정 시간 PC 사용이 없을 시 모니터의 화면을 가려주는 기능입니다. 아래에는 화면보호기를 설정하는 방법을 설명합니다.

화면 보호기 설정하는 방법

- 1 [화면 보호기 변경' 검색 및 클릭]
- 2 [대기 시간'을 3~5분 사이로 입력] > [다시 시작할 때 로그인 화면 표시' 선택]



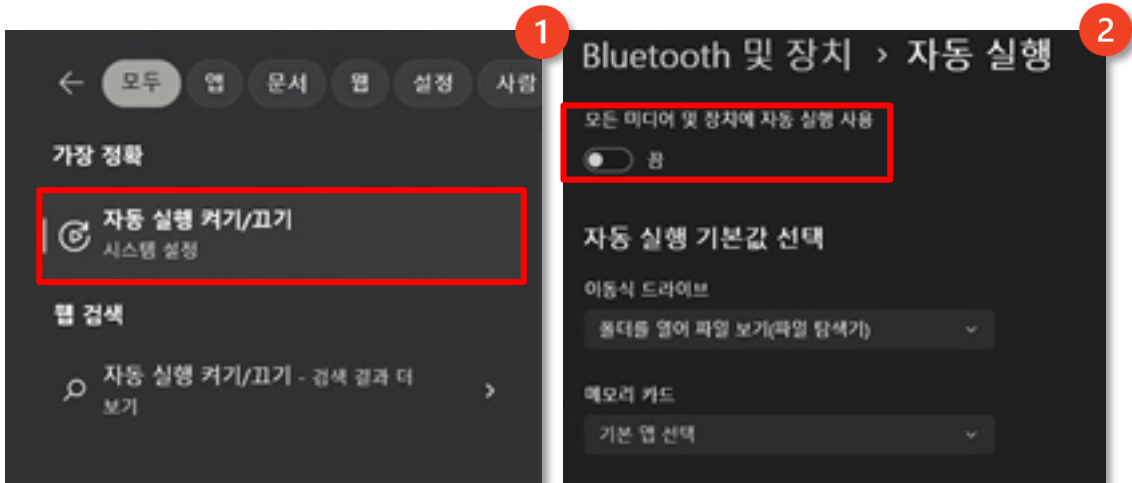
Windows 10/11

6. 이동식 저장매체 자동실행 방지 설정하기

이동식 저장매체가 컴퓨터에 연결되어 자동으로 실행된다면 여러 보안 위협에 노출될 수 있습니다. 특히, 악성코드가 포함된 이동식 저장매체가 자동으로 실행되면 PC나 네트워크 전체가 감염될 위험이 있습니다. 따라서 이동식 저장매체의 자동실행 기능을 비활성화하고, 실행 전 검사를 수행하는 것이 중요합니다.

계정 환경 설정하기

- ① ['자동 실행 켜기/끄기' 검색 및 클릭]
- ② ['모든 미디어 및 장치에 자동 실행 사용' 비활성화]



자동실행 방지 설정 미흡 피해 사례

이동식 저장매체의 자동실행 방지 설정 미흡으로 인한 보안 사고의 사례 중 하나는 2008년 미국 국방성에서 발생한 사건입니다. 악성코드가 포함된 이동식 저장 매체가 PC에 연결되었고, 이를 통해 국방성의 내부 네트워크에 악성코드가 퍼져 나가 대규모 사이버 공격으로 이어졌습니다.

이 사건은 이동식 저장매체가 자동 실행되는 상태에서 악성코드가 포함된 저장매체를 연결하면, 악성코드가 자동으로 실행되어 전체 네트워크를 감염시킬 수 있음을 보여주는 대표적인 사례입니다.

이번 장에서는 인터넷을 사용할 수 있도록 도와주는 프로그램인 웹 브라우저의 보안 설정에 대해서 안내합니다. 국내에서 가장 많이 사용되는 브라우저인 구글 사의 '크롬', 마이크로소프트 사의 '엣지', 네이버 사의 '웨일'을 자세하게 다루고 있습니다.

☑ 웹 브라우저 보안의 중요성

웹 브라우저는 인터넷에 있는 다양한 콘텐츠(웹 문서, 동영상 등)를 검색 및 열람할 수 있게 해주는 응용프로그램을 의미합니다. 웹 브라우저는 인터넷과 연결되기 때문에 인터넷에 있는 유해 콘텐츠가 컴퓨터로 들어오는 주된 경로가 되고 있습니다. 따라서 웹 브라우저에도 적절한 보안 설정을 하는 것이 중요합니다.

가이드라인에서 다루는 제품 확인하기



▲ 구글 크롬



▲ 마이크로소프트 엣지



▲ 네이버 웨일



브라우저 확장프로그램이란?

웹 브라우저 확장프로그램이란, 웹 브라우저의 기본적인 기능에 더해 새로운 기능을 추가할 수 있는 프로그램입니다.

웹 브라우저의 기능을 확장할 수 있고, 인터넷 사용 환경을 개인 맞춤으로 구성할 수 있다는 장점이 있습니다. 웹 브라우저 확장프로그램은 각 브라우저 제공사에서 운영하는 '마켓' 사이트를 통해 구매하거나 설치할 수 있습니다.

대표적인 확장프로그램: 광고 차단 프로그램, VPN 프로그램, 동영상 녹화 프로그램 등

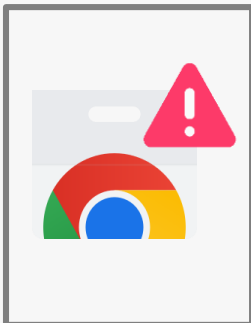


크롬, 엣지: Chrome 웹스토어 / 웨일: 웨일 스토어

하지만 기능이 많아진다는 것은 보안 측면에서 공격 기회가 더 많아질 수 있음을 의미하기도 합니다. 특히 확장프로그램은 웹 브라우저 제조사가 아닌 제3자에 의해서도 만들어질 수 있어 더욱 주의가 필요합니다. 악의적인 목적으로 만들어진 확장프로그램을 설치하게 되면, 그 안의 악성 기능이 실행되어 컴퓨터에 저장된 정보가 유출될 수 있습니다. 따라서 사용자는 보안 관리자가 허가하지 않는 확장프로그램을 설치해서는 안 됩니다.

악성 확장프로그램 적발 실제 사례 (23년 03월 보도)

韓·獨 정보기관 합동, 김수키(북한) 조직의 신종 해킹 수법 경고



(중략) 사이버공격의 수법 중 하나는 '웹 브라우저'의 확장프로그램을 악용한 구글 메일 절취다. 해커는 스피어피싱 방법으로 악성 링크가 포함된 이메일을 피해자에게 발송, 웹 브라우저에서 작동하는 악성 확장프로그램 (이메일을 자동으로 해커에게 전송) 설치를 유도한다. 피해자가 이 프로그램을 설치하면, 해커는 별도 로그인 없이 피해자의 이메일 내용을 실시간으로 절취할 수 있게 된다. (이하 생략)

<출처: 국가정보원>

구글 크롬(Chrome)

1. 업데이트 관리하기

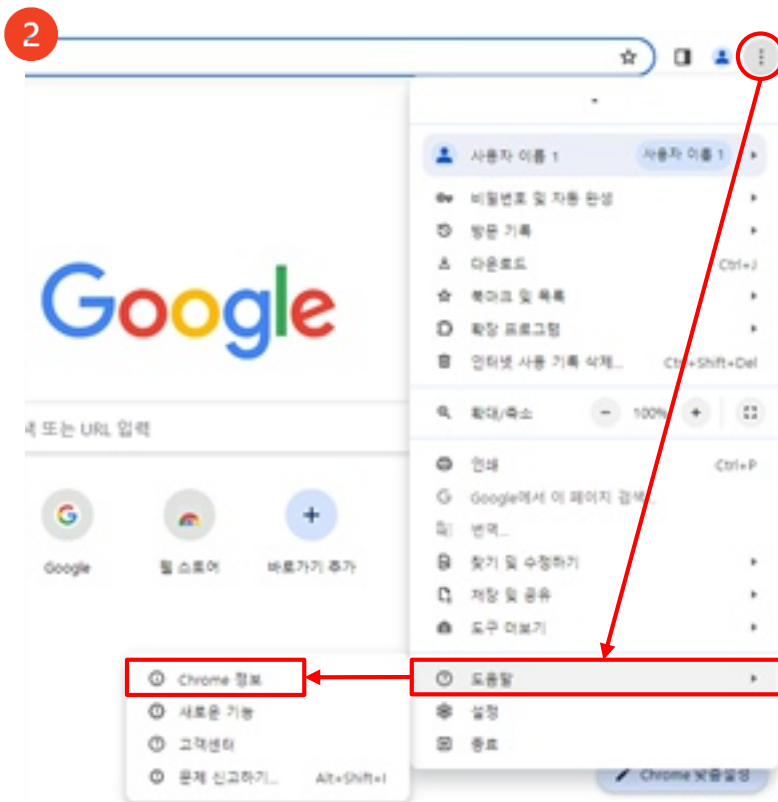
크롬 브라우저는 기본적으로 자동 업데이트가 활성화 있습니다. 브라우저를 재시작할 때 업데이트가 적용됩니다. 업데이트가 오래 미루어지면 웹 브라우저 상단 우측에 대기 중인 업데이트 알림이 표시되며, 이 경우에는 수동 업데이트가 필요합니다.

수동 업데이트하기

- 1 [웹 브라우저 우측 상단 알림 확인]

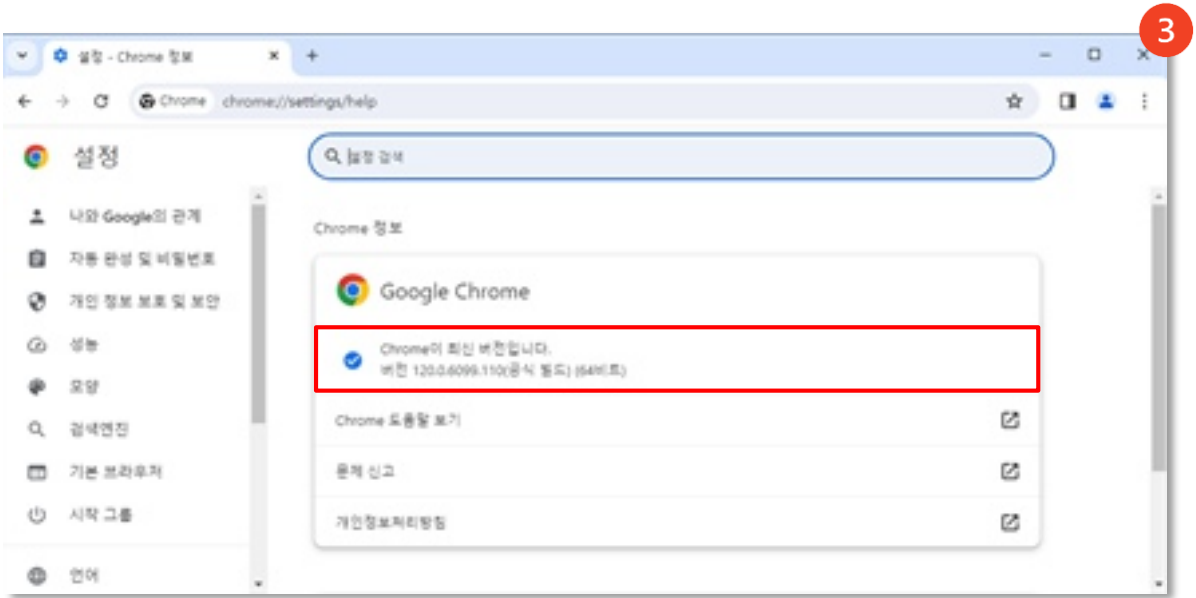


- 2 [웹 브라우저 우측 상단의 : 클릭] > ['도움말' 선택] > ['Chrome 정보' 선택]



구글 크롬(Chrome)

- 3 'Chrome 정보' 에서 현재 웹 브라우저의 버전을 확인할 수 있습니다. 최신버전이 아닌 경우 자동으로 업데이트를 수행합니다. 업데이트가 완료되었다면 '다시 시작'을 클릭해 웹 브라우저를 다시 시작하여 업데이트를 적용해야 합니다.

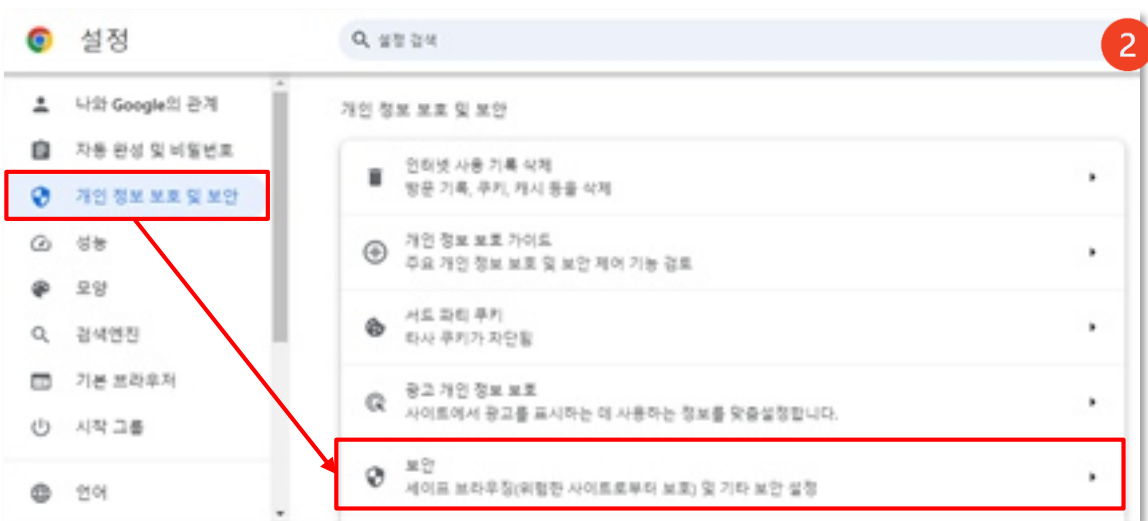
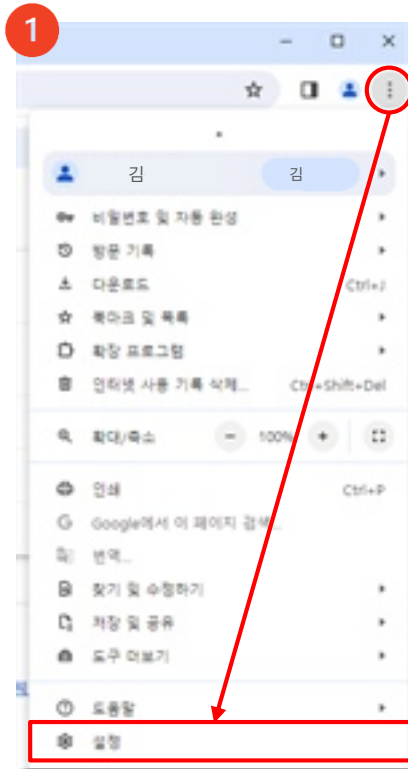


구글 크롬(Chrome)

2. 보안 연결 설정하기

| 업데이트 여부 확인하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정' 선택]
- 2 [개인 정보 보호 및 보안' 선택] > [보안' 선택]



구글 크롬(Chrome)

'항상 보안 연결 사용' 설정은 접속한 웹사이트가 HTTPS를 제공하지 않을 경우 사용자에게 경고 메시지를 표시하거나 그 사이트에 대한 접속을 차단합니다.

3 ['고급'의 '항상 보안 연결 사용' 활성화]



HTTPS가 무엇인가요?

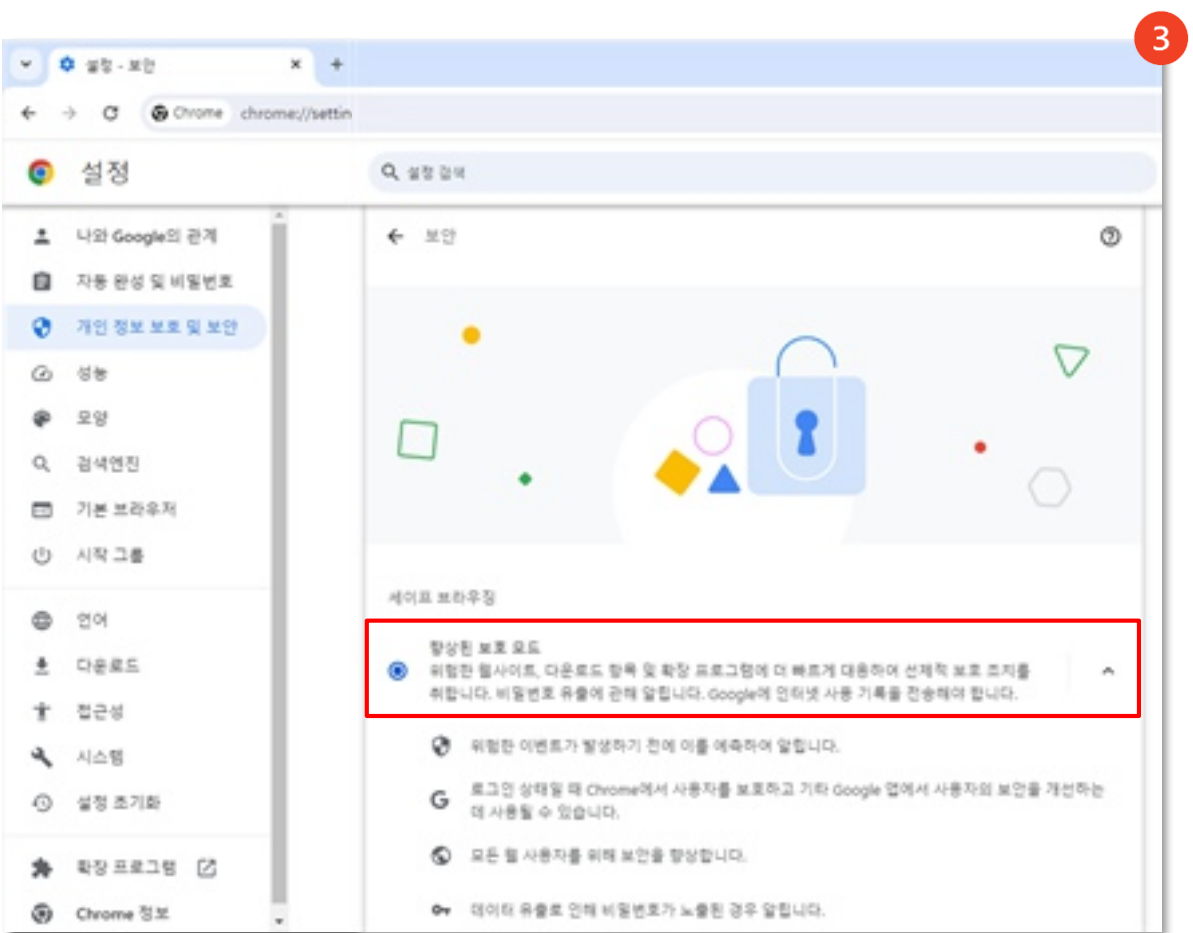
인터넷을 사용할 때, 종종 'HTTPS'라는 용어를 볼 수 있습니다. HTTPS는 웹 사이트가 안전하게 동작한다는 것을 나타내는 중요한 표시입니다.

HTTPS는 웹 사이트와 컴퓨터 사이의 통신을 암호화합니다. 이를 통해 비밀번호나 신용카드 번호와 같은 중요한 정보가 다른 사람에게 노출되지 않도록 할 수 있습니다. 만약 웹 사이트에서 HTTPS를 제공하지 않으면, 누군가가 통신 내용을 도청할 수 있습니다.

구글 크롬(Chrome)

3. 향상된 보호 모드 활성화하기

- 1 [웹 브라우저 우측 상단의 :클릭] > ['설정' 선택] *사진생략
- 2 ['개인 정보 보호 및 보안' 선택] > ['보안' 선택]
- 3 ['세이프 브라우징'에서 '향상된 보호 모드' 선택]

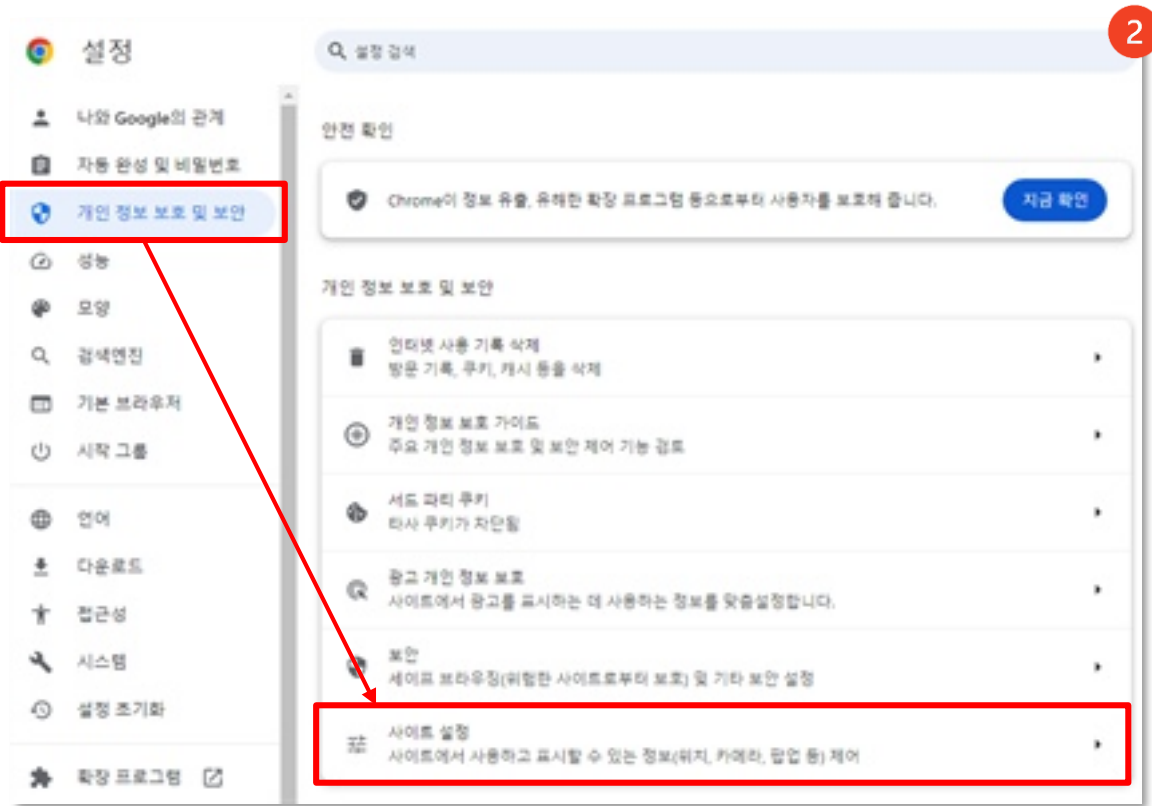


구글 크롬(Chrome)

4. 팝업 및 리디렉션 차단하기

팝업 기능은 웹 브라우저에 작은 창을 띄워 정보를 제공하는 기능을 하며, 리디렉션 기능은 한 사이트에 접속했을 때 다른 사이트로 자동으로 연결해주는 기능을 합니다. 그러나 최근 과도한 광고 팝업 또는 리디렉션을 이용한 낚치 광고가 브라우저 이용자에게 많은 불편을 주고 있어 해당 기능을 차단할 것을 권장합니다.

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정' 클릭] *사진 생략
- 2 ['개인 정보 보호 및 보안' 선택] > ['사이트 설정' 선택]

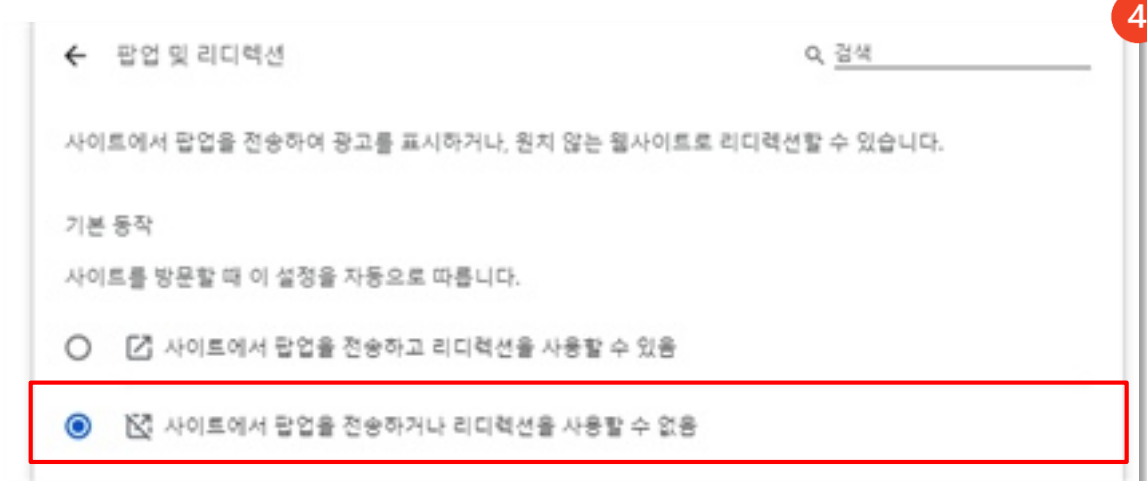


구글 크롬(Chrome)

3 ['콘텐츠'의 '팝업 및 리디렉션' 선택]



4 ['기본 동작'에서 '사이트에서 팝업을 전송하거나 리디렉션을 사용할 수 없음' 선택]



구글 크롬(Chrome)

특정 사이트에 팝업 및 리디렉션 허용

- 5 [하단의 '맞춤설정된 동작' 에서 '팝업 전송 및 리디렉션 사용이 허용됨'의 '추가' 클릭]



- 6 [허용할 사이트의 주소를 입력한 뒤, '추가' 클릭]

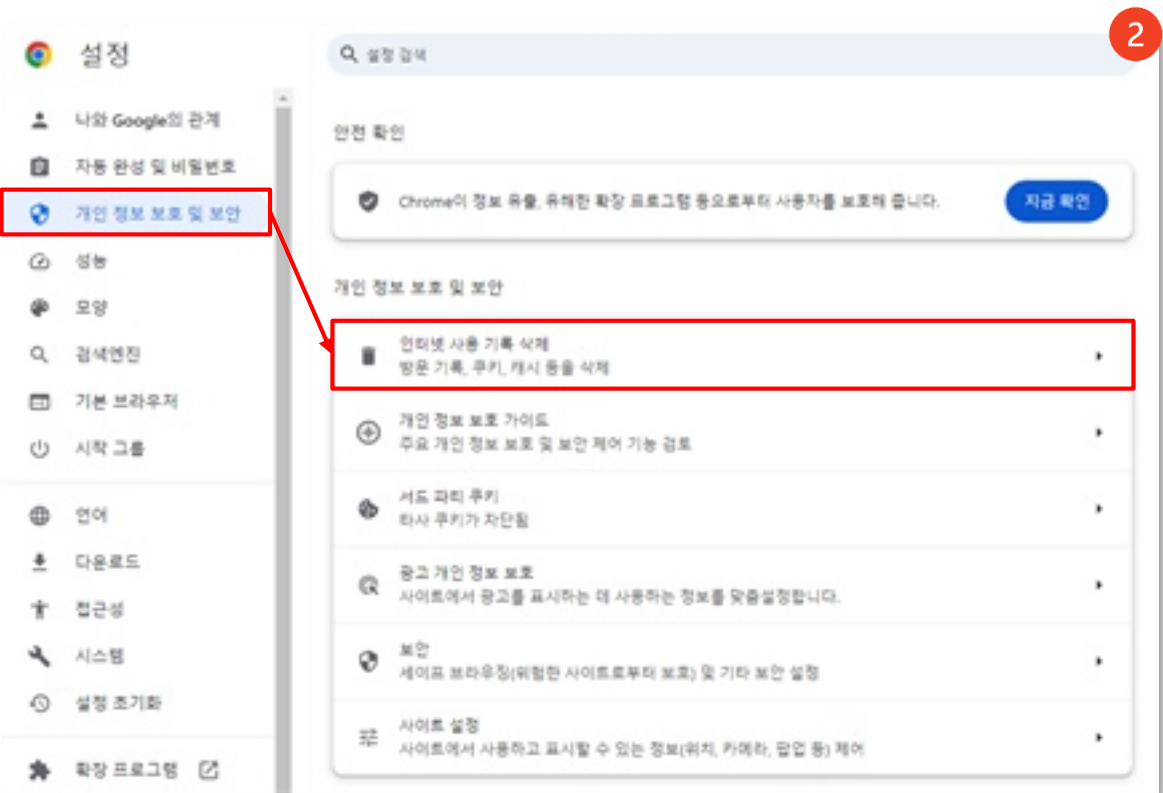


구글 크롬(Chrome)

5. 쿠키 및 임시파일(캐시) 삭제하기

1 쿠키 및 임시파일(캐시) 삭제

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정' 선택]
- 2 [개인 정보 보호 및 보안' 선택] > [인터넷 사용기록 삭제' 선택]

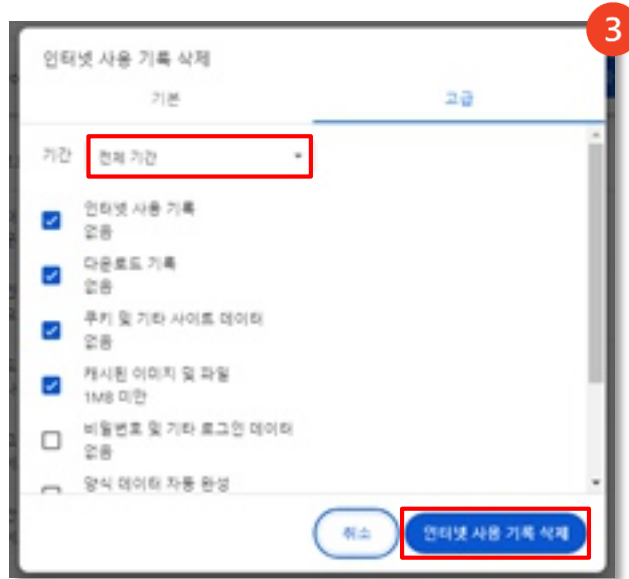


쿠키란 무엇인가요?

쿠키는 사용자의 인터넷 활동을 저장하는 작은 파일을 의미합니다. 사용자의 인터넷 활동을 기록해 PC에 저장해두고, 웹 사이트에 다시 방문했을 때 이 정보를 전송합니다. 쿠키안에 개인정보가 포함되어 있는 경우, 쿠키가 유출되면서 개인정보도 함께 유출될 수 있습니다. 따라서 주기적으로 쿠키를 삭제할 것을 권장합니다.

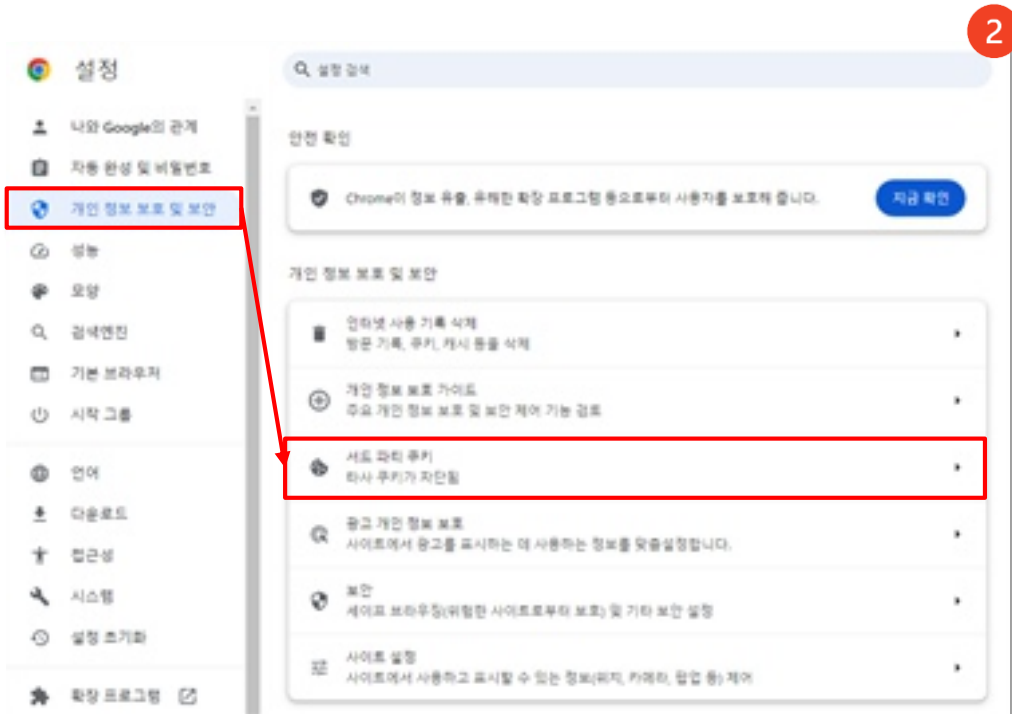
구글 크롬(Chrome)

- 3 [기간을 선택한 후(1시간, 1일, 7일, 4주, 전체) '인터넷 사용 기록 삭제' 클릭]



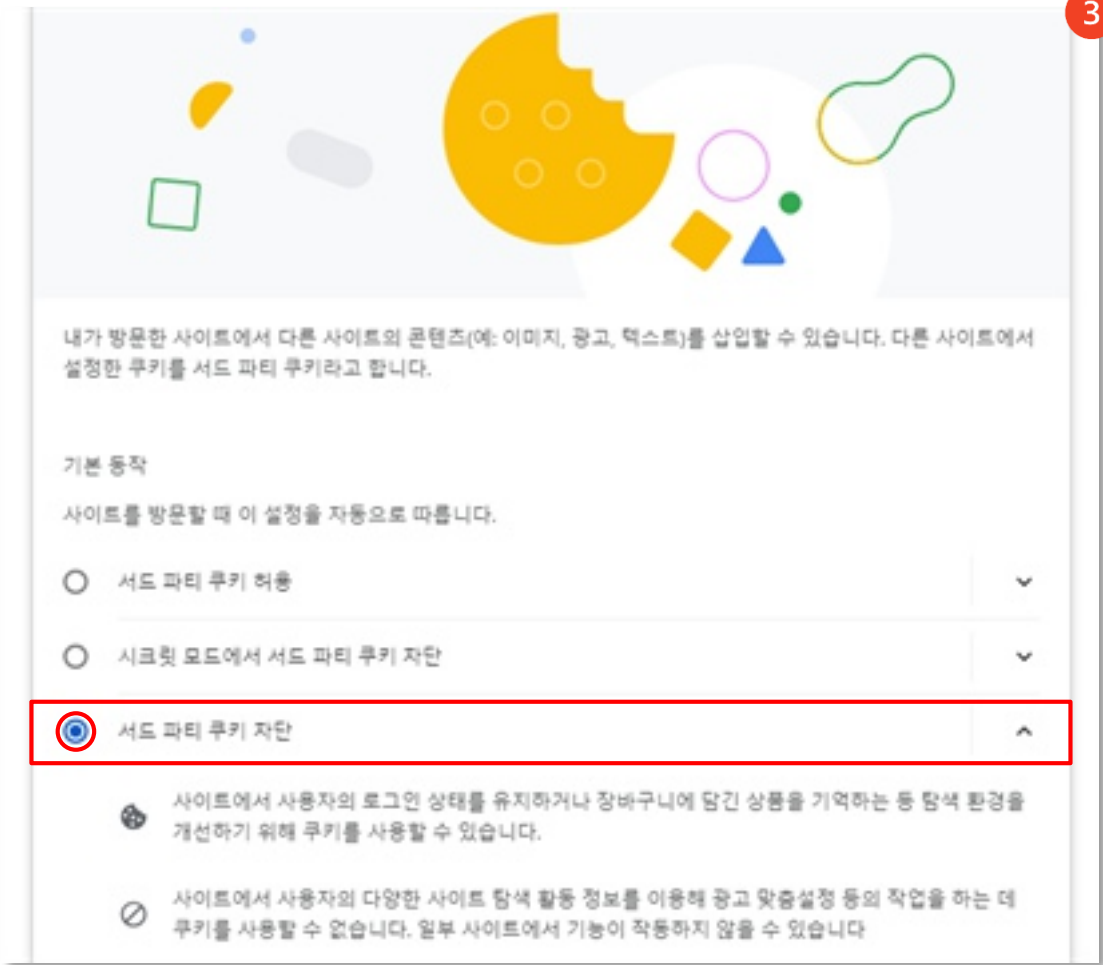
서드파티 쿠키 차단

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택] *사진 생략
- 2 ['개인 정보 보호 및 보안' 선택] > ['서드 파티 쿠키' 선택]



구글 크롬(Chrome)

3 [기본 동작'에서 '서드 파티 쿠키 차단' 선택]



서드파티 쿠키란 무엇인가요?

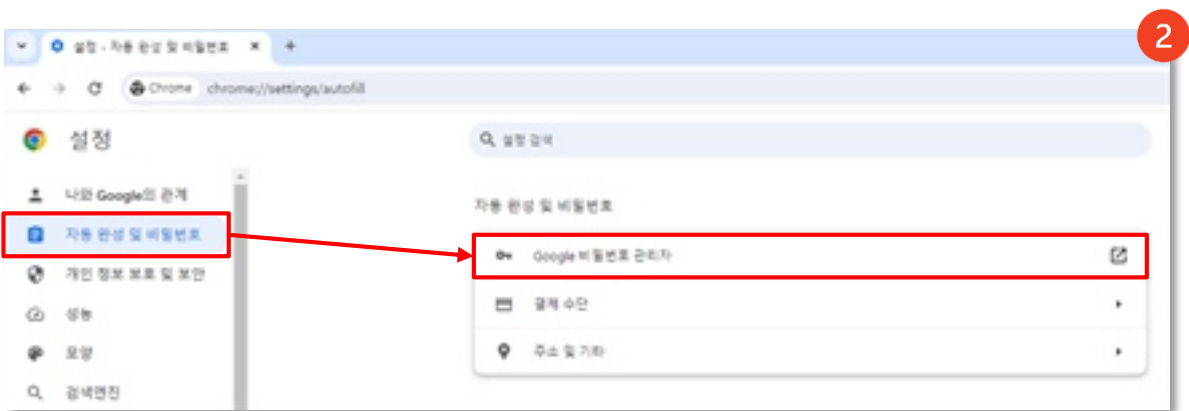
서드파티 쿠키란 사용자가 방문한 사이트가 아닌 다른 사이트에서 생성해 컴퓨터에 저장해놓은 임시저장 파일입니다. 이 안에는 여러 사이트에서의 인터넷 활동이 기록됩니다. 서드파티 쿠키는 사용자의 인터넷 활동을 추적하여 맞춤형 광고를 제공하는 데 주로 활용되고 있습니다. 그러나 이는 사용자가 이용하지 않은 서비스에 의해 활동 내용이 기록되는 것이기 때문에 예상하지 못한 보안 사고가 발생할 수 있습니다. 따라서 차단을 권장합니다.

구글 크롬(Chrome)

6. 중요정보 자동완성 해제하기

| 중요정보 자동완성 해제하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택] *사진 생략
- 2 ['자동완성 및 비밀번호' 선택] > ['Google 비밀번호 관리자' 선택]



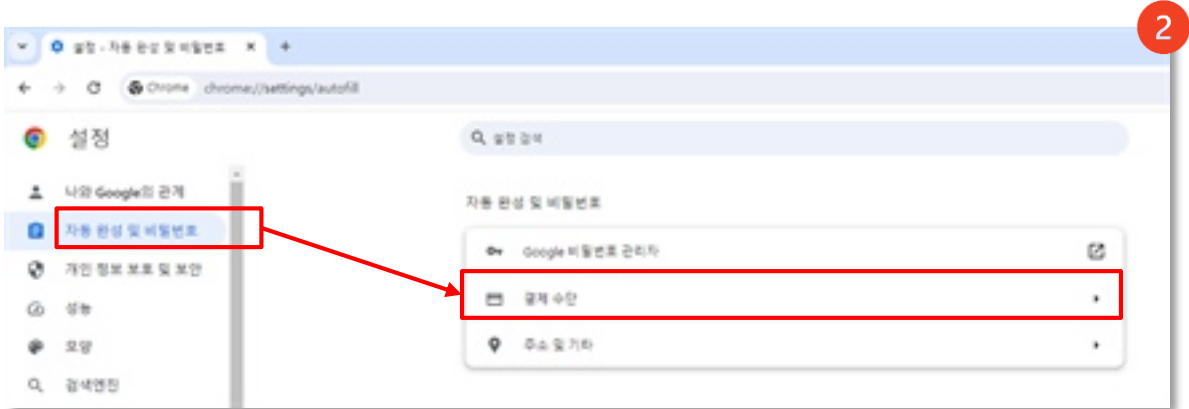
- 3 [좌측 메뉴에서 '설정' 선택] > ['비밀번호 저장 여부 확인'과 '자동으로 로그인' 비활성화]



구글 크롬(Chrome)

결제정보(카드번호) 자동저장 해제하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택] *사진 생략
- 2 ['자동완성 및 비밀번호' 선택] > ['결제 수단' 선택]



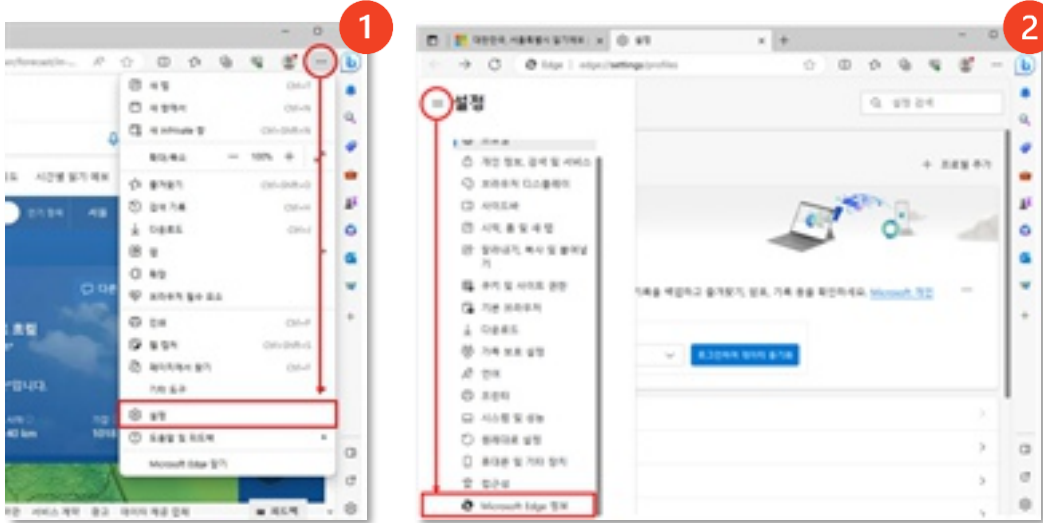
- 3 ['결제 수단'에서 '결제 수단 저장 및 자동 입력'과 '사이트에서 저장한 결제 수단이 있는지 확인하도록 허용' 비활성화]



마이크로소프트 엣지(Edge)

1. 자동 업데이트 활성화하기

- 1 [웹 브라우저 우측 상단의...클릭] > ['설정' 선택]
- 2 [좌측 상단의 ≡ 클릭] > ['Microsoft Edge 정보' 선택]



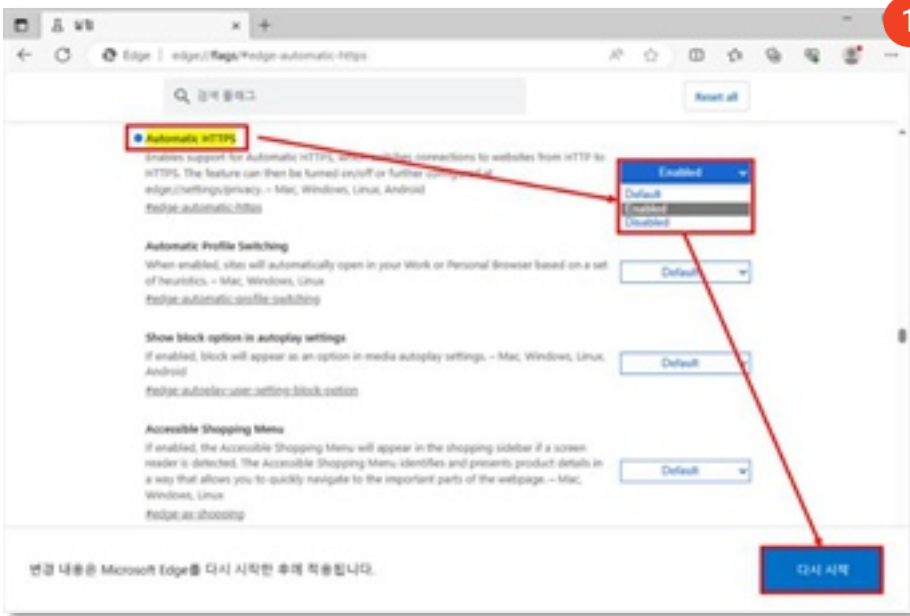
- 3 [버전 확인 후 자동으로 업데이트 진행]
- 4 ['다시 시작'을 클릭하여 웹 브라우저 종료 후 재시작: 업데이트 적용 완료]



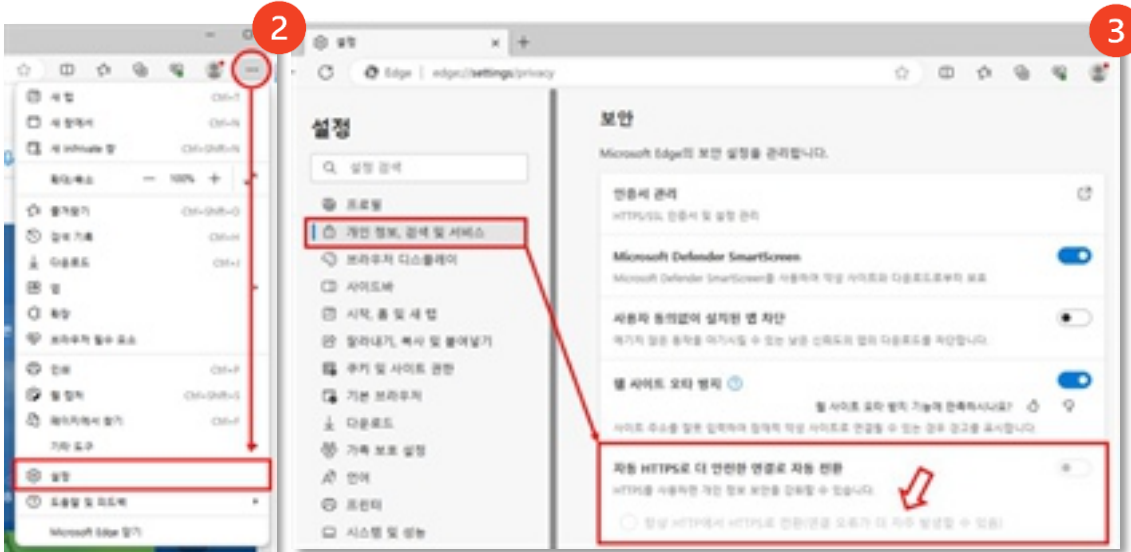
마이크로소프트 엣지(Edge)

2. HTTPS 자동전환 활성화하기

- 1 [웹 브라우저 주소창에 'edge://flags/#edge-automatic-https' 입력] > [노란색으로 강조된 'Automatic HTTPS' 영역을 'Enabled'으로 선택] > ['다시 시작'을 클릭하여 웹 브라우저 재실행]



- 2 [웹 브라우저 우측 상단의 ... 클릭] > ['설정' 선택]
- 3 [좌측 상단의 ≡ 클릭] > [메뉴에서 '설정' 클릭] > ['개인정보, 검색 및 서비스' 선택] > ['보안' 에서 '자동 HTTPS로 더 안전한 연결로 자동 전환' 활성화] > ['항상 HTTP에서 HTTPS로 전환' 선택]



마이크로소프트 엣지(Edge)

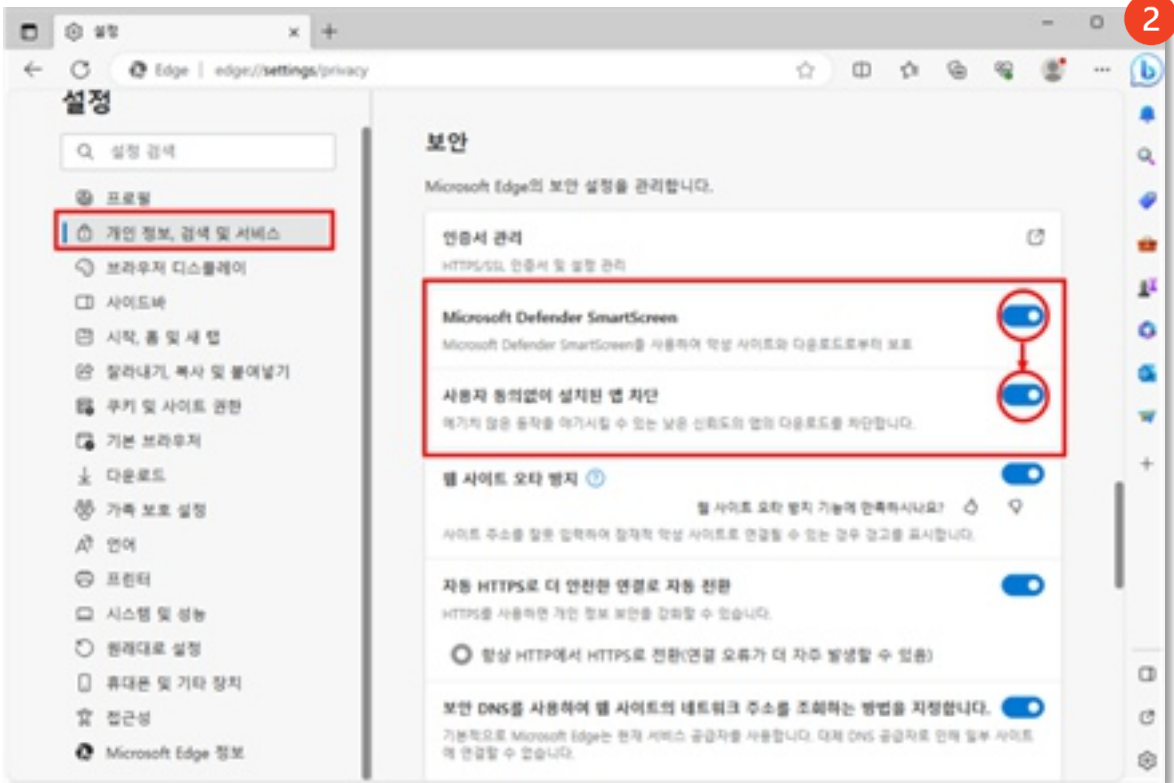
HTTPS가 무엇인가요?

인터넷을 사용할 때, 종종 'HTTPS'라는 용어를 볼 수 있습니다. HTTPS는 웹 사이트가 안전하게 동작한다는 것을 나타내는 중요한 표시입니다.

HTTPS는 웹 사이트와 컴퓨터 사이의 통신을 암호화합니다. 이를 통해 비밀번호나 신용카드 번호와 같은 중요한 정보가 다른 사람에게 노출되지 않도록 할 수 있습니다. 만약 웹 사이트에서 HTTPS를 제공하지 않으면, 누군가가 통신 내용을 도청할 수 있습니다.

3. Smart Screen 활성화하기

- 1 [웹 브라우저 우측 상단의...클릭] > ['설정' 선택] *사진 생략
- 2 [좌측 상단의 ≡ 클릭] > ['개인정보, 검색 및 서비스' 선택] > ['보안' 항목에서 'Microsoft Defender SmartScreen' 활성화] > ['사용자 동의없이 설치된 앱 차단' 활성화]

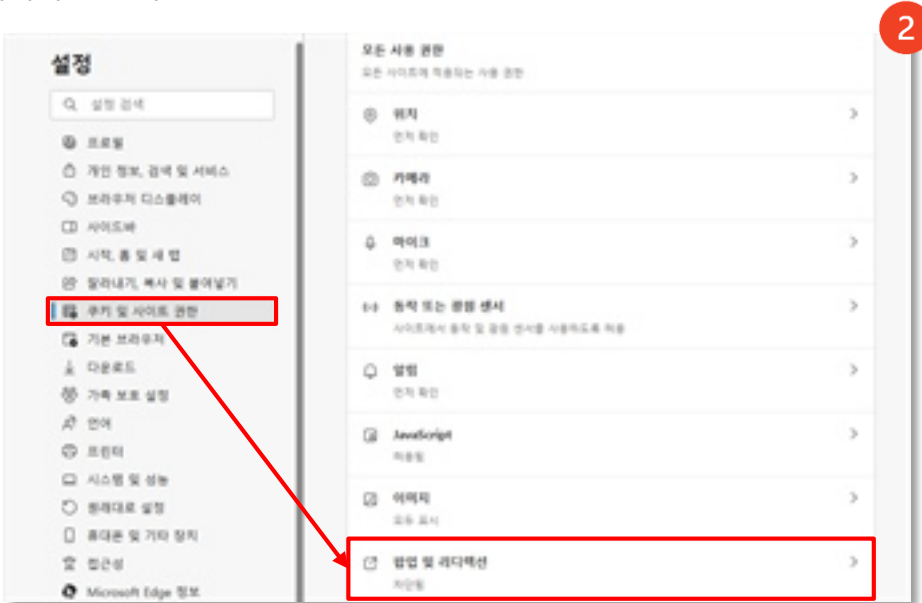


마이크로소프트 엣지(Edge)

4. 팝업 및 리디렉션 차단하기

팝업 기능은 웹 브라우저에 작은 창을 띄워 정보를 제공하는 기능을 하며, 리디렉션 기능은 한 사이트에 접속했을 때 다른 사이트로 자동으로 연결해주는 기능을 합니다. 그러나 과도한 광고 팝업으로 인한 사용자 편의성 저하, 리디렉션을 이용한 낚치 광고와 같은 여러 문제점을 가지고 있어 해당 기능을 차단할 것을 권장합니다.

- 1 [웹 브라우저 우측 상단의...클릭] > [설정' 선택] *사진 생략
- 2 [좌측 상단의 ≡ 클릭] > [쿠키 및 사이트 권한' 선택] > [모든 사용 권한' 항목에서 '팝업 및 리디렉션' 선택]



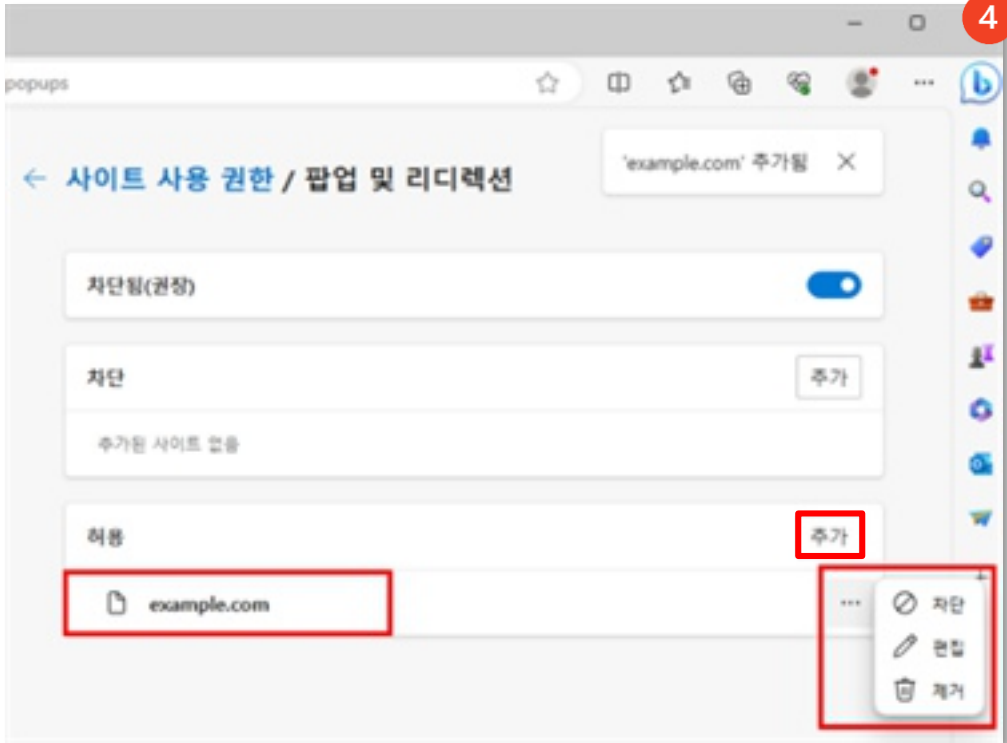
- 3 ['차단됨(권장)' 활성화]



마이크로소프트 엣지(Edge)

하단의 '차단' 영역과 '허용' 영역에서 구체적으로 팝업 및 리디렉션을 차단 및 허용할 사이트를 추가할 수 있습니다.

- 4 [우측의 '추가' 클릭 후 입력창에 팝업 및 리디렉션을 차단/허용할 사이트를 입력]



- 5 [차단 혹은 허용할 사이트의 주소를 입력한 후 '추가'를 클릭해 설정 완료]

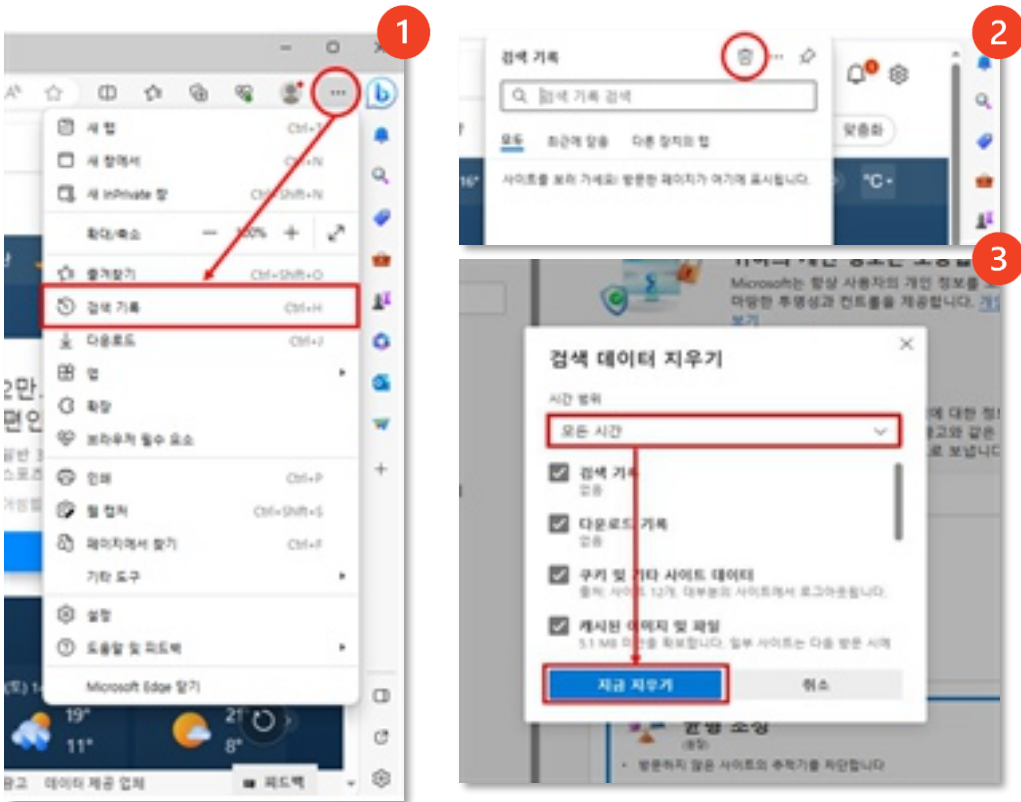


마이크로소프트 엣지(Edge)

5. 쿠키 및 임시파일 삭제하기

1 쿠키 및 임시파일(캐시) 삭제하기

- 1 [웹 브라우저 우측 상단의...클릭] > ['검색 기록' 선택]
- 2 [새로 나타난 창의 우측 상단에 위치한 '휴지통' 아이콘 클릭]
- 3 ['검색 데이터 지우기' 메뉴에서 기간을 설정, (1시간, 1일, 7일, 4주, 전체) 그 후 '지금 지우기' 클릭]



쿠키란 무엇인가요?

쿠키는 사용자의 인터넷 활동을 저장하는 작은 파일을 의미합니다. 사용자의 인터넷 활동을 기록해 PC에 저장해두고, 웹 사이트에 다시 방문했을 때 이 정보를 전송합니다. 쿠키안에 개인정보가 포함되어 있는 경우, 쿠키가 유출되면서 개인정보도 함께 유출될 수 있습니다. 따라서 주기적으로 쿠키를 삭제할 것을 권장합니다.

마이크로소프트 엣지(Edge)

서드파티 쿠키 차단하기

- 1 [웹 브라우저 우측 상단의...클릭] > ['설정' 선택] *사진 생략
- 2 ['쿠키 및 사이트 권한' 선택] > ['쿠키 및 저장된 데이터' 항목에서 '쿠키 및 사이트 데이터 관리 및 삭제' 선택]



- 3 ['타사 쿠키 차단'을 활성화]



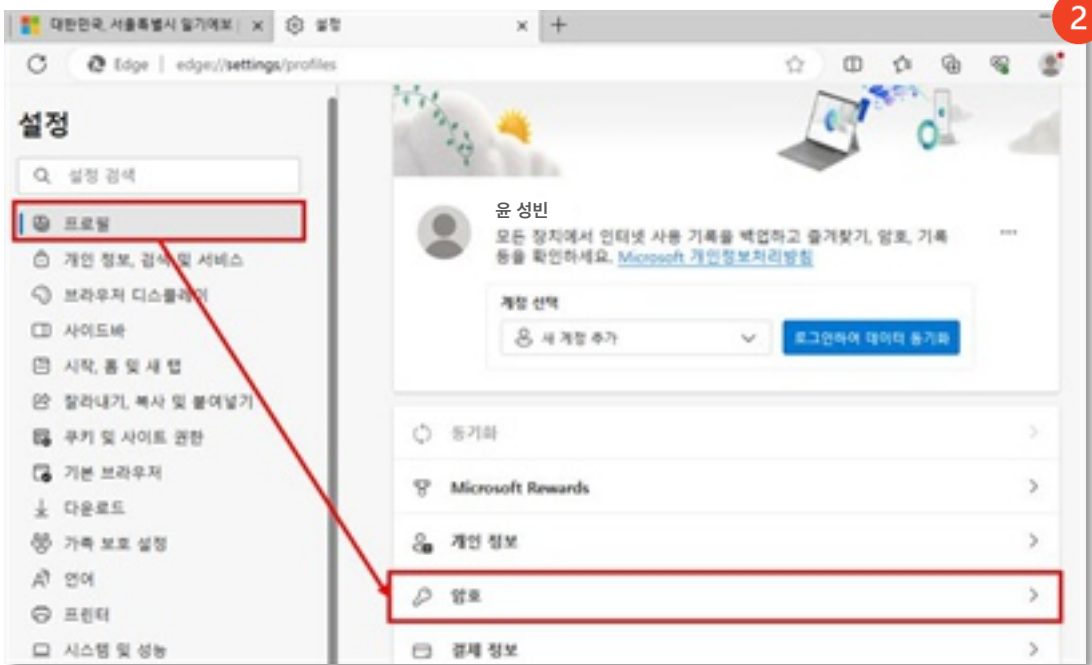
마이크로소프트 엣지(Edge)

6. 중요 정보 자동완성 해제하기

1 중요 정보 자동완성 해제하기

1 [웹 브라우저 우측 상단의...클릭] > ['설정' 선택] *사진 생략

2 [설정] > ['프로필' 선택] > ['암호' 선택]



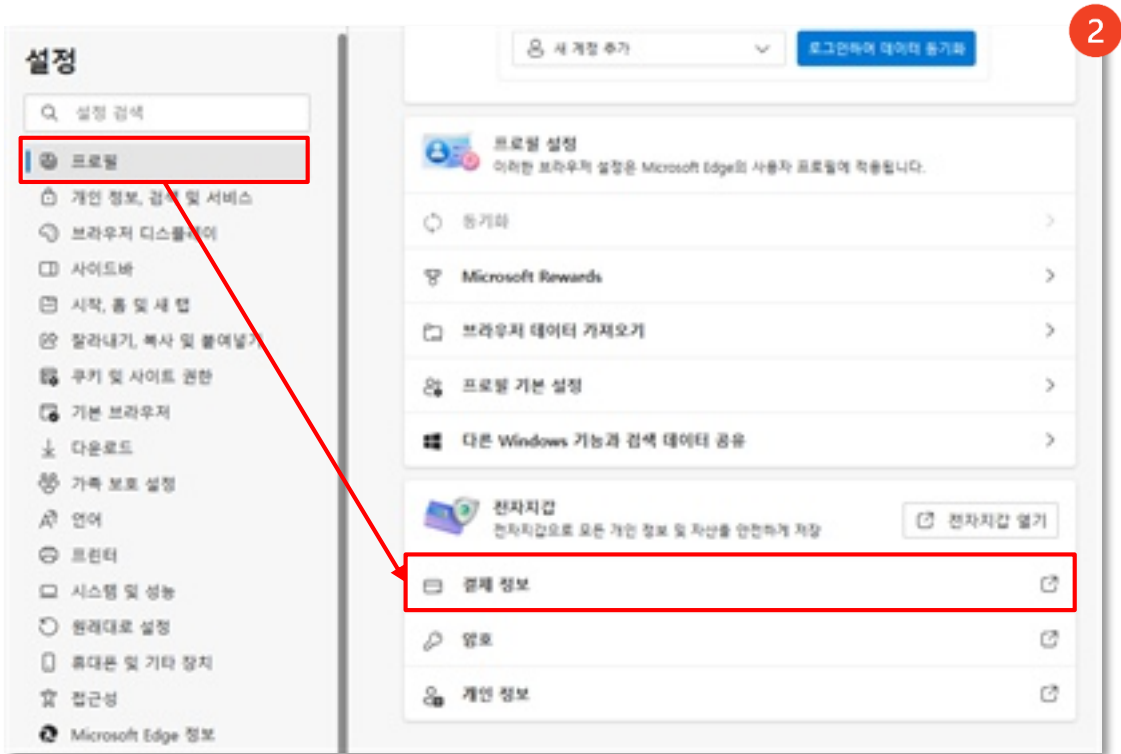
3 ['암호를 저장하도록 제안', '자동으로 암호 저장', '암호 자동 채우기'를 모두 비활성화]



마이크로소프트 엣지(Edge)

결제 정보(카드번호) 자동저장 해제

- 1 [웹 브라우저 우측 상단의...클릭] > ['설정' 선택] *사진 생략
- 2 [설정] > ['프로필' 선택] > ['결제 정보' 선택]



- 3 ['결제 정보 저장 및 채우기'를 비활성화]



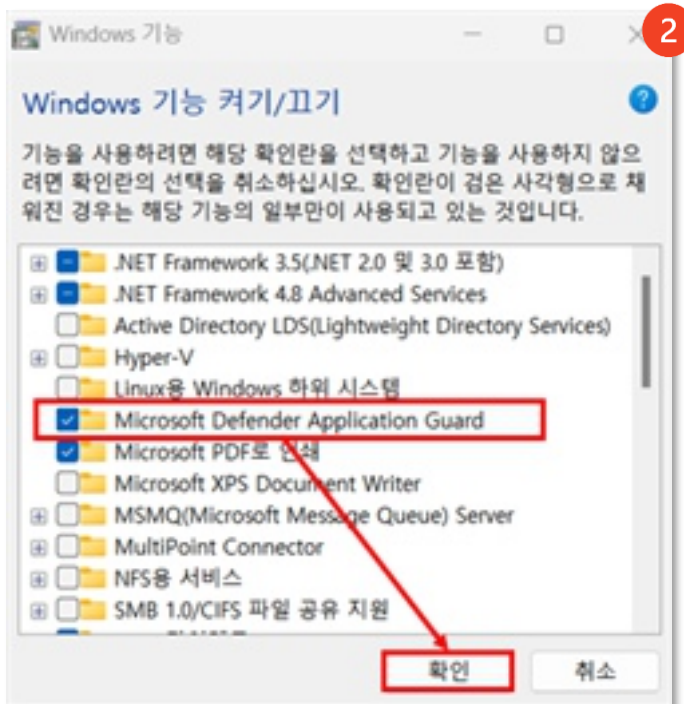
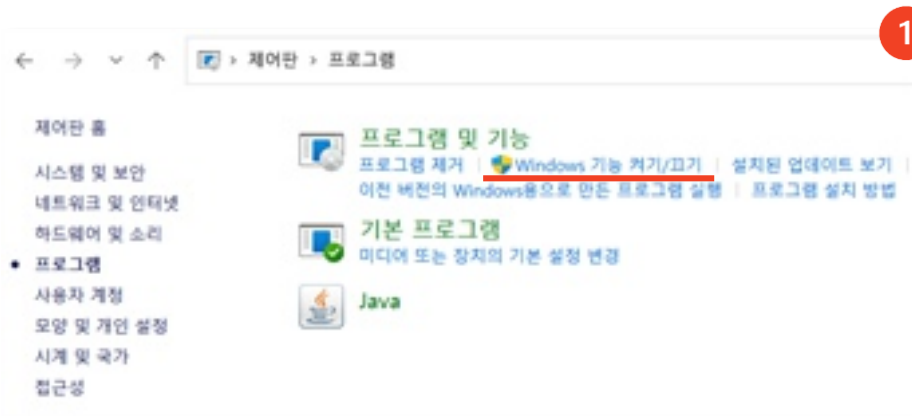
마이크로소프트 엣지(Edge)

7. 브라우저 격리기능 활성화하기

윈도우 시스템 운영체제가 최소 아래 버전 이상을 필요로 합니다.

Windows 10 Enterprise 버전, 버전 1709 이상	Windows 10 Pro 버전, 버전 1803 이상
Windows 10 Education 버전, 버전 1809 이상	Windows 11 Enterprise, 교육 또는 Pro 버전

- 1 [PC 운영체제의 '제어판'의 '프로그램' 클릭] > ['프로그램 및 기능'의 'Windows 기능 켜기/끄기' 클릭] >
- 2 ['Microsoft Defender Application Guard'를 활성화한 후 '확인' 클릭] > [자동으로 설치 후 컴퓨터 재시작]

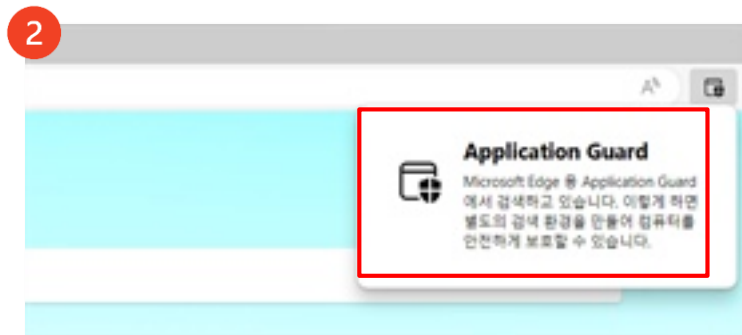
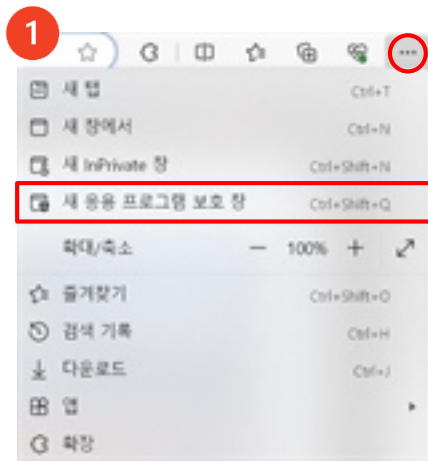


마이크로소프트 엣지(Edge)

브라우저 격리 기능 활성화하기

- 1 [웹 브라우저 우측 상단의...클릭] > ['새 응용 프로그램 보호 창' 선택]
- 2 [새롭게 나타난 브라우저 창에서 인터넷 사용]

'새 응용프로그램 보호 창' 버튼을 클릭 후 새로 나타난 브라우저 창이 브라우저 격리가 적용된 웹 브라우저입니다. 추후 인터넷을 다시 이용할 시에도 웹 브라우저를 연 뒤, '새 응용 프로그램 보호 창'을 클릭하여 웹 브라우저를 새로 열어야 합니다.



브라우저 격리란 무엇인가요?

브라우저 격리 기술은 웹 브라우저와 PC 운영체제를 분리하여, 서로 침입할 수 없도록 장벽을 세우는 것과 같은 기술입니다.

컴퓨터 내 격리된 공간에서 웹사이트에 접속하기 때문에, 악성코드가 PC에 침입하더라도 PC 환경을 안전하게 보호할 수 있습니다.

웹 브라우저에서도 브라우저 격리 기술을 제공하고 있으므로 사용을 권장합니다.

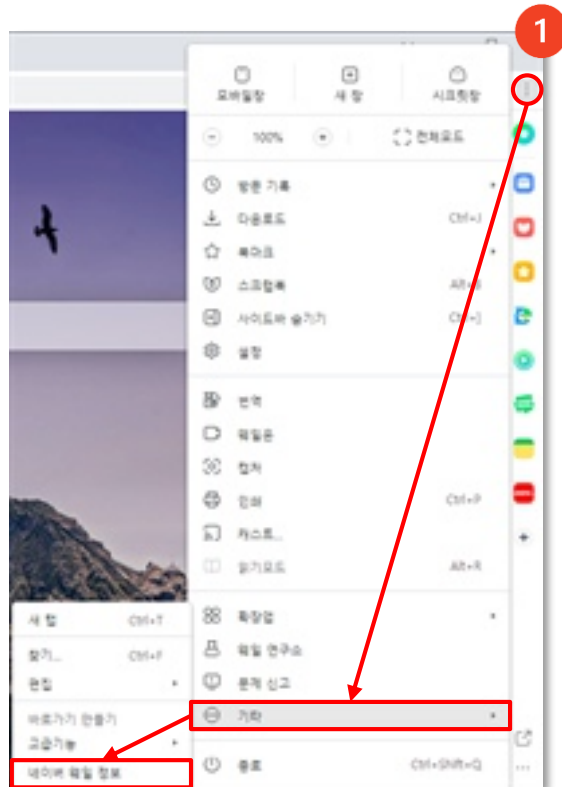
네이버 웨일(Whale)

1. 자동 업데이트 활성화하기

| 계정 환경 설정하기

웨일 브라우저는 기본 설정으로 자동 업데이트가 활성화 되어있습니다. 따라서 PC는 스스로 업데이트를 수행하며 웹 브라우저를 종료한 후 재시작하면 업데이트가 적용됩니다.

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['기타' 선택] > ['네이버 웨일 정보' 선택]
- 2 [버전 확인]



네이버 웨일 정보

NAVER Whale

네이버 웨일이 최신 버전입니다.
버전 3.23.214.17(공식 빌드) (64비트) [자세히 알아보기](#)

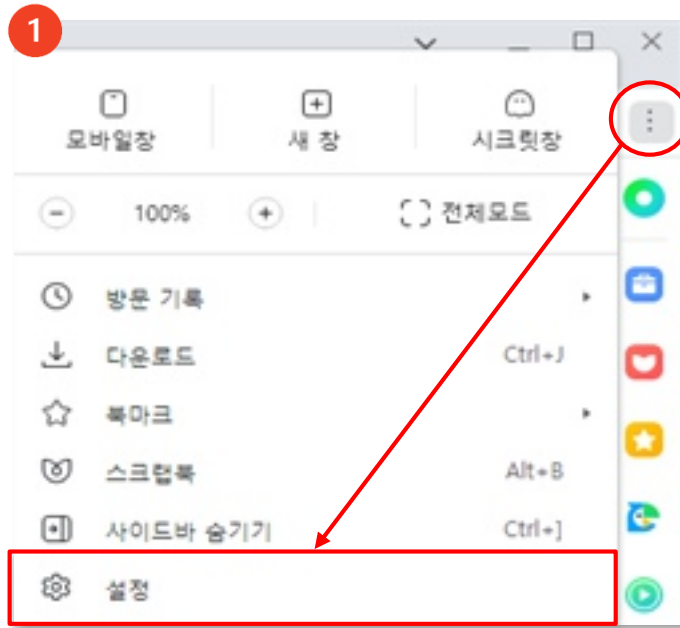
네이버 웨일 도움말 보기

문제 신고

네이버 웨일(Whale)

2. HTTPS 자동 전환 활성화하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택]



- 2 ['개인정보 보호' 선택] > ['보안' 선택]



네이버 웨일(Whale)

3 [‘고급’에서 ‘항상 보안 연결 사용’ 활성화]



HTTPS가 무엇인가요?

인터넷을 사용할 때, 종종 'HTTPS'라는 용어를 볼 수 있습니다. HTTPS는 웹 사이트가 안전하게 동작한다는 것을 나타내는 중요한 표시입니다.

HTTPS는 웹 사이트와 컴퓨터 사이의 통신을 암호화합니다. 이를 통해 비밀번호나 신용카드 번호와 같은 중요한 정보가 다른 사람에게 노출되지 않도록 할 수 있습니다. 만약 웹 사이트에서 HTTPS를 제공하지 않으면, 누군가가 통신 내용을 도청할 수 있습니다.

네이버 웨일(Whale)

3. 팝업 차단 및 관리하기

웨일에서는 기본적으로 '스마트 팝업 사용' 기능이 기본적으로 설정되어 있습니다. 스마트 팝업은 네이버 웨일에서 제공하는 기능으로 팝업을 쉽게 종료할 수 있도록 팝업을 화면의 한 부분에만 띄우는 기능입니다. 기본적으로 팝업을 사용하는 정책이므로 팝업을 사용하지 않으려면 아래와 같이 설정하십시오.

팝업차단 활성화하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택] *사진 생략
- 2 ['기본' 선택] > [하단 '클린 웹' 에서 '팝업' 선택]
- 3 ['차단' 선택]



네이버 웨일(Whale)

팝업 허용 사이트 관리하기

- 1 [팝업'에서 하단 '맞춤설정된 동작' - '차단' 또는 '허용' 의 '추가' 클릭]
- 2 [팝업을 차단 또는 허용할 사이트의 주소 입력 후 '추가' 클릭]



네이버 웨일(Whale)

4. 쿠키 및 임시파일(캐시)관리 하기

1. 쿠키 및 임시파일(캐시) 삭제

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정 선택]
- 2 [개인정보 보호 선택] > [인터넷 사용기록 삭제 선택]
- 3 [기간을 선택한 후 (1시간, 1일, 7일, 4주, 전체) '인터넷 사용 기록 삭제' 클릭]



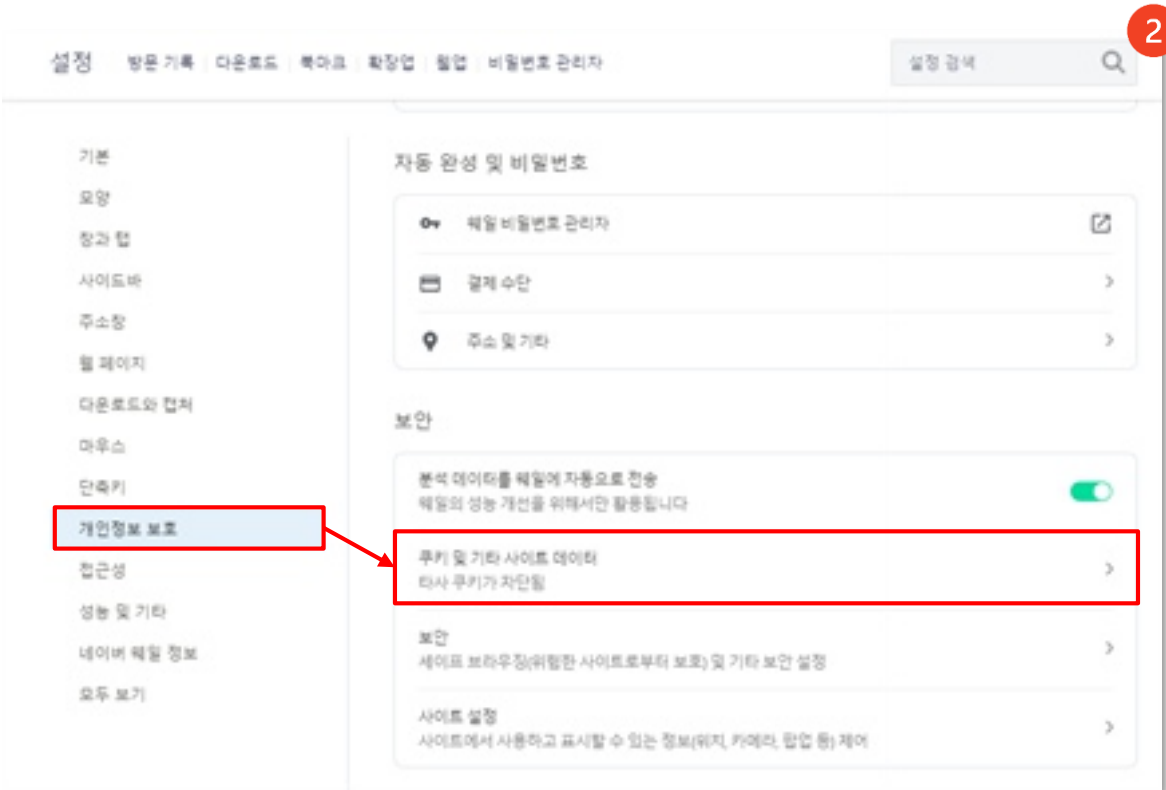
네이버 웨일(Whale)

쿠키란 무엇인가?

쿠키는 사용자의 인터넷 활동을 저장하는 작은 파일을 의미합니다. 사용자의 인터넷 활동을 기록해 PC에 저장해두고, 웹 사이트에 다시 방문했을 때 이 정보를 전송합니다. 쿠키안에 개인정보가 포함되어 있는 경우, 쿠키가 유출되면서 개인정보도 함께 유출될 수 있습니다. 따라서 주기적으로 쿠키를 삭제할 것을 권장합니다.

서드파티 쿠키 차단하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정' 선택]
- 2 ['개인정보 보호' 선택] > ['쿠키 및 기타 사이트 데이터' 선택]



네이버 웨일(Whale)

3 [일반 설정'의 '서드 파티 쿠키 차단' 선택]



서드파티 쿠키란 무엇인가요?

서드파티 쿠키란 사용자가 방문한 사이트가 아닌 다른 사이트에서 생성해 컴퓨터에 저장해놓은 임시저장 파일입니다. 이 안에는 여러 사이트에서의 인터넷 활동이 기록됩니다. 서드파티 쿠키는 사용자의 인터넷 활동을 추적하여 맞춤형 광고를 제공하는데 주로 활용되고 있습니다. 그러나 이는 사용자가 이용하지 않은 서비스에 의해 활동 내용이 기록되는 것이기 때문에 예상하지 못한 보안 사고가 발생할 수 있습니다. 따라서 차단을 권장합니다.

네이버 웨일(Whale)

5. 중요정보 자동완성 해제하기

| 중요정보 자동완성 해제하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > [설정' 선택] *사진 생략
- 2 [개인정보 보호' 선택] > [자동완성 및 비밀번호' 항목에서 '웨일 비밀번호 관리자' 선택]



- 3 [좌측 메뉴에서 '설정' 선택] > ['설정'에서 '비밀번호 저장 여부 확인'과 '자동으로 로그인'을 비활성화]



네이버 웨일(Whale)

결제정보(카드번호) 자동저장 해제하기

- 1 [웹 브라우저 우측 상단의 : 클릭] > ['설정' 선택]
- 2 ['개인정보 보호' 선택] > ['자동완성 및 비밀번호' 항목에서 '결제 수단' 선택]
- 3 ['결제 수단 저장 및 자동 입력'과 '사이트에서 저장한 결제 수단이 있는지 확인하도록 허용'을 모두 비활성화]

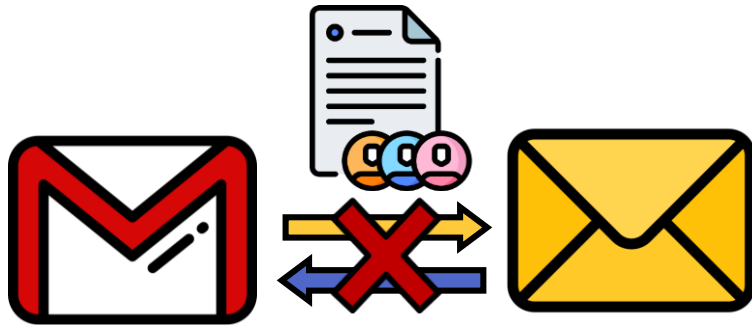


이것만은 지키자!

행동수칙

이메일 편

1



외부 이메일을 통해 업무자료를 주고받지 않아요!

포털사이트(네이버 등) 이메일은 외부에서도 접근이 가능해서 공격자에게 공격을 당할 수 있습니다. 포털사이트 계정이 공격당하면 그 이메일에 남아있는 업무자료나 기밀 정보가 유출될 수 있습니다.

2



연락처, 이메일 주소 등 외부에 공개되어 있는 회사 정보를 관리해요!

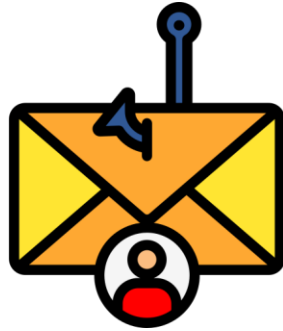
공격자들은 외부에 공개되어 있는 회사 사이트나 SNS 계정에서 정보를 수집하여 공격에 활용하기도 합니다. 따라서, 회사 정보가 외부에 얼마나 공개되어 있는지를 파악하고 관리해야 합니다.

이것만은 지키자!

행동수칙

이메일 편

3



사칭 및 사기 이메일에 속지 않도록 주의해요!

공격자들은 정부기관, 협력사나 포털사이트 운영자를 사칭하여 이메일을 보냅니다. 실제로 회사와 관련이 있는 사람을 사칭하기 때문에, 이메일을 그대로 신뢰하게 될 가능성이 높아 주의해야 합니다.

4



수상한 첨부파일을 다운 받거나 가짜 링크에 접속하지 않아요!

수상한 이메일에 첨부된 파일을 다운 받거나, 링크(URL)를 클릭하였다가 악성코드에 감염될 수 있습니다. 이 경우 회사의 기밀 정보가 유출되거나, 회사 파일이 훼손되는 피해가 발생할 수 있습니다.

이번 장에서는 인터넷을 통해 편지를 주고받을 수 있는 '이메일'에 대하여 다룹니다. 이메일을 통해 발생한 해킹 사고 사례를 살펴보고, 이메일을 안전하게 사용할 수 있는 방법을 설명합니다.

☑ 이메일 보안은 왜 해야 할까요?

이메일은 인터넷을 통해 업무상 연락을 주고받을 수 있는 중요한 도구입니다. 이메일은 회사 내부 뿐만 아니라 외부 협력사 그리고 고객과의 소통을 가능하게 하는 통로로 활용되고 있습니다. 이메일의 높은 활용도 때문에 공격자들은 주로 이메일을 통해 해킹을 시도하고 있습니다.

정교하게 만들어진 악성 이메일은 가짜임을 구분하기 어려우며, 실수로 악성 이메일의 첨부파일을 다운로드하면 악성프로그램에 감염될 수 있습니다. 따라서 업무상 이메일을 사용할 때 보안 사고가 일어나지 않도록 주의를 기울일 필요가 있습니다.



외부에 공개되는 기업 정보 관리 필요



최근 특정 회사를 목표로 오랜 시간에 걸쳐 공격을 시도하는 'APT 공격'이 유행하고 있습니다. 공격자들은 인터넷에 공개된 회사 웹사이트 또는 SNS 계정에서 수집한 회사에 관한 정보를 공격에 활용합니다. 따라서 인터넷 상에 회사 정보가 얼마나 공개되어 있는지 파악하고 관리해야 합니다. 언제든지 공개되어

있는 접근경로를 통해서 언제나 공격자의 침입이 일어날 수 있음을 주의해야 합니다. 특히 외부와의 접촉이 많은 고위 간부, 인사, 영업 직무 담당자의 경우 더욱 공격에 주의할 필요가 있습니다.

관리가 필요한 정보

공격자는 회사 공식 웹 사이트, SNS 계정, 또는 언론보도 등 공개된 정보를 통해 정보를 수집하여 공격을 시도할 수 있습니다.



회사에 관한 정보

- 조직 현황
- 주요 사업
- 사무실 및 영업소 주소
- 부서별 연락처 등

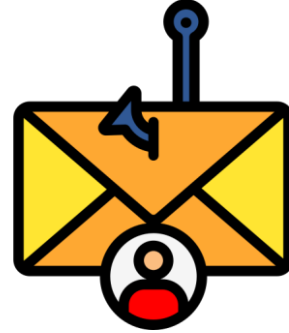


임직원에 관한 정보

- 임직원 이름
- 임직원 직책 및 소속
- 연락처 및 메일주소

사칭 및 사기 이메일에 속지 않기

공격자들은 회사 담당자를 속이기 위해 겉으로 보기에 판단하기 어려운 가짜 이메일을 보냅니다. 주로 정부 기관, 협력사 또는 포털사이트 운영자를 사칭합니다. 보통 이메일을 받는 사람의 정보를 알고 있는 경우가 많으므로 업무상 관련이 있는 기관이나 사람을 사칭하여 이메일을 보내기도 합니다. 사칭 이메일을 받은 담당자는 일상적인 업무 연락이라 생각하여 이메일을 믿게 될 가능성이 매우 높습니다. 최근에는 거래처를 사칭한 가짜 이메일에 속아 돈을 송금하는 '이메일 사기'도 많은 문제가 되고 있습니다.



사칭 이메일 사례

가짜 이메일주소 생성 예시

사칭 이메일의 주소를 정상 주소와 유사하게 만들어 속게끔 유도하는 경우가 많습니다. 이메일 주소를 면밀히 확인하여 가짜 이메일 주소가 아닌지 확인해야 합니다.

유형	예시
중간 철자 삭제	(정상) widgetspo@freemail.com (변조) widgetpo@freemail.com
숫자 재배치	(정상) acmepof868@freemail.com (변조) acmepof686@freemail.com
도메인 변경	(정상) 000@daum.net (변조) 000@daurn.net (정상) 000@naver.com (변조) 000@navor.com
글자 변환	(정상) sales@gmail.com (변조) sales@gmail.com 소문자 l을 대문자 l로 바꿈, 글꼴 크기를 키워서 확인해보면 구분 가능 비슷한 예로 영문자 O와 숫자 0을 혼동하게 하는 사례도 존재

사칭 및 사기 이메일에 속지 않기

공공기관 사칭

공공기관을 사칭하여 특정 자료를 요구하거나, 이메일에 첨부된 링크 또는 파일을 클릭하게 하는 경우가 많습니다. 특히 국세청, 관세청 같이 업무상 자주 연락하는 관공서의 이름으로 발송된 이메일은 방심하기 쉬우므로 더욱 주의해야 합니다. 받은 이메일이 의심되는 경우 해당 공공기관을 통해 내용을 재확인해야 합니다.

공공기관을 사칭한 해킹 메일 예시

실제 2023년에 국세청을 사칭하여 발송된 이메일입니다. 빨간 상자로 표시된 부분의 첨부파일을 다운로드 받으면 개인정보를 탈취하는 가짜 사이트로 연결되었습니다.



<출처: 국세청>

사칭 및 사기 이메일에 속지 않기

포털사이트 운영자 사칭

공격자는 이메일 발송자 이름을 '네이버', 'NAVER 고객센터'와 같이 포털사이트 관리자를 사칭해 해킹 이메일을 보냅니다. 그리고 '(알림)새로운 환경에서 로그인 되었습니다.', '[중요] 회원님의 계정이 이용 제한되었습니다.', '해외 로그인 차단 기능이 실행 되었습니다.' 등 계정에 문제가 생긴 것처럼 제목을 단 메일을 발송하니 주의가 필요합니다.

네이버 운영자를 사칭한 해킹 이메일 예시

링크를 클릭하면 실제와 유사하게 만들어진 가짜 로그인 페이지로 연결됩니다. 가짜사이트에서 계정과 비밀번호를 입력하도록 유도하며, 속아서 입력하면 공격자에게 그 정보가 보내집니다.

회원님의 본인확인 이메일 주소가 삭제되었습니다.

안녕하세요 김 회원님.

회원님의 **본인확인 이메일 주소가 삭제되어** 해당 내역을 안내해 드립니다.

본인확인 이메일 주소 삭제에 따른 안내

변경 일시 2021-09-09(금) 11:55

변경 방법 **내정보>회원정보>연락처 수정**

회원님이 직접 본인확인 이메일 주소를 삭제한 적이 없는데 이 메일을 받았다면 다른 사람에 의해 본인확인 이메일 주소가 삭제되었을 수 있습니다. 다른 사람이 내 회원정보에 접근한 것은 아닌지 점검해주세요.

더불어 본인확인 이메일 주소는 아이디, 비밀번호 찾기 등 본인확인이 필요한 경우 또는 비밀번호 변경 등 보안과 관련된 알림을 받을 때 사용되니 꼭 최신 정보로 업데이트해주세요.

자세한 내용은 **도움말**을 참고해 주세요.

본인확인 이메일 주소 등록하러 가기>

링크 클릭 시 계정입력을 유도하는
피싱 사이트로 연결

<출처: 국가정보원 보도자료(23.05.25) '국정원, 국내 '포털사이트' 사칭한 北 해킹공격 주의 촉구'의 자료를 재구성>

사칭 및 사기 이메일에 속지 않기

공격자는 자신이 포털사이트 운영자임을 믿게 하기 위해 포털사이트 공식 이메일 주소와 비슷한 가짜 주소를 사용해 사칭 이메일을 보내므로 주의하여야 합니다.

구분	공식 이메일주소	사칭 이메일주소 예시	
네이버	네이버	account_noreply@navercorp.com	account_norply@naver <u>cop</u> .com
	네이버 고객센터	help@help.naver.com	help@helpnaver.com
	네이버 메일	navermail_noreply@navercorp.com	<u>no-reply</u> @navecorp.com
다음 카카오	카카오	noreply@kakaocorp.com	noreply@kakaocrop. <u>net</u>
	다음 메일	notice-master@daum.net	notice-master@daum. <u>nat</u>
	카카오 메일	noreply_kakaomail@kakao.com	noreply- <u>master</u> @kakao.com

네이버 로그인 화면과 동일하게 만들어진 피싱사이트의 예시

로그인을 유도하는 피싱사이트는 실제와 동일한 모습으로 만들어져 있어 진짜인지 판단하기 어렵습니다. 주소창의 주소 또한 공식 주소와 유사하게끔 만들어져 더욱 헛갈리기 쉽습니다.

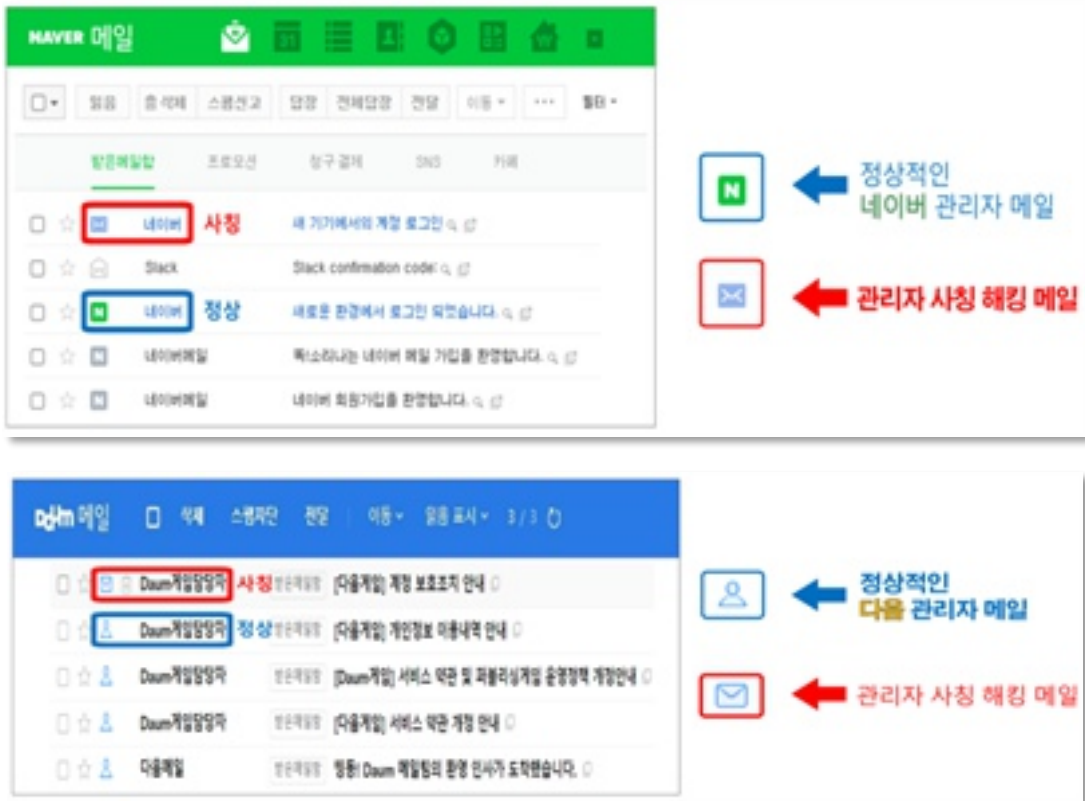


<출처: 국세청 보도자료(23.1.17) '국세청 사칭, 이메일에 속지마세요'의 자료를 재구성>

사칭 및 사기 이메일에 속지 않기

해킹 이메일 식별방법

네이버와 다음에서는 공식 이메일을 받은 경우 특별한 아이콘을 표시해 사칭메일을 구분할 수 있도록 하고 있습니다.



<출처: 국가정보원>

사칭 및 사기 이메일에 속지 않기

무역 사기 이메일 사례

최근 유행하는 '무역 사기 이메일'은 거래처의 이메일주소와 유사한 가짜 주소를 사용하거나, 실제로 거래 상대방을 해킹하여 피해자에게 사기 이메일을 보내는 수법입니다. 주로 거래기업끼리 주고받는 이메일을 오랫동안 지켜보다, 거래 과정 중간에 무역대금을 송금받는 계좌가 바뀌었으니 다른 계좌로 대금을 보내라는 방식으로 송금을 유도합니다. 정교한 방식으로 공격을 수행하므로 사기를 인지하지 못하는 경우가 많아 피해가 확산하고 있습니다.

최근 5년간 (2016~2020) 국내 무역회사 대상 외환 사기거래 (금융감독원)



피해 건수 **2582건**

총 피해액 **1379억원**

최근 무역 사기 이메일 피해사례

◇ 발생시기: 2022년 3월

◇ 피해금액: US\$ 54,000

◇ 발생국가: 영국

국내 기업 A사는 영국 현지의 거래 업체이며, 대금 송금을 진행하는 과정에서 이메일 사기를 당했다.

20년 전부터 거래를 지속해 온 영국 현지 공급업체 B사와의 거래조건은 발주 시 전신환 선송금이였다. 금년 3월경 기존과 마찬가지로 A사에서 B사에 발주를 진행하고 PI 및 대금 계좌를 받아 주문 대금을 송금했다. 그런데 알고 보니 이메일이 해킹된 사실을 미처 인지하지 못한 채 해커가 보낸 변경 계좌로 대금을 송금한 것이였다.

A사는 B사로 위장한 해커들로부터 현지 은행과의 문제로 대금 수취가 불가능하다며 재송금 요청을 받았고 해커로부터 전달받은 기 송금 건에 대한 반환 전문(위조 문서로 추측됨) 확인 후 추가 주문 금액까지 합쳐 새로운 계좌로 일괄 송금하였다. 이후 해커와의 연락은 끊기고 진짜 B사와의 유선 통화로 피해 사실을 인지하게 되었다.

<출처: KOTRA>

사칭 및 사기 이메일에 속지 않기

무역 사기 이메일 대응방법



이메일로 계좌정보를 변경하겠다는 이메일을 수신한 경우
대금 송금 전, 반드시 유선 및 화상통화를 통해 이중 확인



해외기업 소재지와 대금수취은행 소재지가 상이한 경우 주의
(예: 몽골기업과 거래 중 대금은 홍콩 은행으로 송금 요청을 받은 경우)



피해 발생을 인지한 경우 가장 먼저 은행에 지급정지를 요청한 뒤,
해외에서도 수사가 진행될 수 있도록 상대 기업에 협조 요청

수상한 첨부파일 및 링크 클릭하지 않기

악성 이메일에 첨부된 파일을 다운로드 받거나, URL을 클릭하는 경우 악성프로그램에 감염될 수 있습니다. 특히 악성 URL을 클릭하는 경우 악성프로그램을 유포하는 사이트로 강제로 접속되어 사용자 PC에도 악성프로그램이 설치될 수 있습니다. 공격자는 이를 통해 회사 PC에 저장된 중요 정보를 외부로 유출하거나, PC의 자료를 모두 사용할 수 없게 만든 뒤 정상화해주는 대가로 금전을 요구하는 협박성 공격인 랜섬웨어 공격을 수행할 수 있습니다.

첨부파일의 경우 문서 파일의 '매크로 바이러스'가 많이 활용되는 수법이므로 '오피스' 편을 참고하여 방어 조치를 할 것을 권고합니다.

리디렉션의 경우 브라우저 설정 상 강제로 리디렉션이 되지 않도록 조치할 수 있으므로 '웹 브라우저' 편을 참고하여 방어조치를 할 것을 권고합니다.

외부 이메일을 통한 업무자료 송수신 자제

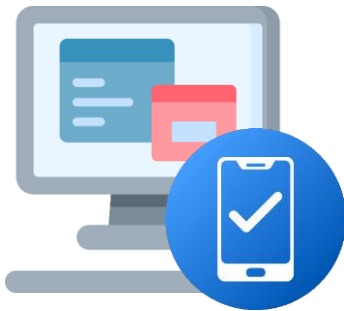
혹시 포털사이트에서 제공하는 이메일을 통해 회사 업무를 수행하고 계십니까? 구글, 네이버, 다음과 같은 포털 사이트에서 제공하는 이메일 서비스는 개인용으로 사용하기에는 좋지만, 회사 업무에 사용하는 것은 위험할 수 있습니다. 포털사이트 계정은 외부에서도 자유롭게



접근이 가능하기 때문에 공격자의 표적이 되기 쉽습니다. 계정이 해킹당한 경우 이메일에 남아있는 중요한 자료가 유출될 가능성이 있고, 이렇게 유출 사고가 발생하더라도 그 유출 사실과 경위를 확인하기 매우 어렵습니다. 따라서 업무용 회사 이메일이 있다면 이를 통해서 이메일을 주고받기를 권장합니다.

회사 내부에서 사용하는 자체 이메일이 없어 부득이하게 포털 사이트 이메일을 사용해야 하는 경우, 자신의 포털사이트 계정을 안전하게 관리해야 할 필요가 있습니다.

포털사이트 계정 보안하기



2단계 인증



해외 로그인 차단

네이버

2단계 인증 설정하기

2단계 인증은 사용자가 로그인을 시도하는 경우 휴대전화를 통해 본인이 로그인을 수행하고 있음을 인증하는 기술입니다. 이를 통해 계정정보가 노출되어도 다른 사람이 로그인할 수 없도록 보안 조치를 할 수 있습니다.

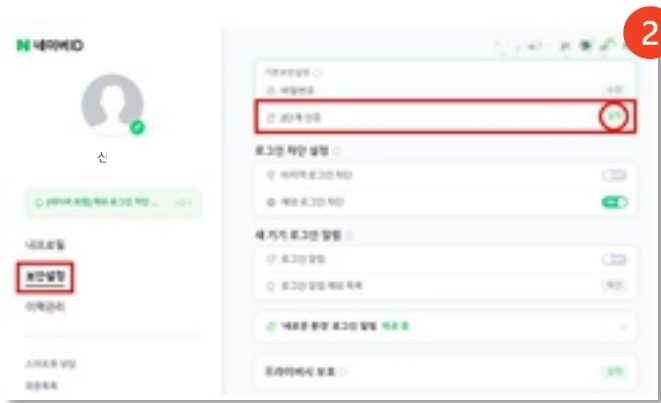
1 [로그인 후 별명 옆의 '네이버ID' 클릭]



2 ['보안설정' 클릭 후 '2단계 인증 설정' 클릭]

3 [비밀번호 재입력 후 인증 알림을 받을 수 있는 기기 선택 후 다음 클릭]

4 [인증 수행 후 설정 완료]

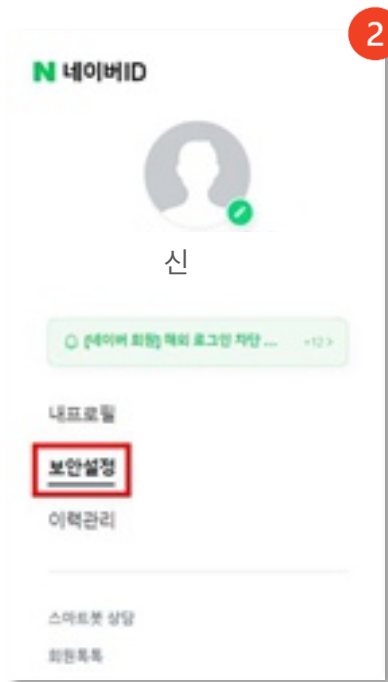


네이버

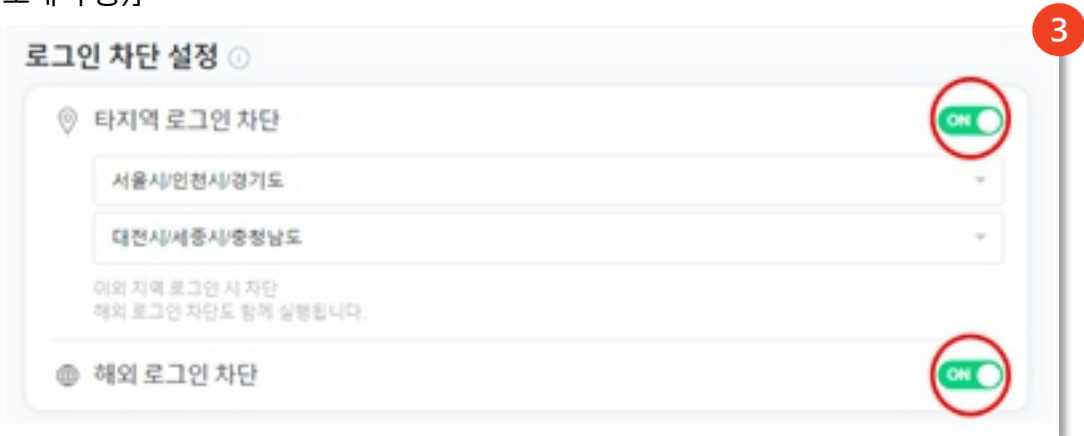
해외로그인 차단

해외에서 로그인을 시도하는 경우 공격 시도일 가능성이 높습니다. 따라서 해외에서는 로그인을 할 수 없도록 차단하는 기능을 활성화해야 합니다.

- 1 [로그인 후 별명 옆의 '네이버ID' 클릭] *사진 생략
- 2 ['보안설정' 클릭]



- 3 ['로그인 차단 설정'] > ['해외 로그인 차단' 활성화] > [필요시 '타지역 로그인 차단 (국내 특정 지역에서만 로그인을 허용하는 기능)' 활성화 후 로그인 가능 지역 설정(사무실 소재지 등)]



다음(카카오)

2단계 인증 설정하기

- 1 [로그인 후 메인화면 회원정보창에서 '계정 닉네임' 클릭]



- 2 ['계정 관리' 페이지에서 '계정 보안' 메뉴 클릭] > ['정보 보호'-'2단계 인증'의 '설정하기' 클릭]



- 3 [2단계 인증] > ['카카오톡' 또는 '전화번호' 중 선택하여 인증 후 설정 완료]



다음(카카오)

해외로그인 차단

- 1 [메인화면 회원정보창에서 계정 닉네임 클릭] *사진 생략
- 2 ['계정 관리' 페이지에서 '계정 보안' 메뉴 클릭]



- 3 [비밀번호 재입력 후 인증 알림을 받을 수 있는 기기 선택 후 다음 클릭]



- 4 ['정보 보호'->'국가별 로그인 제한'의 '설정하기' 클릭] > [비밀번호 입력] > ['국가별 로그인 제한' 활성화]



구글

2단계 인증 설정하기

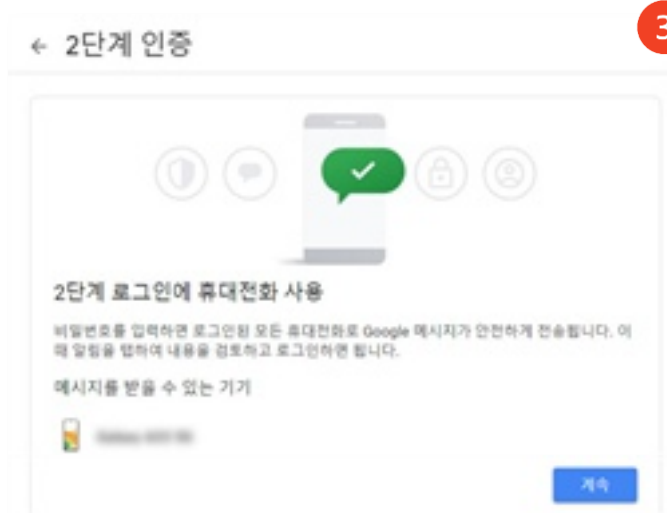
- 1 ['Google 계정' 접속] > ['탐색' 패널에서 '보안' 클릭]



- 2 ['Google에 로그인'에서 2단계 인증 - 시작하기를 선택]



- 3 [비밀번호 입력] > [인증에 사용할 휴대전화 등록]

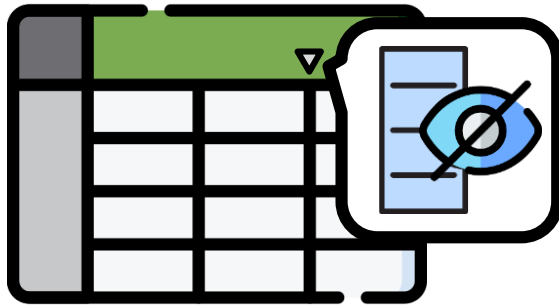


이것만은 지키자!

행동수칙

오피스 편

1



엑셀 숨기기 기능을 사용하지 않아요!

엑셀 숨기기 기능은 내용을 삭제하는 것이 아닙니다. 단지 파일 내에서만 '보이지 않도록 하는' 기능이기에 때문에, 숨기기 기능을 함부로 사용할 경우 회사의 중요 정보가 노출될 수 있습니다.

이번 장에서는 회사에서 사용하는 문서작업 도구인 오피스 프로그램의 보안 설정을 안내합니다. 대표적인 오피스 프로그램인 Microsoft의 Word, Excel, PowerPoint와 한글과컴퓨터의 한글, 한셀, 한쇼의 보안 기능을 다룹니다.

☑ 꼭 정품 오피스 프로그램을 사용해야 할까요?

오피스 프로그램을 정품이 아닌 불법 복제본으로 사용하면 바이러스나 악성코드에 감염될 위험이 있습니다. 또한 불법 복제본을 사용하는 것은 저작권 침해 행위로 법적 처벌을 받을 수 있으며, 판매사에게 불법 프로그램 사용에 대한 손해배상 책임을 져야할 수 있기 때문에 꼭 정품을 사용하시기 바랍니다.

Microsoft Office는 Microsoft 공식 사이트에서 구독 형식으로 구매할 수 있습니다. 5인 이하 소규모 사업장이라면 비교적 저렴한 가격으로 Word, Excel, PowerPoint를 사용할 수 있습니다.

<https://www.microsoft.com/ko-kr/microsoft-365/business> - Microsoft 공식 사이트

가이드라인에서 다루는 제품 확인하기



▲ Word 2021



▲ Excel 2021



▲ PowerPoint 2021



▲ 한글 2022



▲ 한셀 2022



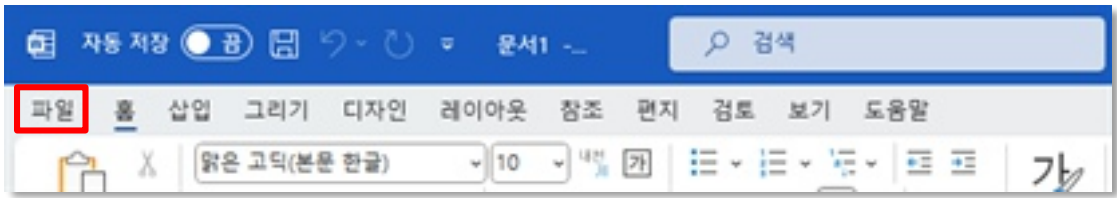
▲ 한쇼 2022

워드(Word)

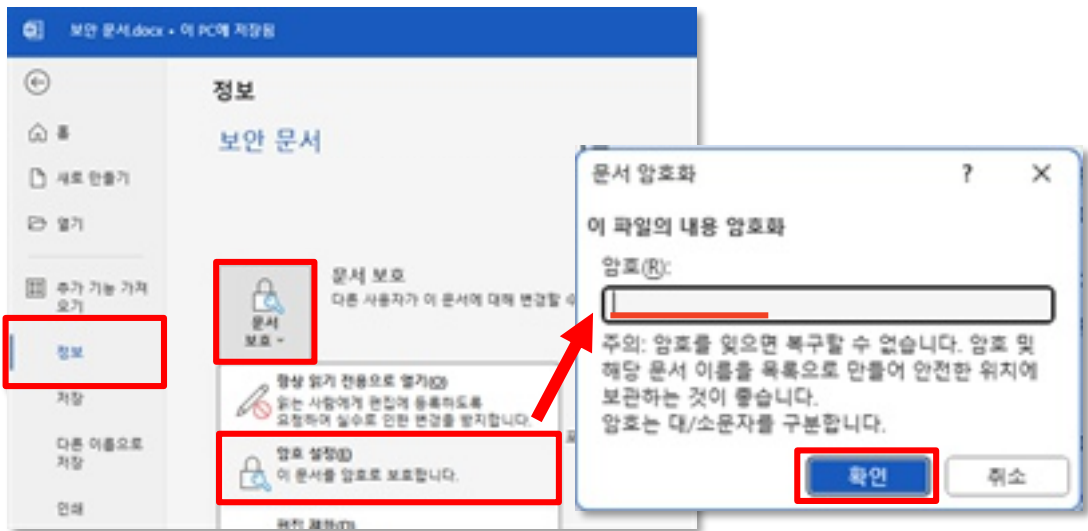
1. 파일 보안 설정하기

| 파일 암호화 기능 사용하기

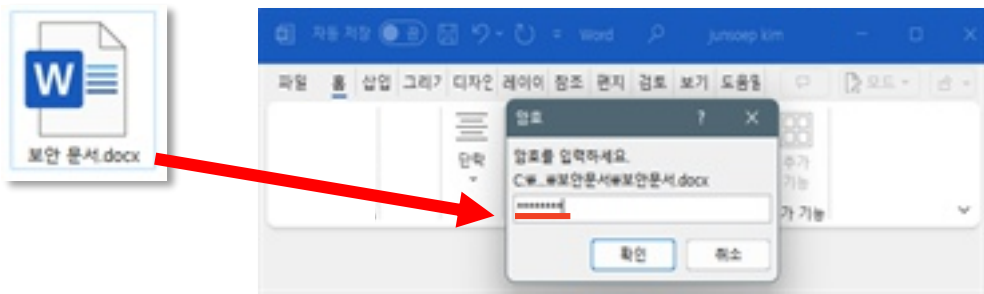
- ① [좌측 상단 '파일' 클릭]



- ② ['정보' 탭 클릭] > ['문서 보호' 클릭] > ['암호 설정' 클릭] > [암호 입력] > ['확인' 클릭]



- ③ [보호 파일 실행] > [암호 입력]



엑셀(Excel)

1. 파일 보안 설정하기

| 파일 암호화 기능 사용하기

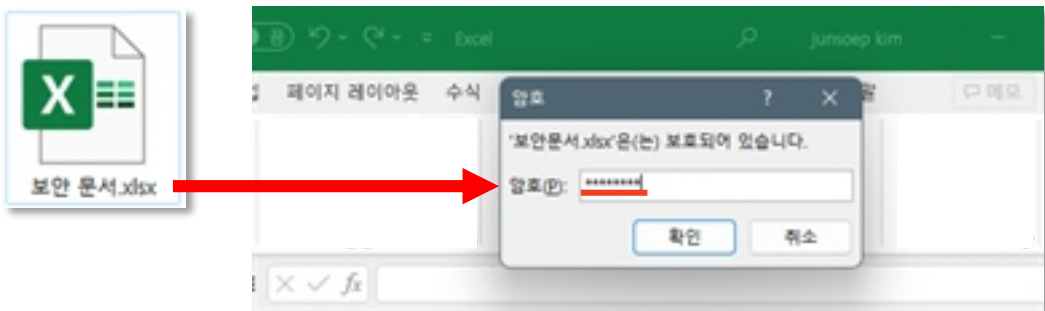
- 1 [좌측 상단 '파일' 클릭]



- 2 ['정보' 탭 클릭] > ['문서 보호' 클릭] > ['암호 설정' 클릭] > [암호 입력] > ['확인' 클릭]



- 3 [보호 파일 실행] > [암호 입력]



엑셀(Excel)

2. 매크로 보안 설정하기

| 매크로 사용 안함 설정하기

- 1 [좌측 상단 '파일' 클릭]



- 2 [좌측 하단 '옵션' 클릭]

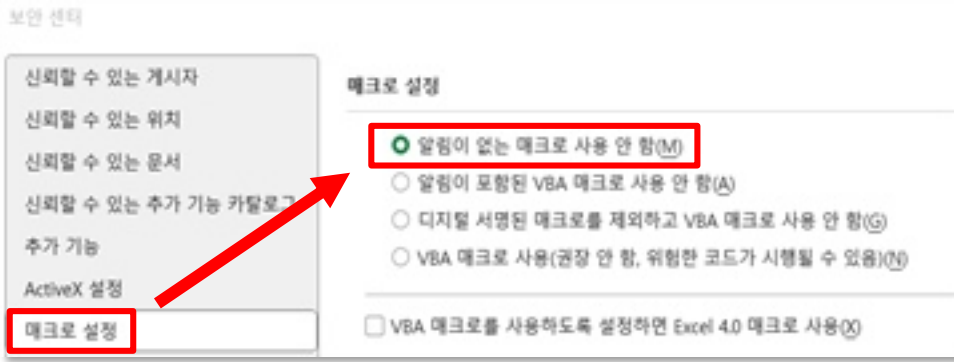


- 3 ['보안센터' 탭 클릭] > ['보안 센터 설정' 클릭]



엑셀(Excel)

- 4 ['매크로 설정' 탭 클릭] > ['알림이 없는 매크로 사용 안 함' 선택]



매크로 기능 사용하지 않기

매크로 바이러스란 문서파일에 매크로 언어로 된 악성코드를 삽입한 형태의 바이러스입니다. 문서 파일을 열었을 때 자동으로 악성기능이 실행됩니다. 바이러스를 통해 회사의 중요 정보를 탈취하거나 시스템에 손상을 입힐 수 있습니다. 따라서, 프로그램에서 제공하는 매크로 보안 설정 기능을 활용하여 바이러스가 실행되지 않게 해야합니다.

파워포인트(PowerPoint)

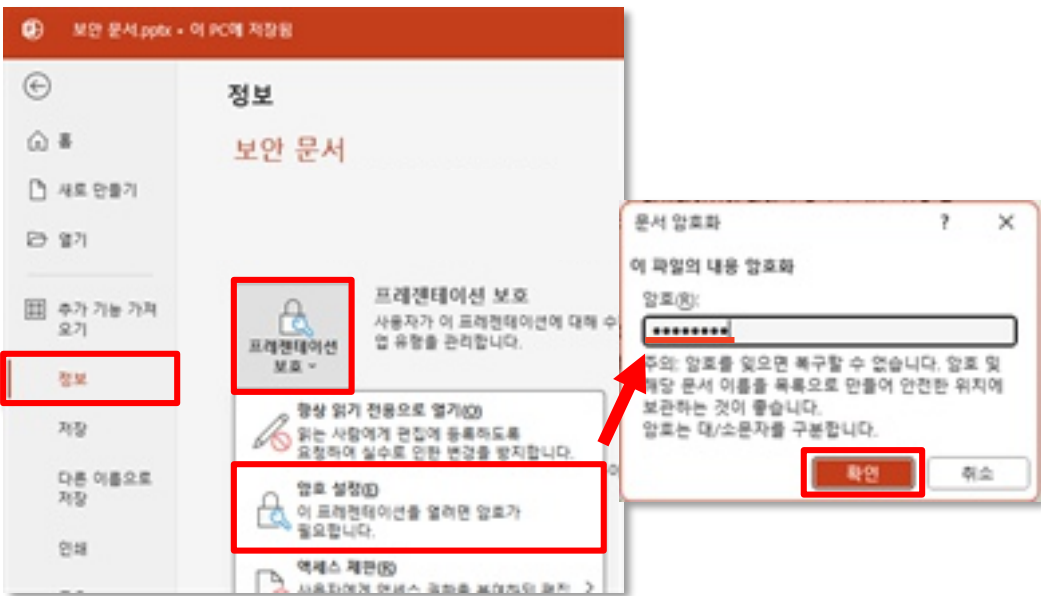
1. 파일 보안 설정하기

| 파일 암호화 기능 사용하기

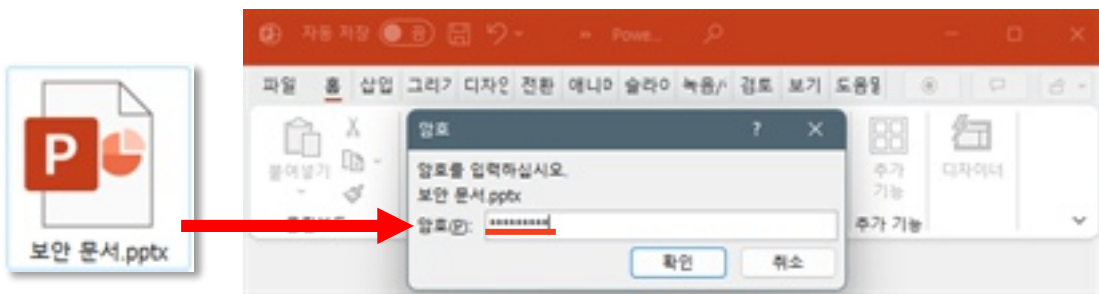
- 1 [좌측 상단 '파일' 클릭]



- 2 ['정보' 탭 클릭] > ['문서 보호' 클릭] > ['암호 설정' 클릭] > [암호 입력] > ['확인' 클릭]



- 3 [보호 파일 실행] > [암호 입력]



파워포인트(PowerPoint)

2. 매크로 보안 설정하기

| 매크로 사용 안함 설정하기

- 1 [좌측 상단 '파일' 클릭]



- 2 [좌측 하단 '옵션' 클릭]



- 3 ['보안센터' 탭 클릭] > ['보안 센터 설정' 클릭]



파워포인트(PowerPoint)

- 4 ['매크로 설정' 탭 클릭] > ['알림이 없는 매크로 사용 안 함' 선택]



매크로 기능 사용하지 않기

매크로 바이러스란 문서파일에 매크로 언어로 된 악성코드를 삽입한 형태의 바이러스입니다. 문서 파일을 열었을 때 자동으로 악성기능이 실행됩니다. 바이러스를 통해 회사의 중요 정보를 탈취하거나 시스템에 손상을 입힐 수 있습니다. 따라서, 프로그램에서 제공하는 매크로 보안 설정 기능을 활용하여 바이러스가 실행되지 않게 해야합니다.

파워포인트(PowerPoint)

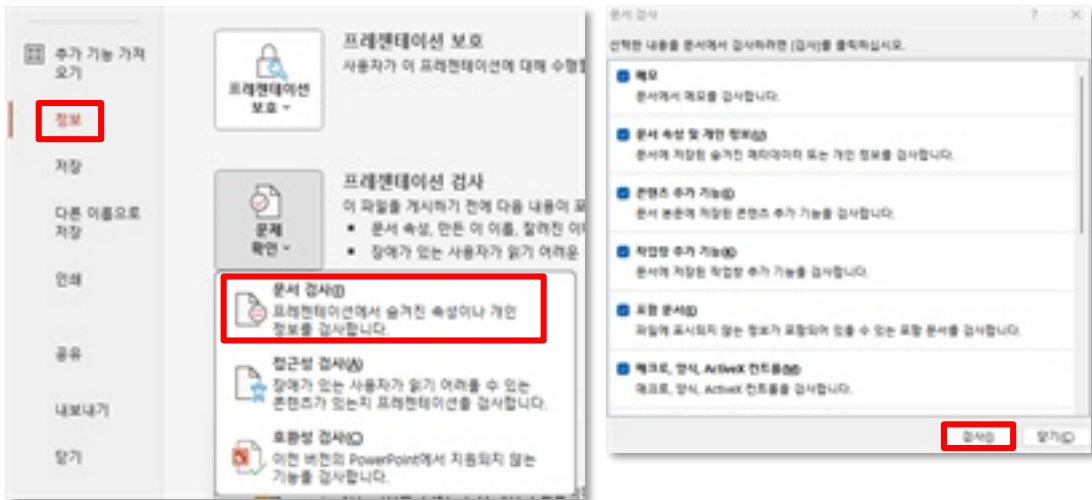
3. 파워포인트 프레젠테이션 보호 확인하기

| 문서 검사하기

- 1 [좌측 상단 '파일' 클릭]



- 2 ['정보' 탭 클릭] > ['문제 확인' 클릭] > ['문서 검사' 클릭] > [검사 수행 후 결과 확인]



한글

1. 파일 비밀번호 설정하기

| 파일 암호화 기능 사용하기

- 1 [상단바 '보안' 탭 클릭] > [문서 암호 설정' 클릭]



- 2 [열기/쓰기 암호 입력]



중요 정보가 포함된 문서에는 비밀번호설정하기

회사 기밀과 같은 중요한 문서 파일은 다른 사람이 함부로 읽을 수 없도록 조치해야 합니다. 이를 위해 문서 프로그램 내의 비밀번호 설정 기능을 사용할 수 있습니다.

한글

새 문서 자동 비밀번호 설정하기

- 1 [상단바 '도구' 탭 클릭] > ['환경설정' 클릭]



- 2 ['파일' 탭 클릭] > ['새 문서를 저장할 문서 암호 설정' 선택]



- 3 ['보안센터' 탭 클릭] > ['보안 센터 설정' 클릭]

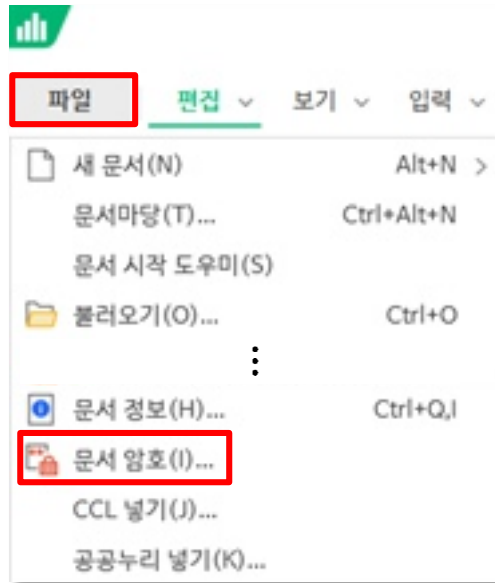


한셀

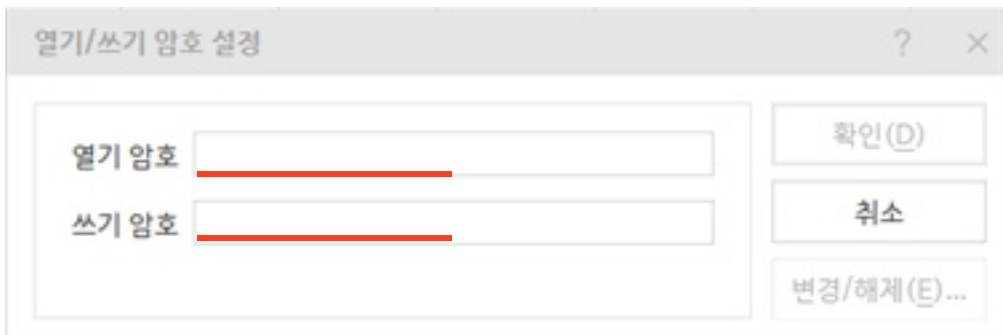
1. 파일 보안 설정하기

| 파일 암호화 기능 사용하기

- 1 [좌측 상단 '파일' 클릭] > ['문서 암호' 클릭]



- 2 [열기/쓰기 암호 입력]



중요 정보가 포함된 문서에는 비밀번호 설정하기

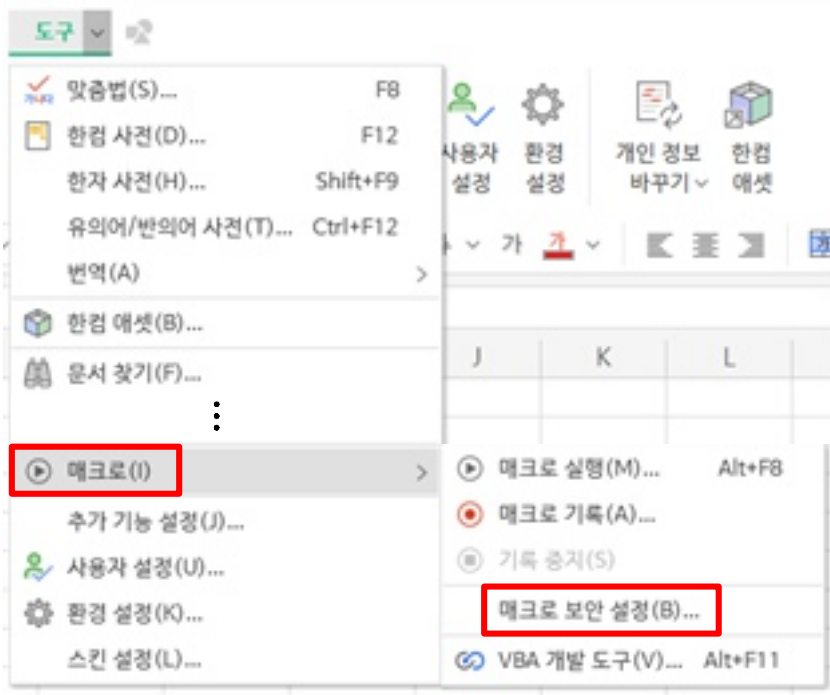
회사 기밀과 같은 중요한 문서 파일은 다른 사람이 함부로 읽을 수 없도록 조치해야 합니다. 이를 위해 문서 프로그램 내의 비밀번호 설정 기능을 사용할 수 있습니다.

한셀

2. 매크로 보안 설정 높이기

| 매크로 실행 안함 설정하기

- 1 [상단바 '도구' 클릭] > ['매크로' 클릭] > ['매크로 보안 설정' 클릭]



- 2 ['보안 수준' 탭 클릭] > [보안 수준 '매우 높음' 선택] > ['설정' 클릭]



한쇼

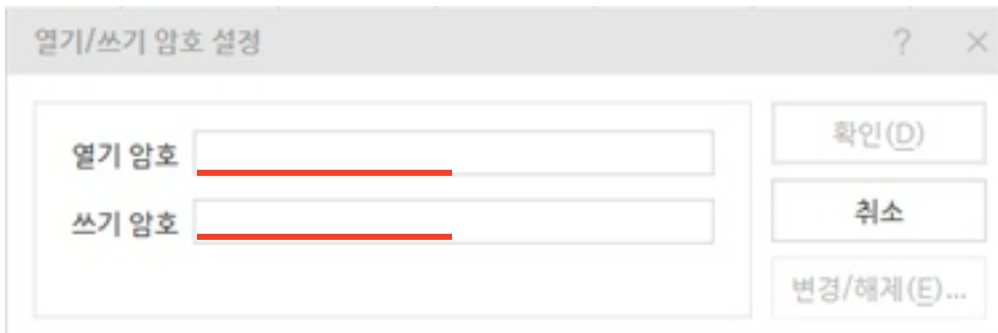
1. 파일 비밀번호 설정하기

| 파일 암호 기능 사용하기

- 1 [좌측 상단 '파일' 클릭] > ['문서 암호' 클릭]



- 2 [열기/쓰기 암호 입력]



이번 장에서는 대표적으로 사용되는 메신저인 카카오톡의 PC 버전에서 할 수 있는 보안 설정에 대해 다룹니다. 카카오톡에서 어떤 보안 설정을 할 수 있는지, 이러한 보안 설정을 통해 어떤 효과를 낼 수 있는지 알아보겠습니다.

☑ 카카오톡 잠금모드를 꼭 활성화해야 하나요?

카카오톡 잠금 기능을 활성화하지 않을 경우, 화면에 카카오톡 대화방이 그대로 노출될 수 있습니다. 잠시 자리를 비운 사이 누군가 대화방을 몰래 확인한다면, 사적으로 주고받은 대화 내용뿐만 아니라 업무상 주고받은 데이터 또한 유출될 가능성이 있습니다. 개인의 사생활과 영업 비밀을 보호하기 위해서 카카오톡 대화방은 최대한 노출이 되지 않아야 합니다.

☑ 회사 PC로 메신저를 사용해도 될까요?

회사 PC로 메신저 애플리케이션을 사용하는 경우, 사내 규정과 정책을 준수해야 합니다. 회사는 필요에 따라 대화 내용을 확인할 수 있고, 이는 비밀번호 설정 여부와 관계없이 회사의 자산을 확인하는 것이므로 법적인 문제가 발생하지 않습니다. 메신저를 통해 전송한 메시지나 파일에 회사 비밀이 포함되어 있을 경우 법적 책임을 지게 될 수 있어 주의하여야 합니다.

가이드라인에서 다루는 제품 확인하기



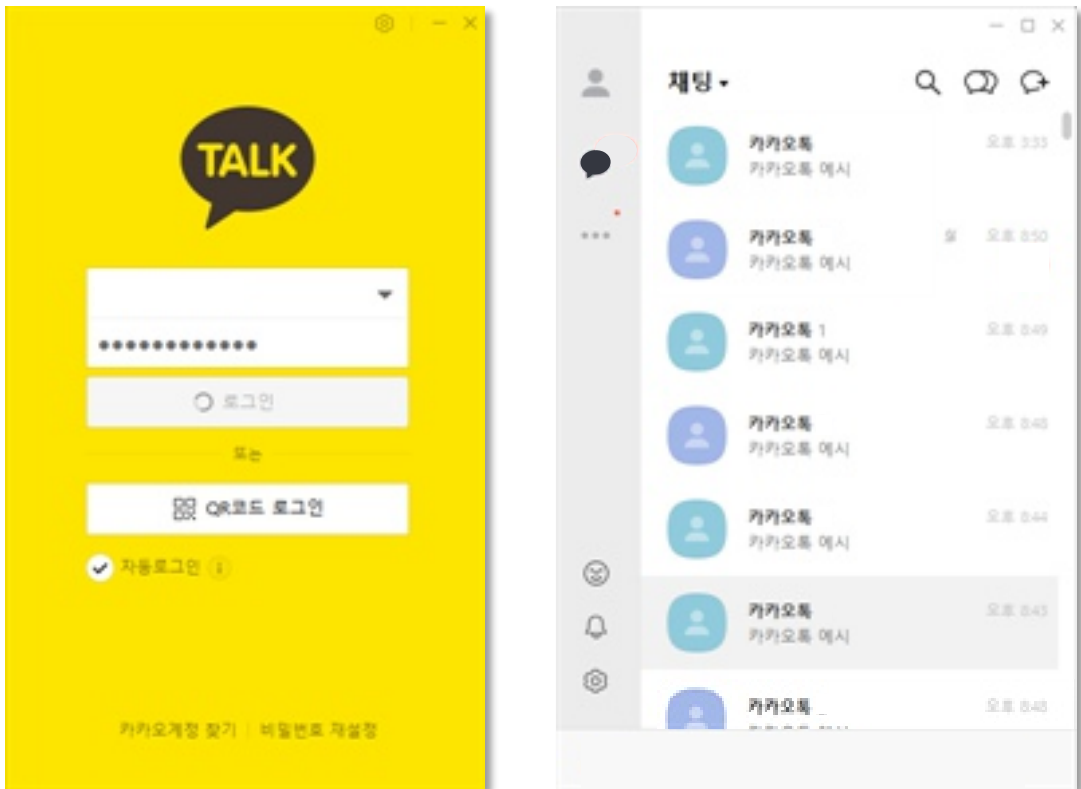
▲ 카카오톡

카카오톡

1. 잠금 모드 설정하기

기본적으로 PC 버전 카카오톡은 팝업 창을 최소화하거나 컴퓨터가 절전 모드에 들어갈 경우 잠금 모드가 활성화됩니다. 이 경우 비밀번호가 설정되어 있지 않다면 카카오톡 대화방이 그대로 노출될 수 있습니다.

▶ 잠금 모드의 비밀번호가 설정되어 있지 않은 경우 예시



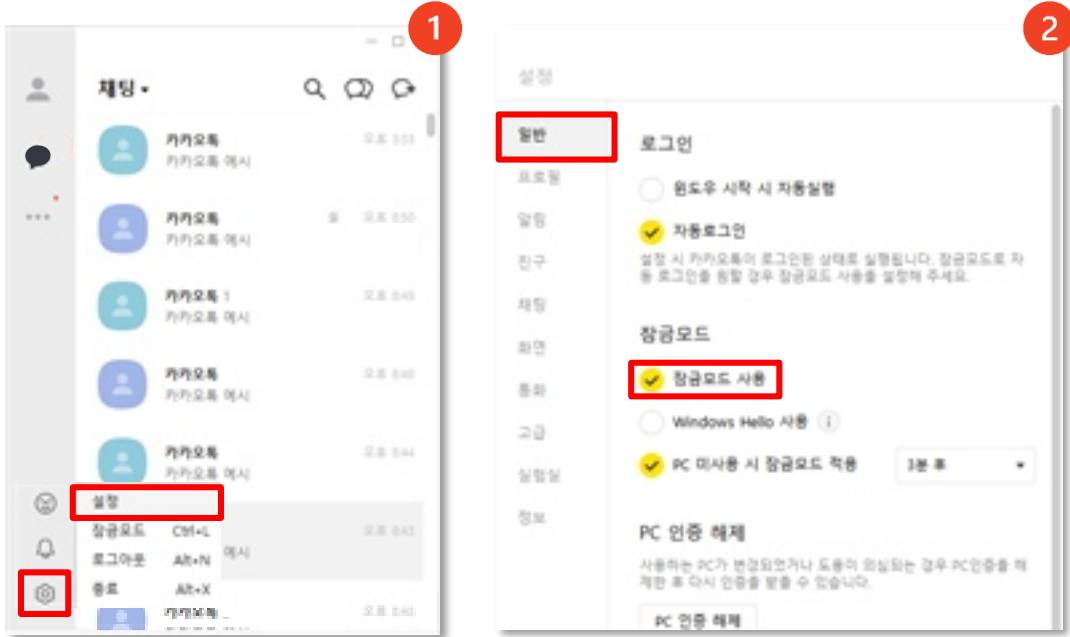
카카오톡 대화방이 노출되어 있다면?

카카오톡 대화방이 그대로 노출되어 있는 상태라면 잠시 자리를 비운 사이 누군가 카카오톡 메신저를 확인해 회사 업무 데이터를 유출 할 수 있습니다. 또한, 개인의 사생활을 보호하기 위해서라도 카카오톡 대화방은 최대한 노출이 되지 않아야 합니다. 이를 위해 카카오톡 PC 버전에서 제공하고 있는 잠금 모드를 사용해야 합니다.

카카오톡

잠금 모드 활성화하기

- 1 [좌측 하단 '톱니바퀴' 클릭] > ['설정' 클릭]
- 2 ['일반' 탭 클릭] > ['잠금모드 사용' 선택]



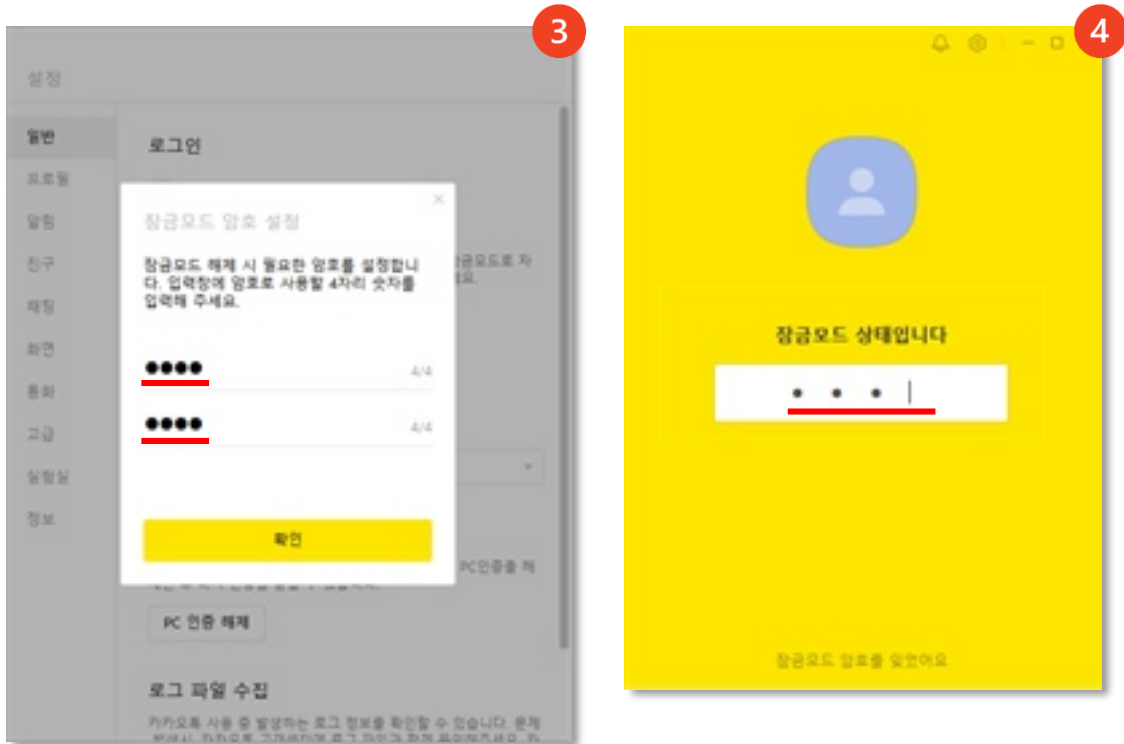
PC 미사용 시 잠금 모드 적용

PC 카카오톡에는 자리를 비우면 자동으로 잠금 모드에 들어가는 'PC 미사용 시 잠금 모드 적용' 기능이 있습니다. 기본적으로 3분 동안 자리를 비우면 잠금 모드가 적용됩니다. 적용 시간은 사용자가 직접 설정할 수 있지만, 장시간 자리를 비웠을 때 발생할 수 있는 사고를 예방하기 위해 3분 이하로 설정하는 것을 권장합니다.



카카오톡

- 3 [잠금모드 4자리 비밀번호 입력]
- 4 [잠금모드 적용 확인]



4자리 비밀번호 사용시 주의사항

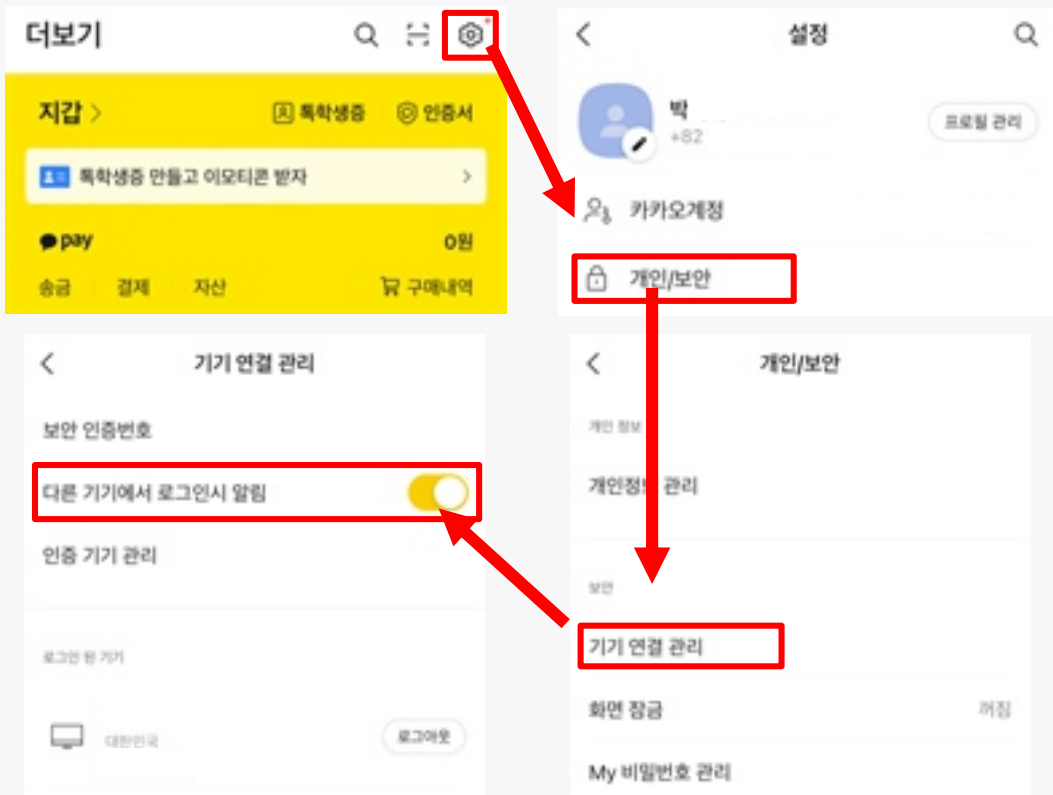
잠금 모드 사용시 비밀번호는 4자리 숫자로 구성됩니다. 이때 '1234', '1111'과 같이 연속되거나 반복되는 비밀번호를 사용하지 않아야 합니다.

카카오톡

PC 로그인 시 모바일 알림 활성화하기

모바일 카카오톡에는 다른 기기에서 로그인을 할 경우 이를 모바일을 통해 알려주는 알림 기능이 있습니다. 해당 기능을 사용하면 PC에서 로그인했을 때 알림 메시지가 모바일 카카오톡으로 전송됩니다.

[모바일 카카오톡 실행] > [우측 하단 '더 보기' 클릭] > [우측 상단 '설정' 클릭] > [개인/보안' 클릭] > [기기 연결 관리' 클릭] > ['다른 기기에서 로그인 시 알림' 활성화]

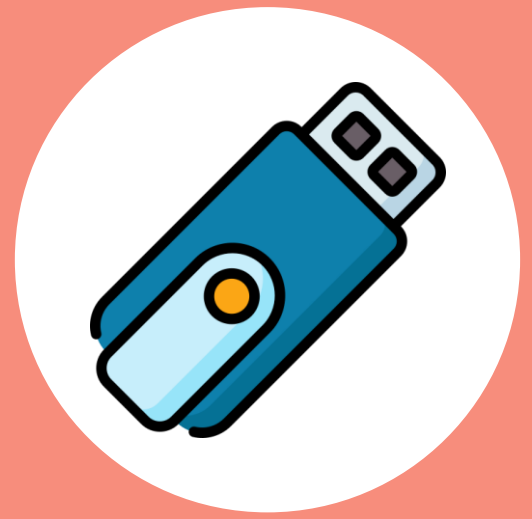


해당 기능을 활성화하면 PC버전 카카오톡 로그인 시 모바일 카카오톡으로 알림이 오는 것을 확인할 수 있습니다.



제2장 임직원 보안수칙

II. 저장매체



i. 시스템 ... 99

1. Windows BitLocker ... 100

ii. 시중 소프트웨어 ... 106

1. SanDisk ... 107



이번 장에서는 회사에서 데이터 저장을 위해 사용하는 저장매체의 보안 설정에 대해서 안내합니다. 이를 위해 Windows에서 제공하고 있는 BitLocker 기능을 통해 저장매체를 안전하게 사용하는 방법에 대하여 다룹니다.

✔ 저장매체에도 보안기능이 있나요?

저장매체에도 보안 기능이 있습니다. 크게 두가지로, Windows 운영체제 기능을 통해 PC에서 보안 설정을 하는 방법과 제조사에서 제공하는 보안 프로그램을 활용하는 방법이 있습니다. 이번 장에서는 PC에서 할 수 있는 보안 설정 방법을 안내합니다.

✔ 회사 안에서만 저장매체를 사용하는데도 보안설정이 필요할까요?

저장매체를 회사 밖으로 들고나가지 않는다고 해도 유출 사고는 발생할 수 있습니다. 실제로 회사 내에서 저장매체를 분실해 회사 기밀문서가 유출되는 사고가 계속 발생하고 있습니다. 이를 막기 위해 중요한 자료를 담고 있는 저장매체에 보안 조치를 해두어야 합니다.

가이드라인에서 다루는 제품 확인하기



▲ Windows BitLocker

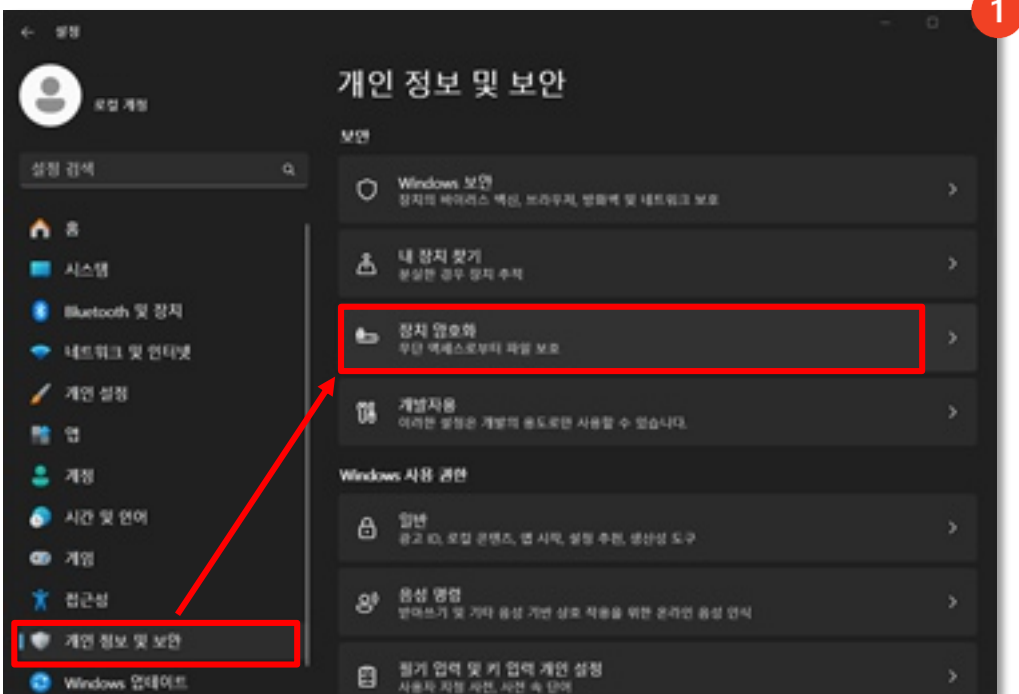
Windows BitLocker

0. 장치 암호화 활성화하기

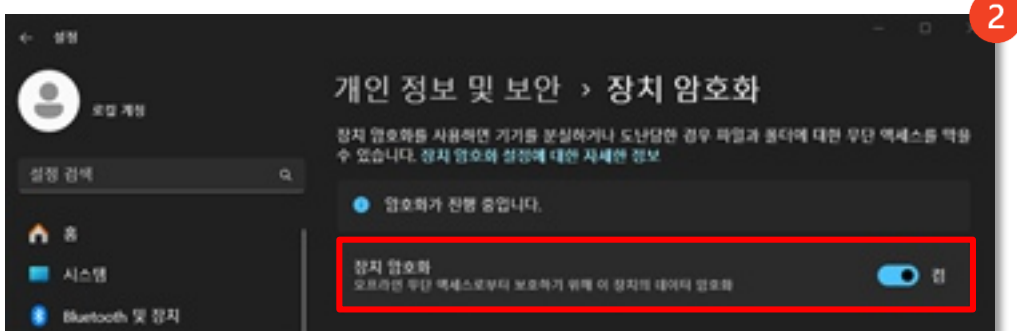
BitLocker 기능을 활성화하기 전, 장치 암호화 기능을 활성화합니다.

I 계정 환경 설정하기

- 1 [설정] > ['개인 정보 및 보안' 클릭] > ['장치 암호화' 클릭]



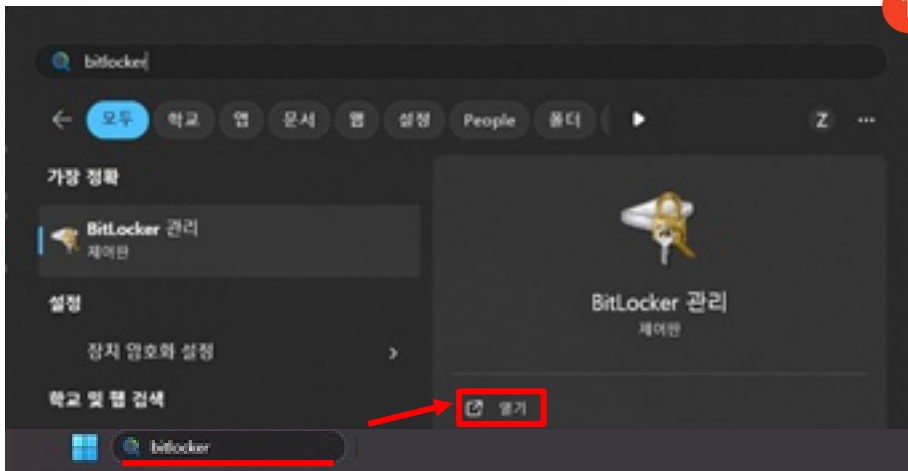
- 2 ['장치 암호화' 활성화]



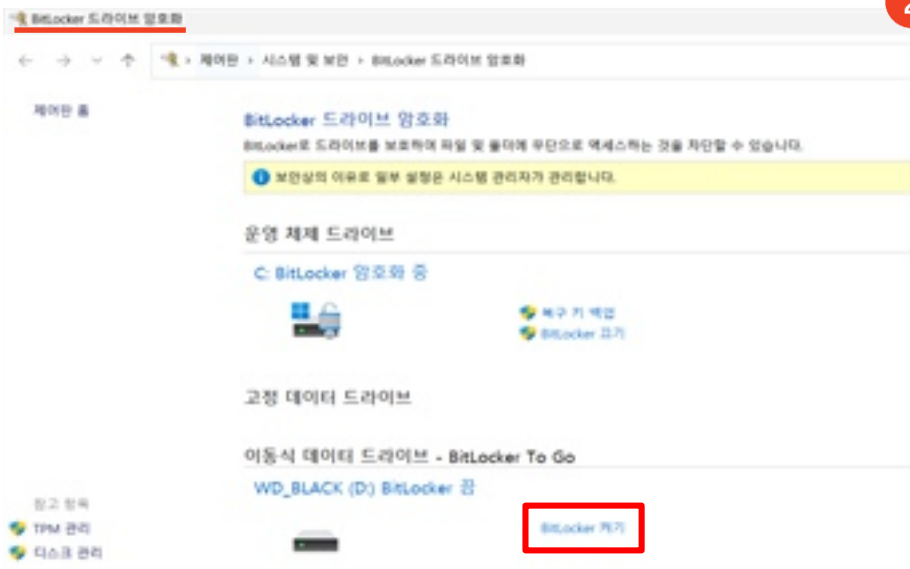
Windows BitLocker

표준 BitLocker 암호화를 활성화하기

1. ['Bitlocker' 검색 및 '열기' 클릭]



2. [BitLocker 드라이브 암호화] > [암호화 대상 드라이브 'BitLocker 켜기' 클릭]



BitLocker, 정보를 안전하게 지켜요!

BitLocker는 저장매체에 저장된 파일을 다른 사람이 접근하지 못하도록 하고, 중요한 데이터가 유출되지 않도록 도와줍니다. BitLocker 기능을 활성화하면 저장매체를 잃어버리는 경우에도 비밀번호가 설정되어 있어 저장매체 내 파일을 안전하게 보호할 수 있습니다.

Windows BitLocker

드라이브(저장매체)의 잠금을 해제할 방법을 선택합니다. 비밀번호 방식과 스마트 카드를 이용한 방식이 있습니다. 아래에서는 비밀번호 방식의 설정 방법을 안내합니다.

- 3 ['암호를 사용하여 드라이브 잠금 해제' 클릭] > [사용할 비밀번호 입력 후 '다음' 클릭]



비밀번호 설정 시 주의점

비밀번호를 사용하여 드라이브 잠금을 해제할 경우, 대/소문자, 숫자, 공백 및 기호를 반드시 포함해야 하며, 사용하는 비밀번호는 쉬운 문자(예: 일렬로 나열된 번호, 같은 번호 반복 등)로 지정하지 않아야 합니다.

Windows BitLocker

- 4 [복구 키 백업 방식 '파일에 저장' 선택] > ['다음' 클릭]



- 5 [사용 용도에 따른 암호화할 드라이브 공간 선택] > ['다음' 클릭]



복구 키를 파일에 저장할 경우 주의점

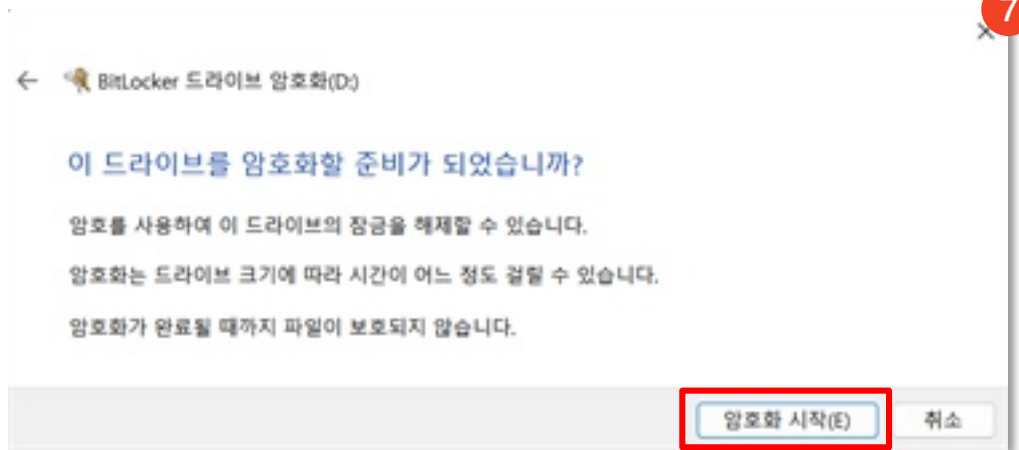
복구 키를 파일에 저장할 경우, 복구 키가 저장된 파일이 유출되지 않도록 각별한 주의가 필요합니다.

Windows BitLocker

- 6 [드라이브 형태에 따라 사용할 암호화 모드 선택] > ['다음' 클릭]



- 7 ['암호화 시작' 클릭]

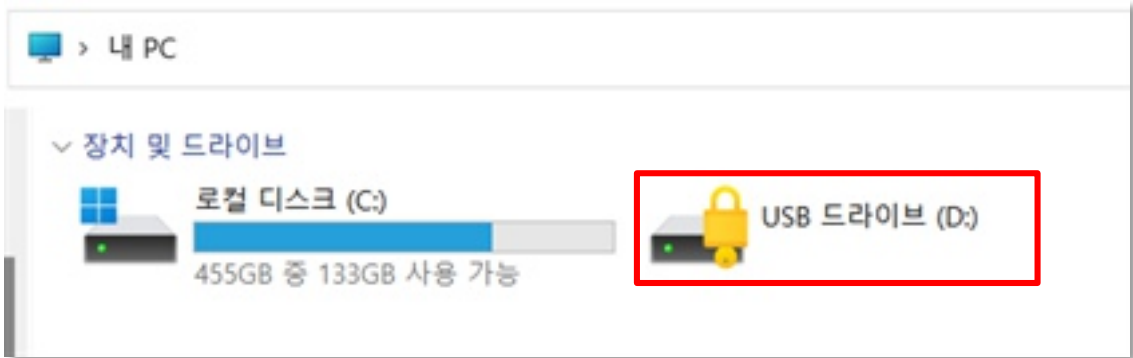


드라이브 암호화 시 소요 시간

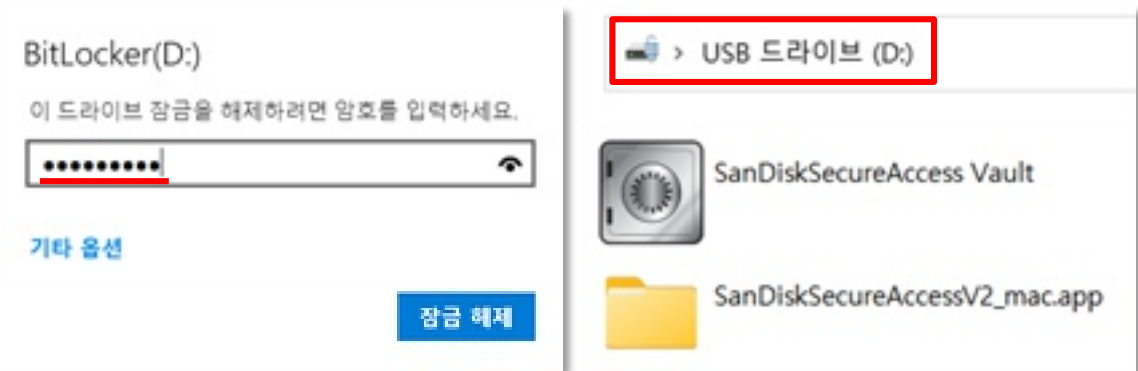
BitLocker를 이용한 드라이브 암호화 시, 저장매체의 용량이 커질수록 암호화에 걸리는 시간도 비례하여 늘어나게 됩니다. 짧게는 몇 분에서 길게는 몇 시간까지 소요될 수 있습니다.

Windows BitLocker

BitLocker 기능이 제대로 활성화되었다면 아래 사진과 같이 저장매체 아이콘에 자물쇠 모양이 생성됩니다.



비밀번호를 입력하여 잠금을 해제할 수 있습니다. 잠금 해제시 저장매체 아이콘이 열린 자물쇠로 변경됩니다.



이번 장에서는 저장매체의 제조사에서 제공하는 보안 기능에 대해서 안내합니다. 이 기능을 통해 저장매체 안의 중요한 파일에 대한 추가적인 보안 설정을 할 수 있습니다. 이번 장에서는 Western Digital 사의 SanDisk USB의 보안 기능인 PrivateAccess를 다룹니다.

✔ PrivateAccess 기능은 SanDisk 제품 외 사용이 불가능한가요?

PrivateAccess 기능은 SanDisk 제품 외에는 실행되지 않습니다. PrivateAccess를 사용할 수 없다면 대신 앞서 소개한 장치 암호화 기능이나 BitLocker 기능을 사용할 수 있습니다. 이외에도 제조사 별로 제공하는 소프트웨어를 통해 보안 설정을 할 수 있습니다.



제조사 명	소프트웨어 명	기능
Western Digital	WD security	비밀번호 설정
Samsung	Samsung Magician Samsung Portable SSD Software	비밀번호 설정 USB 보안 부팅디스크 설정 암호화 드라이브 설정

가이드라인에서 다루는 제품 확인하기

SanDisk®

▲ SanDisk

SanDisk PrivateAccess

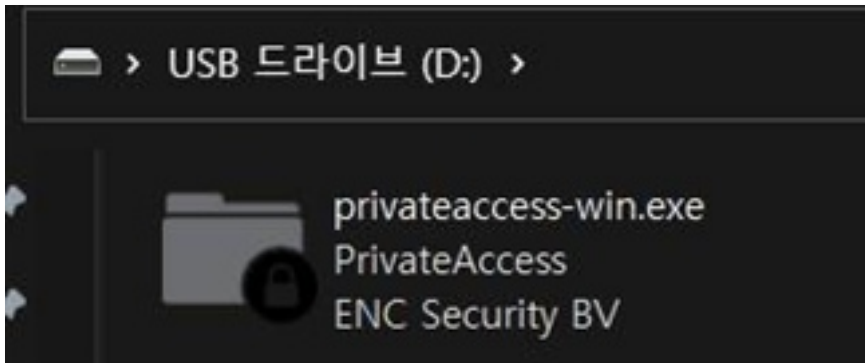
1. SanDisk PrivateAccess 사용하기

PrivateAccess 설치하기

SanDisk에서 제공하는 PrivateAccess 프로그램은 제품 내에 기본적으로 내장되어 있지만, 설치되어 있지 않은 경우 SanDisk 공식 홈페이지에서 프로그램을 다운받을 수 있습니다.

https://support-ko.wd.com/app/answers/detailweb/a_id/49570/initiator/user

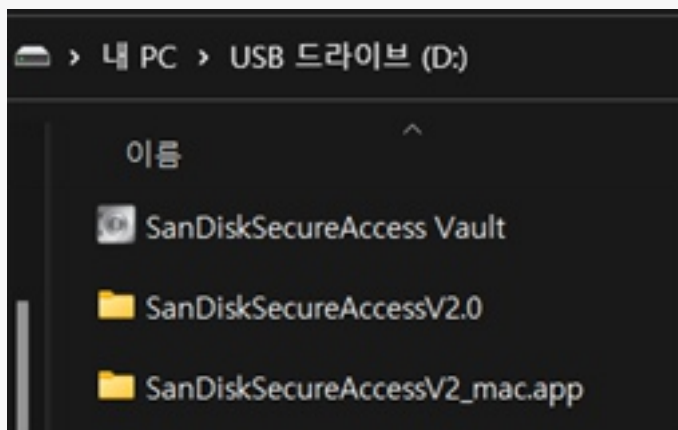
- SanDisk 제품용 PrivateAccess 지원 정보 및 다운로드



프로그램 실행 시 주의 사항

PrivateAccess 프로그램은 SanDisk 제품에서만 실행되기 때문에 다운로드 이후 저장매체 안에서 해당 프로그램을 실행해야 합니다.

만약, PrivateAccess의 이전 버전인 SecureAccess 프로그램이 내장되어 있는 경우 PrivateAccess로의 업데이트를 권장합니다.

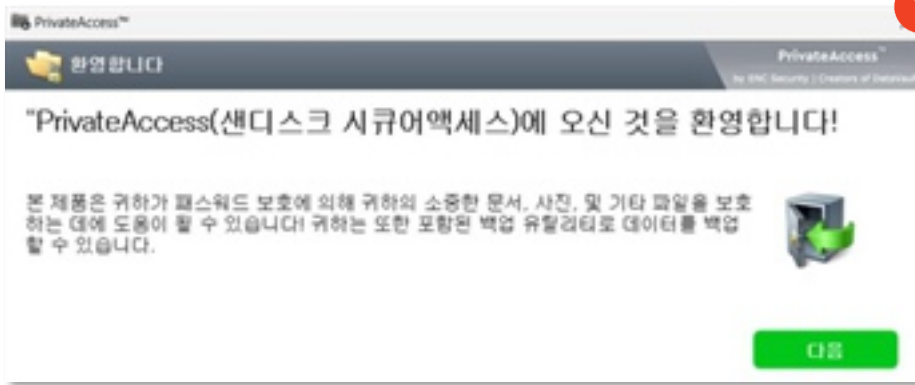


▲ SanDiskSecureAccess가 내장된 경우

SanDisk PrivateAccess

PrivateAccess 실행하기

- 1 ['PrivateAccess' 실행] > ['다음' 클릭]



- 2 [비밀번호 생성] > [사용할 비밀번호 입력]



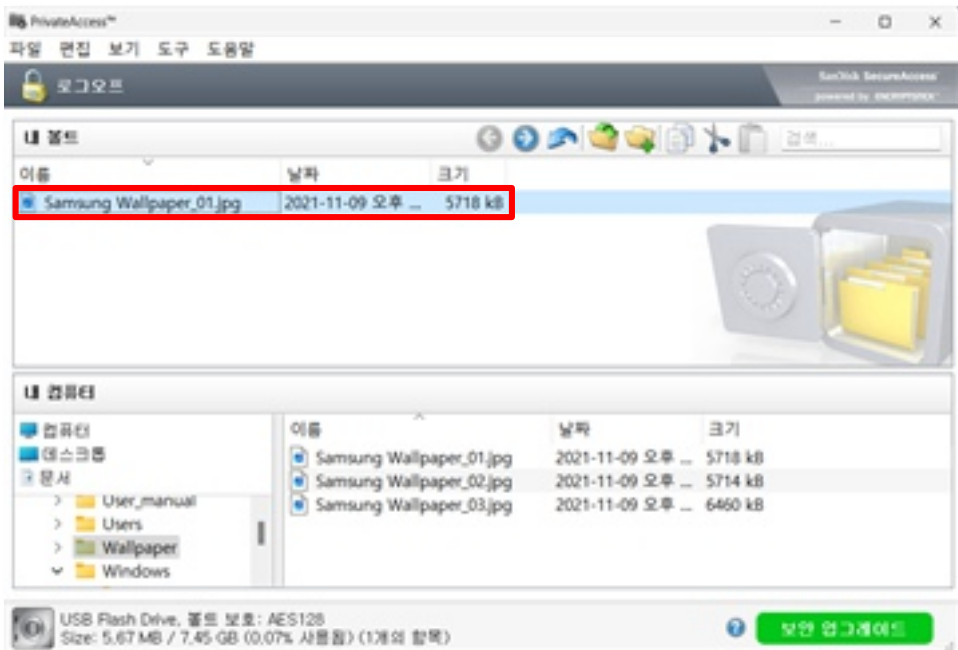
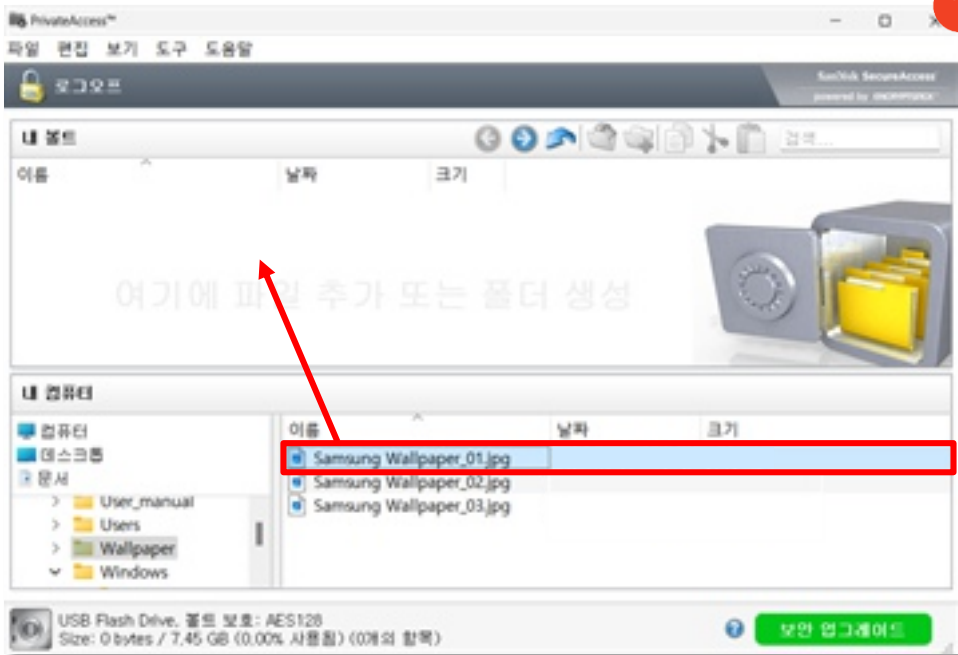
비밀번호 생성 시 유의사항

비밀번호 힌트 작성 시 사용하는 비밀번호를 그대로 입력하지 않도록 유의해야 합니다.

SanDisk PrivateAccess

PrivateAccess에 파일 저장하기

- 1 [PrivateAccess 프로그램 실행] > [좌측 하단에서 원하는 파일 드래그]



SanDisk PrivateAccess

PrivateAccess에 파일 저장하기

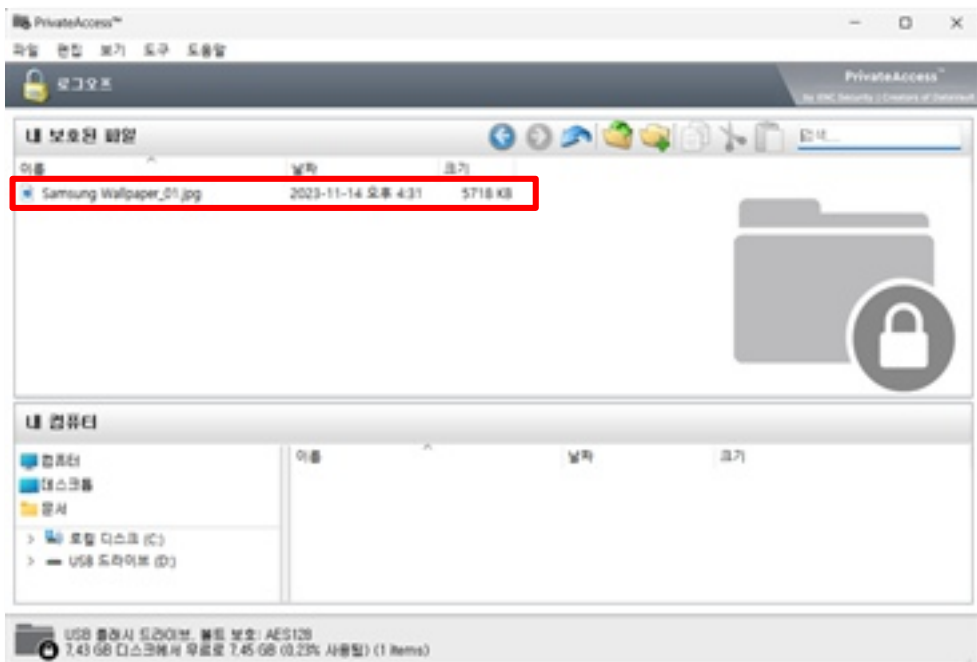
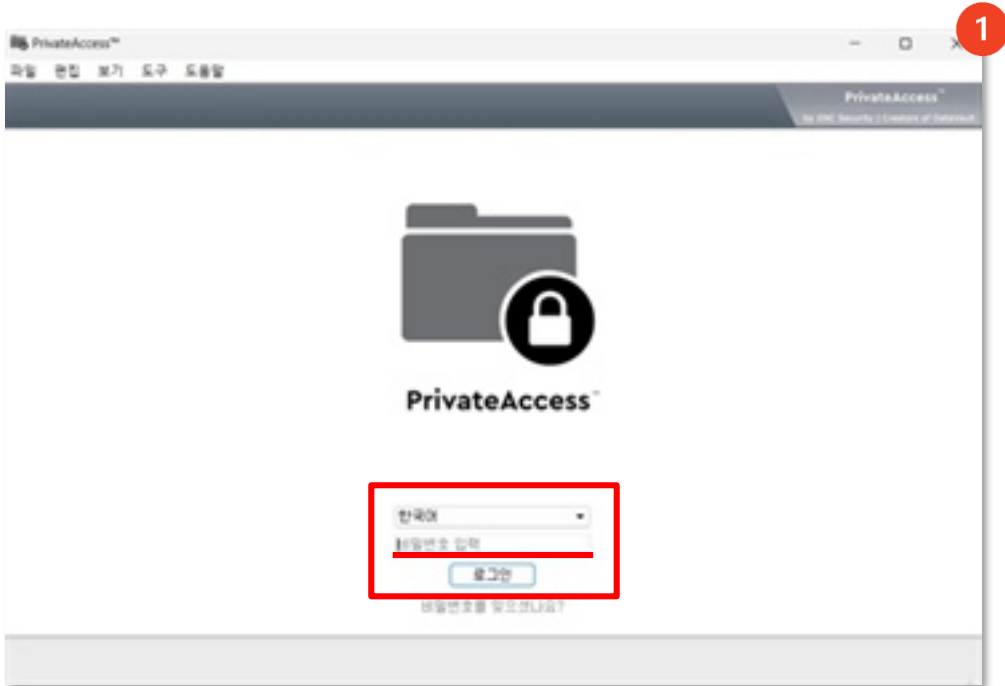
PrivateAccess을 통해 파일을 저장합니다. PrivateAccess를 통해 저장된 파일은 윈도우에서는 숨김처리 되기 때문에 이 프로그램을 사용해야만 접근할 수 있습니다.



SanDisk PrivateAccess

PrivateAccess에서 파일 확인하기

- 1 [PrivateAccess 프로그램 실행] > [비밀번호 입력] > [보호된 파일 확인]



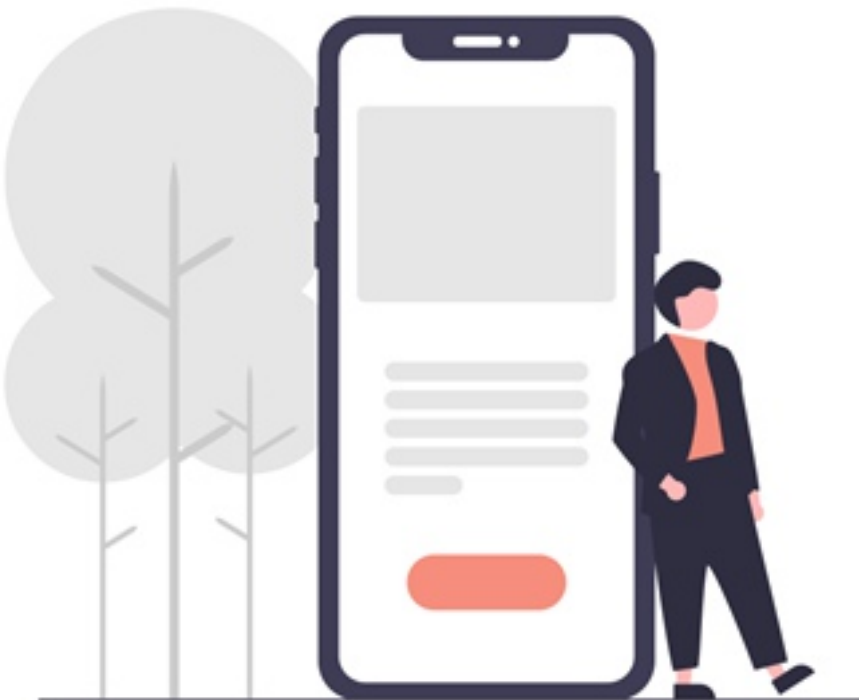
제2장 임직원 보안수칙

III. 모바일



i. 운영체제 ... 113

1. 안드로이드 ... 116
2. iOS ... 119



이것만은 지키자!

행동수칙

모바일 편

1



임직원의 스마트폰에는 최신 버전의 백신 앱을 설치해 주기적으로 검사해요!

임직원의 스마트폰에는 회사의 중요 정보가 들어 있을 수 있으므로 백신 앱을 필수로 설치해야 합니다. 백신 앱을 통해 악성코드의 침입을 방지하고, 스마트폰이 회사 네트워크에 연결되었을 때 생길 수 있는 위험을 사전에 차단하여, 회사의 정보를 보호할 수 있습니다.

2



출처가 불분명한 문자나 링크는 실행하지 않아요!

출처가 불분명한 문자나 링크(URL)에 악성코드가 포함된 경우가 많으므로, 문자나 링크를 실행한 스마트폰은 바이러스에 감염될 위험이 있습니다. 그로 인해 스마트폰에 저장된 개인정보뿐만 아니라 회사의 중요한 정보까지도 유출될 수 있습니다.

이것만은 지키자!

행동수칙

모바일 편

3



공식 스토어에서만 앱을 다운받아요!

공식 스토어에서 제공하는 앱은 검증 과정을 거쳐 안전한 경우가 많습니다. 공식 스토어가 아닌 곳에서 다운받은 앱은 악성코드 등의 위험이 있으므로, 스마트폰 감염을 통한 회사의 정보 유출을 방지하려면 공식 스토어에서만 앱을 다운받아야 합니다.

4



이용하는 웹사이트가 안전한 웹사이트인지 확인합니다.

이용하는 웹사이트가 통신하는 과정에서 안전하지 않다는 경고가 나오면, 중요한 정보가 노출되거나 탈취될 위험이 있다는 의미입니다. 안전한 통신을 제공하는 웹사이트를 이용하는 것도 회사의 보안을 유지하는데 중요합니다.

이번 장에서는 스마트폰, 태블릿 PC 등 개인이 업무를 위해 사용하는 모바일 기기의 보안 위험을 줄이는 방법을 제시합니다.

☑ 모바일 보안은 왜 해야 할까요?

개인 모바일 기기를 회사에 가져와 업무에 활용하는 것을 'BYOD(Bring your own device)'라고 합니다. 이는 업무 효율성을 높일 수 있다는 장점이 있지만, 반대로 회사 데이터에 접근하는 기기가 많아지므로 보안에 취약하다는 단점이 있습니다. 개인 기기가 정보 유출의 원인이 될 수 있다는 점을 알고 사용에 주의해야 합니다.

가이드라인에서 다루는 제품 확인하기



▲ 안드로이드



▲ iOS

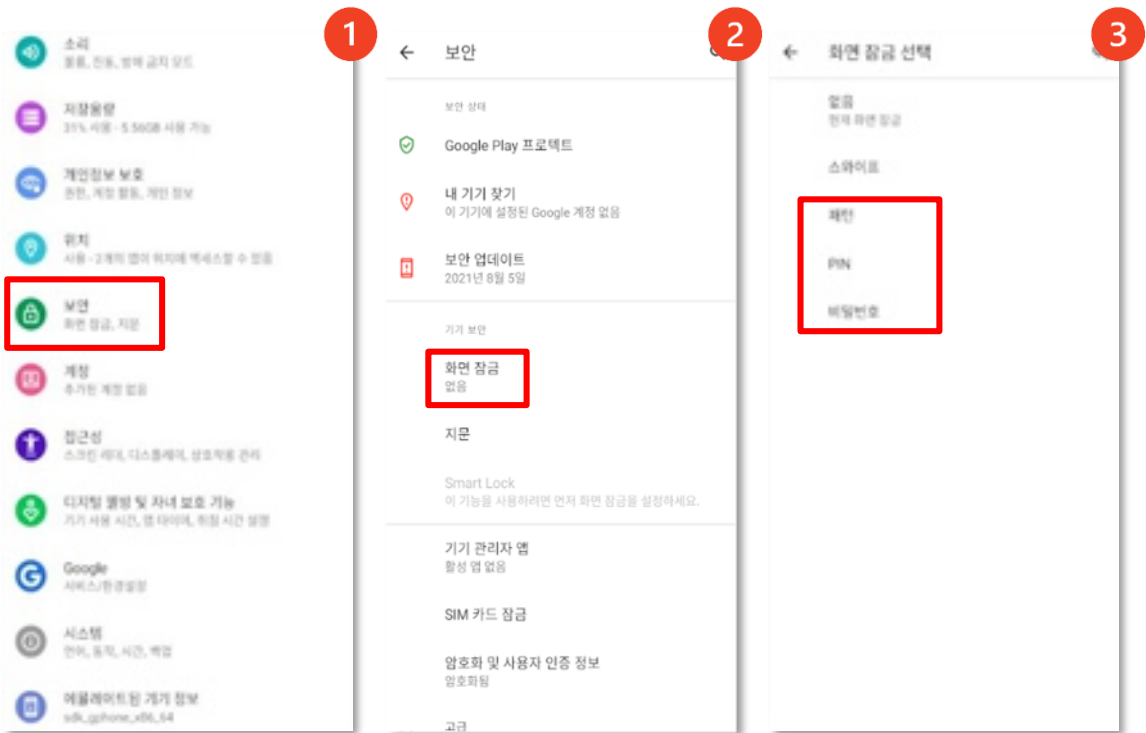


안드로이드

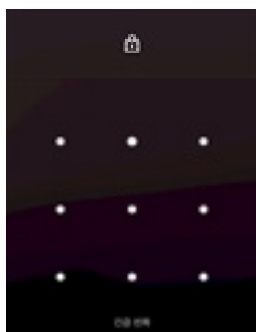
1. 기기 보안 설정하기

| 화면 잠금 설정하기

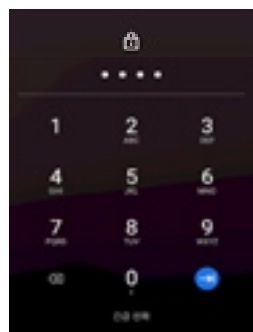
- 1 [설정' 실행] > ['보안' 선택]
- 2 ['화면 잠금' 선택]
- 3 ['패턴', 'PIN', '비밀번호' 중 화면 잠금 방식 선택]



| 잠금화면 설정 예시



▲ 패턴방식



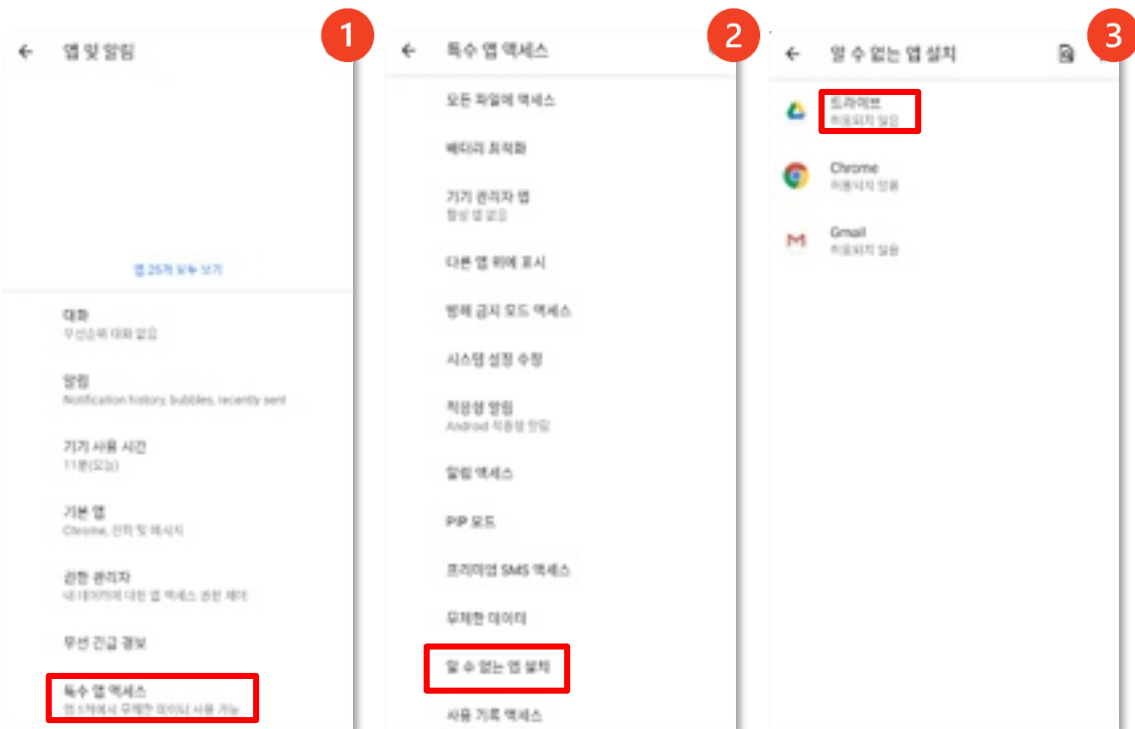
▲ PIN방식

안드로이드

I '출처를 알 수 없는 앱 설치' 허용 금지 설정하기

악성 앱으로부터 스마트폰을 보호하기 위해서 '출처를 알 수 없는 앱 설치'는 모두 허용하지 않아야 합니다. 아래 경로에서 허용 여부를 설정할 수 있습니다.

- 1 ['설정' 실행] > ['앱 및 알림' 선택] > ['특수 앱 액세스' 선택]
- 2 ['알 수 없는 앱 설치' 선택]
- 3 ['허용되지 않음' 상태인지 확인]



iOS에서의 '출처를 알 수 없는 앱'

아이폰 등의 iOS 기기에서는 신뢰하지 않는 개발자의 앱 설치가 기본 설정으로 막혀있습니다.



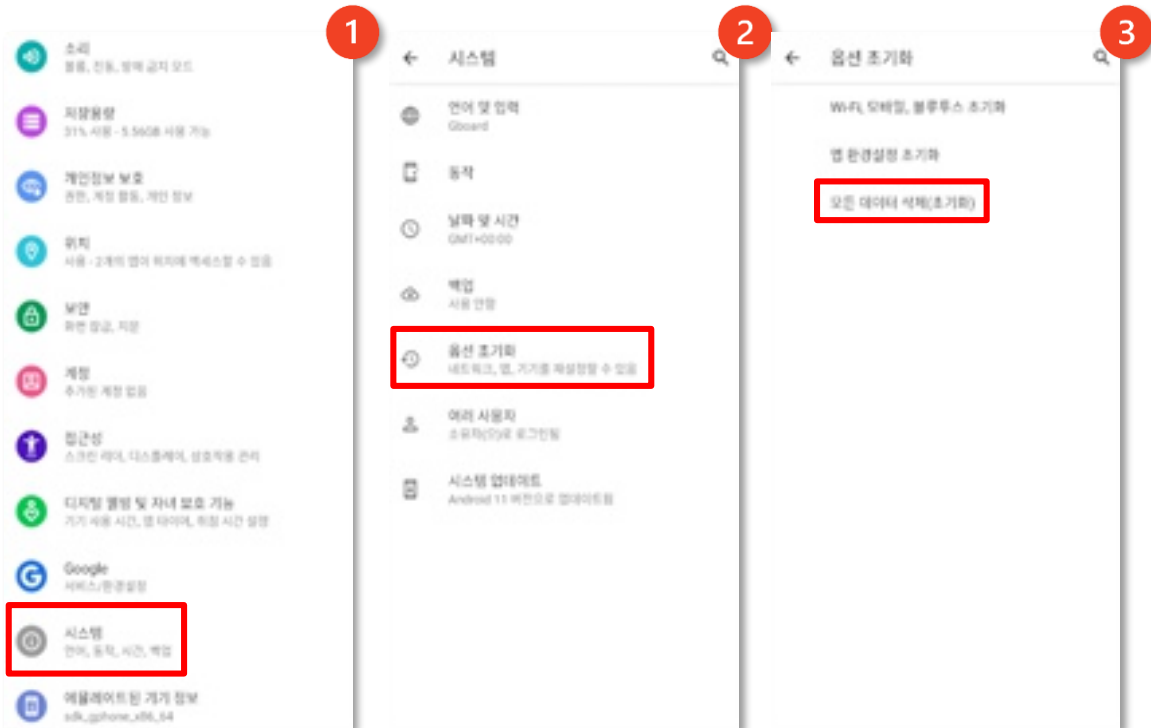
안드로이드

2. 기기 초기화하기

| 모든 데이터 삭제하기

기기를 타인에게 양도할 때에는 초기화 기능을 통해 데이터를 완전히 삭제해야 합니다.

- 1 ['설정' 실행] > ['시스템' 선택]
- 2 ['옵션 초기화' 선택]
- 3 ['모든 데이터 삭제(초기화)' 선택]

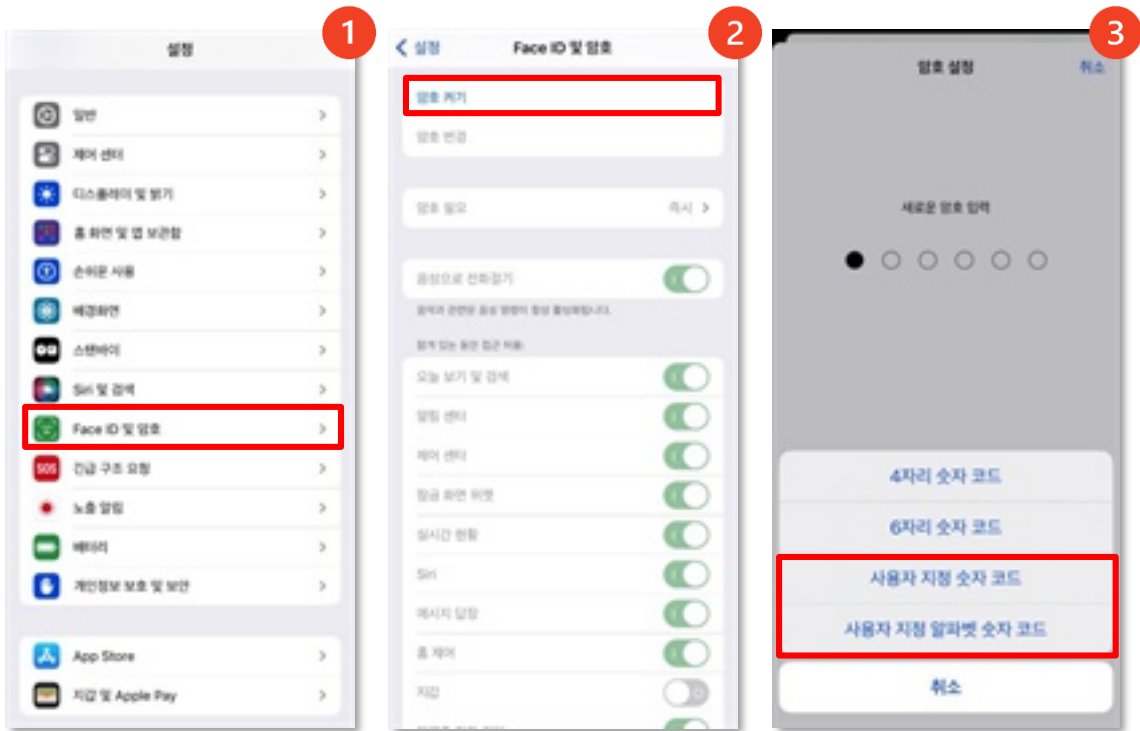


iOS

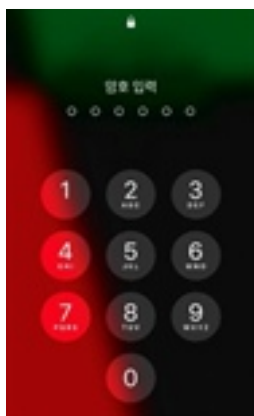
1. 기기 보안 설정하기

비밀번호 켜기

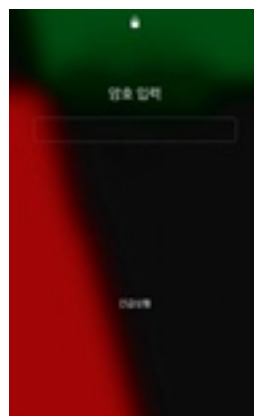
- 1 [설정' 실행] > ['Face ID 및 암호' 선택]
- 2 ['암호 켜기' 선택]
- 3 ['사용자 지정 숫자코드' 혹은 '사용자 지정 알파벳 숫자 코드' 선택 후 비밀번호 입력]



잠금화면 설정 예시



▲ 사용자 지정 숫자 코드



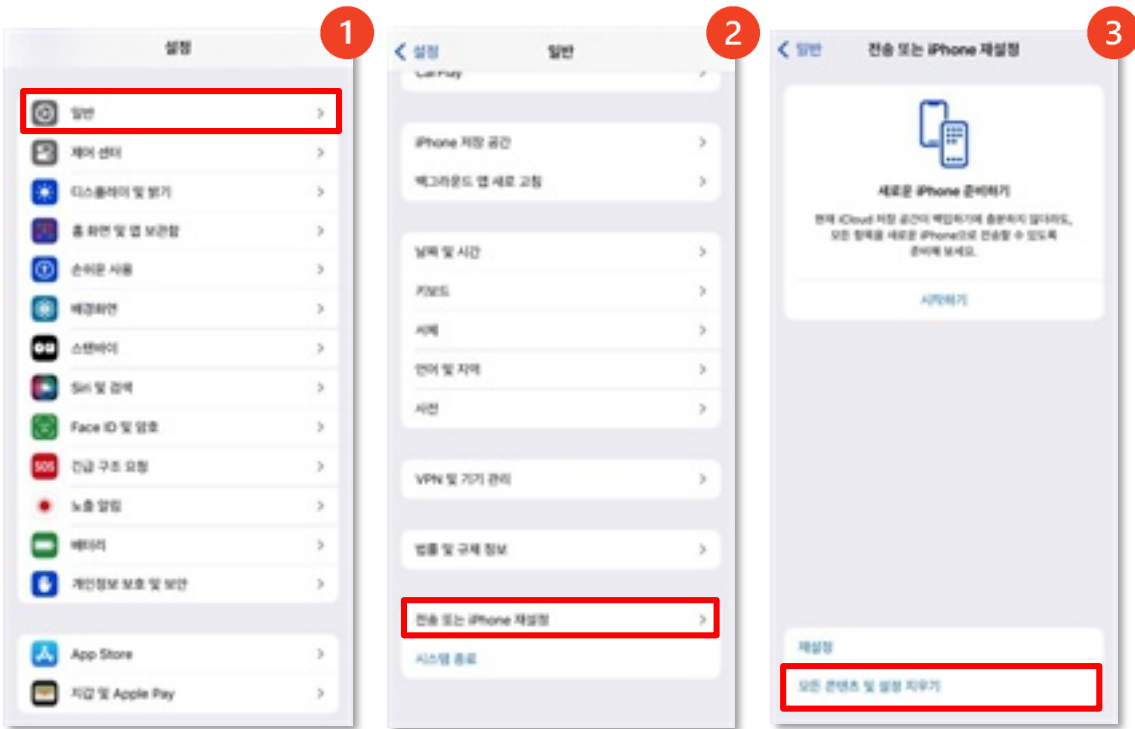
▲ 사용자 지정 알파벳 숫자 코드

iOS

2. 기기 초기화하기

| 모든 콘텐츠 및 설정 지우기

1. ['설정' 실행] > ['일반' 선택]
2. ['전송 또는 iPhone 재설정' 선택]
3. ['모든 콘텐츠 및 설정 지우기' 실행으로 기기 초기화하기]



3

침해사고 발생 시 대처 방법

본 장에서는 기업 내 침해사고 발생 시 대처 방법에 대해 다룹니다. 침해사고가 발생했을 때 신고할 수 있는 주요 기관인 경찰청, 한국인터넷진흥원, 중소벤처기업부에서의 신고 방법에 대해 설명하며, 이외에도 도움을 받을 수 있는 정부기관에 대해 안내합니다.

침해사고를 완전히 예방하는 것은 어려우며, 큰 피해를 막기 위해서는 침해사고가 발생했을 때 신속하고 정확한 대응이 이루어져야 합니다. 이번 편에서는 침해사고가 발생했을 때 신고할 수 있는 주요 기관과 그 신고 방법에 대해 살펴보겠습니다.

① 침해사고가 발생했을 때 꼭 신고해야 할까요?

기업에서 침해사고가 발생하면, 그 즉시 이 유관기관 혹은 **한국인터넷진흥원**에 알려야 합니다. 빠르게 대응할수록 기업의 피해를 줄일 수 있고, 업무 복귀시점을 앞당길 수 있습니다.

② 신고 기관별 차이점이 있나요?

경찰청은 **정보통신망을 통한 모든 형태의 범죄** 행위에 대한 신고를 받을 수 있습니다. 이는 정보통신망 침해 범죄 뿐만 아니라 정보통신망을 이용한 범죄, 불법 콘텐츠 범죄 등도 포함됩니다.

한국인터넷진흥원(KISA)는 유출된 정보의 유형에 상관 없이 **정보통신망 침해 범죄**에 대한 신고를 처리하고 있습니다.

중소벤처기업부는 사고의 종류에 상관 없이 **중소기업기술에 대한 범죄** 행위에 대한 신고를 받습니다.

중소기업의 기술이 정보통신망 침해로 인해 유출되었을 경우, 세 기관에 모두 신고가 가능합니다. 중요한 것은, **'빠른 신고를 통해 적절한 초동대응을 하는 것'**입니다.

가이드라인에서 안내하는 신고 사이트 확인하기



▲ 경찰청
사이버범죄 신고시스템



▲ 한국인터넷진흥원
인터넷침해사고대응지원센터



▲ 중소기업부
중소기업 기술보호 울타리

경찰청

사이버범죄 신고시스템



지원 대상

정보통신망* 침해 범죄를 당한 모든 기업

* 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제

지원 내용

사이버 상에서 일어나는 범죄행위에 대한 형사처벌

피해 유형

☑ 해커 또는 외부인이 컴퓨터에 침입해서 기업 데이터를 유출한 경우 (단순침입 포함)


☑ 해커가 기업 컴퓨터 시스템에 악성 프로그램을 유포해서 장애를 일으킨 경우


☑ 해커가 시스템이나 데이터 프로그램을 훼손, 삭제, 변경한 경우

신고 방법 ecrm.police.go.kr (사이버범죄 신고 시스템)

- 온라인: [ECRM 홈페이지 하단 신고하기] > ['긴급한 사안이 아닙니다.' 선택] > ['오프라인 사안이 아닙니다.' 선택] > [범죄유형-'해킹' 선택]
- 오프라인: 가까운 경찰서 직접 방문



 긴급신고 112(무료)

 민원상담 182(유료)

한국인터넷진흥원

인터넷 침해사고 대응 지원 센터



| 지원 대상

- 정보통신망* 침해 범죄를 당한 **모든 기업**
- 중소기업기술 침해 행위를 당한 **중소기업****

* 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제

** 「중소기업기본법」 제2조에 해당하는 중소기업

| 지원 내용

- 침해사고 발생 원인 및 침투경로 분석
- 재발방지를 위한 원인제거 지원
- 임직원 대상 온라인/오프라인 보안교육 진행

| 피해 유형

- 컴퓨터 시스템에 외부에서 접속한 흔적이 있는 경우
- 비정상적인 네트워크 성능 저하 및 특정 또는 모든 웹 사이트 접속이 어려운 경우
- 컴퓨터 파일이 바이러스에 의해 암호화된 경우

| 신고 방법 boho.or.kr (KISA 인터넷 보호나라)

- 온라인: [홈페이지 상단 정보보호 서비스] > [중소기업 피해지원] 선택
> [하단 '신고하기' 선택]



- 해킹·스팸개인정보침해 신고 118(무료)
- KISA 대표번호 1433-25(유료)

중소벤처기업부

중소기업 기술보호 울타리



중소벤처기업부

| 지원 대상

- 중소기업기술 침해 행위를 당한 **중소기업***
*「중소기업기본법」 제2조에 해당하는 중소기업

| 지원 내용

- 중소기업 기술침해에 대한 행정조사
- 침해내용(검토)에 따라 타부처 및 분쟁 조정제도 이관
- 가해기업에 대한 시정 권고 및 공표
- 행정조사 결과 기술피해가 인정되는 경우, 지원심사를 거쳐 법무지원단을 통한 민사소송 비용지원

| 피해 유형

- ☑ 기업기술이 타인에 의해 부정한 방법으로 취득·사용되는 피해를 입은 경우

| 신고 방법 mss.go.kr (중소벤처기업부) ultari.go.kr (중소기업 기술보호 울타리)

- 온라인: [중소벤처기업부 홈페이지(www.mss.go.kr)] > [민원·신고] > [신고센터] > [기술침해행위 신고]
- 오프라인: 세종특별자치시 가름로 180 중소기업부 기술보호과 기술침해조사팀 (서면 접수)



중소벤처기업부 기술보호과 기술침해조사팀
044-204-7786~7

침해사고 발생 시 도움을 받을 수 있는 유관기관 한 눈에 확인하기

보안 분야 전문가가 아니라면, 침해사고가 발생했을 때 적절한 대응 방법을 정확히 알기는 어려울 것입니다. 따라서 망설이지 말고, 즉시 아래의 전화번호로 연락하여 신속한 조치를 취하는 것이 필요합니다.

기관명	지원내용	연락처 · 홈페이지
 국가정보원 NATIONAL INTELLIGENCE SERVICE	<ul style="list-style-type: none"> 국내 첨단기술을 보호하고 산업보안활동을 수행 	<ul style="list-style-type: none"> 111 www.nis.go.kr
 중소벤처기업부	<ul style="list-style-type: none"> 중소기업지원 정책 	<ul style="list-style-type: none"> 1357 www.mss.go.kr
 산업통상자원부	<ul style="list-style-type: none"> 산업기술유출방지 및 보호에 관한 법률 및 정책 	<ul style="list-style-type: none"> 1577-0900 www.motie.go.kr
 공정거래위원회	<ul style="list-style-type: none"> 산업기술 유출범죄 전문 수사 및 예방 기업지원활동 	<ul style="list-style-type: none"> 1670-0007 (공정위 상담안내) www.ftc.go.kr
 특허청	<ul style="list-style-type: none"> 부정경쟁방지 및 영업비밀 보호에 관한 법률 및 정책 	<ul style="list-style-type: none"> 1544-8080 www.kipo.go.kr
	<ul style="list-style-type: none"> 지적재산권 침해 및 기술(영업비밀) 유출범죄 전문수사 	<ul style="list-style-type: none"> 1666-6464 www.ippolice.go.kr
 개인정보보호위원회	<ul style="list-style-type: none"> 개인정보 사고 발생 시 신고 및 문의 처리 	<ul style="list-style-type: none"> 02-2100-3025 (대표전화) 1833-6972 (개인정보분쟁조정위원회) www.pipc.go.kr
 한국인터넷진흥원 KISA	<ul style="list-style-type: none"> 침해사고 발생 시 초기대응 및 지원 	<ul style="list-style-type: none"> 1433-25 (대표전화) 118 (해킹 · 스팸개인정보침해) www.kisa.or.kr
 대·중소기업 농어업협력재단	<ul style="list-style-type: none"> 중소기업 기술보호 역량강화 지원사업 및 피해구제에 대한 상담 기능 수행 	<ul style="list-style-type: none"> 02-368-8700 www.win-win.or.kr
 K-ipcare 한국지식재산보호원 Korea Intellectual Property Protection Agency	<ul style="list-style-type: none"> 기업의 영업비밀 보호 및 체계적인 관리 One-Stop 지원 	<ul style="list-style-type: none"> 02-2183-5800 www.koipa.re.kr
 경찰청 KOREAN NATIONAL POLICE AGENCY	<ul style="list-style-type: none"> 산업기술 유출범죄 전문 수사 및 예방 기업지원활동 	<ul style="list-style-type: none"> 182 ecrm.police.go.kr (사이버범죄 신고시스템)
 한국산업기술보호협회 The Korean Association for Industrial Technology Security	<ul style="list-style-type: none"> 산업기술 유출방지 및 보호에 관한 정책지원 및 중소기업 지원 	<ul style="list-style-type: none"> 02 -3489-7014 www.kaits.or.kr

중소기업 기술 유출 방지 IT 보안 가이드라인

2023년 12월 발행
발행처 산업기밀보호센터

본 가이드라인은 공공의 목적을 위하여 한국인터넷진흥원의
주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드,
중소기업 정보보호 실무 가이드, 클라우드 취약점 점검 가이드
및 각 제품의 사용 안내서 등을 기반으로 제작되었습니다.

The background features several red geometric shapes: a small circle at the top left, a large circle at the top right, a semi-circle at the middle left, a ring in the center, and a thick line at the bottom right. The text is positioned in the upper left quadrant.

중소기업
기술 유출 방지
IT 보안
가이드라인