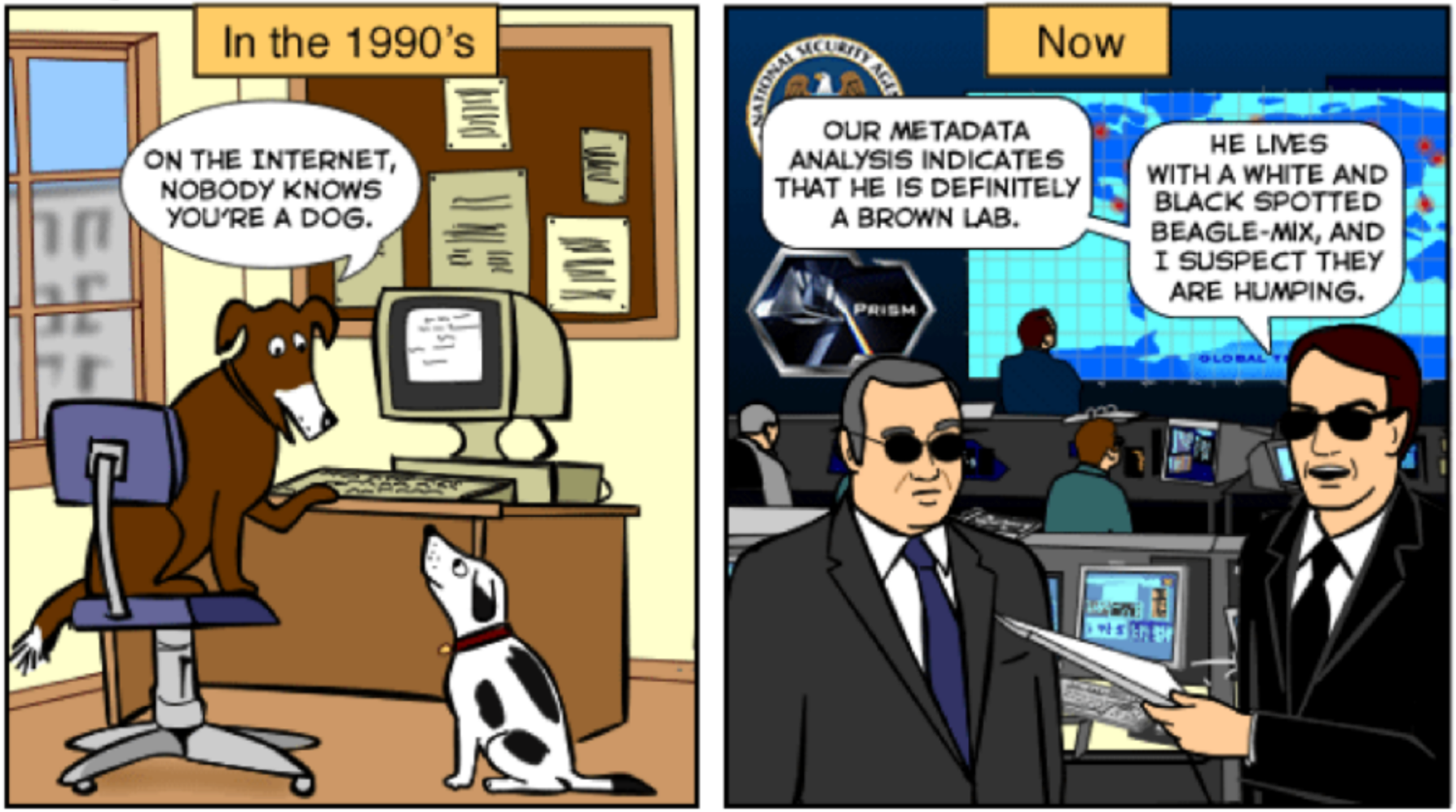
언택트 원격 환경의 사이버 보안 이슈 및 현황

조상현 Ph.D.
네이버 정보보호최고책임자(CISO)

NAVER

The Joy of Tech™

by Nitrozac & Snaggy



joyoftech.com

우리 삶 속에 빠르게 다가온 언택트의 시대

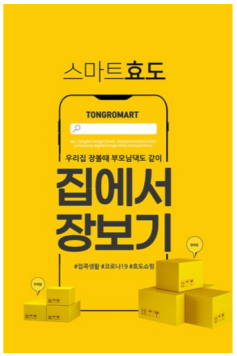
언택트 (UN + CONTACT) , NO-CONTACT, ZERO CONTACT

소비 환경, 업무 환경의 변화

언택트 마케팅 : 사람과의 접촉을 최소화하는 비대면 형태의 마케팅 기법

기계로 메뉴를 주문하는 키오스크나 가상현실(VR) 쇼핑, 인공지능(AI) 챗봇

온라인 교육, 화상 회의, 원격(재택) 근무, 온라인 면접의 보편화



COVID-19 위기 상황과 보안 위협

사회적 이슈는 사회공학적 해킹 기법으로 빠르게 진화함

- 기존의 사이버 공격에 대한 탐지 대응 체계는 약화될 수 있음
- 원격근무 급증에 따른 네트워크 가용성의 문제와 정보 유출 가능성 증가
- 언택트 비즈니스에서의 신원 확인 한계와 이를 악용한 사이버 범죄의 급증

  악성코드, 피싱 사이트, 금융 사기, 가짜 앱 등

(1) 회상 회의 증가에 따른 해커 공격 집중

- ❖ 줌 폭격 (Zoom Bombing) : 원격수업을 진행하던 중 신원을 알 수 없는 사용자가 입장하여 방해
- ❖ 공식 사이트가 아닌 블로그나 카페 등에서 악성코드가 포함된 설치파일 다운로드 설치
- ❖ 다양한 데이터 유출 가능성 (회의 내용, 캡쳐, 공유 자료 유출)
- ❖ 딥페이크 (Deepfake : 조작영상)의 확산 위협

Zoom says it has 300 million daily meeting participants, not users

로이터, 2020/04/30

March 30, 2020

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

COVID-19 팬데믹 중에 화상회의 및 온라인 강의실 하이재킹 공격에 대한 FBI 경고

Intel report warns Zoom could be vulnerable to foreign surveillance

DHS document urges government users to assess their risk.

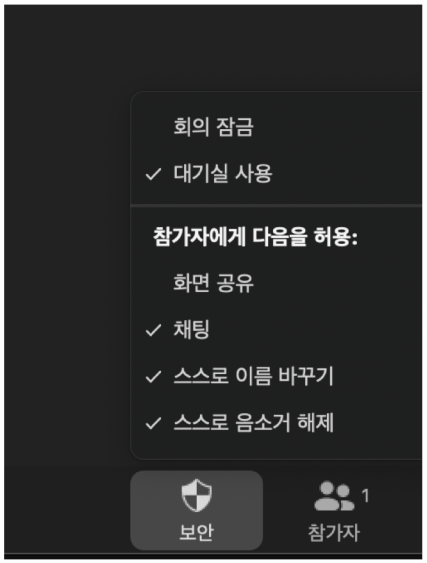
인텔보고서에서는 줌은 외부 감시에 취약할 수 있다고 경고

German government restricts use of Zoom over security concerns - reports

독일 정부는 보안 문제로 줌 사용 제한

화상 회의 보안 대책

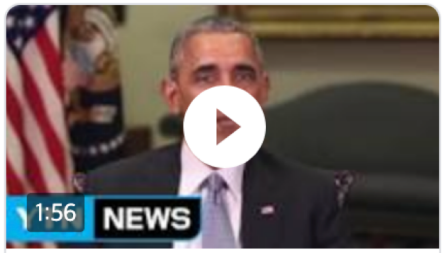
1. 안전한 화상 회의 서비스 사용과 신속한 보안 업데이트
2. 회의방 무단 침입 방지를 위한 비밀번호 (PIN) 필수 사용
3. 회의 참여 웹 주소와 비밀번호 외부 공개 금지
4. 회의 참여자의 신원 확인하고 모든 참여자가 회의방에 입장 후에는 회의방 잠금(Locking)
5. 원칙적으로 회의내용 녹화 금지하고 녹화 시 적절한 암호화 조치
6. 회의 주최자만 PC화면 공유 가능하게 하고, 사적인 대화 차단



딥페이크(Deepfake) 위험성 증가

합성 사진의 수준을 넘어서 딥러닝과 같은 AI기술을 활용하여 사람의 얼굴이나 목소리를 흉내내는 기술

사진, 음성, 동영상등 '감쪽같은 가짜'에서 '완전한 가짜' 만들기



'하지도 않은 말이 화면에'...'딥페이크' 영상 주의보 / YTN

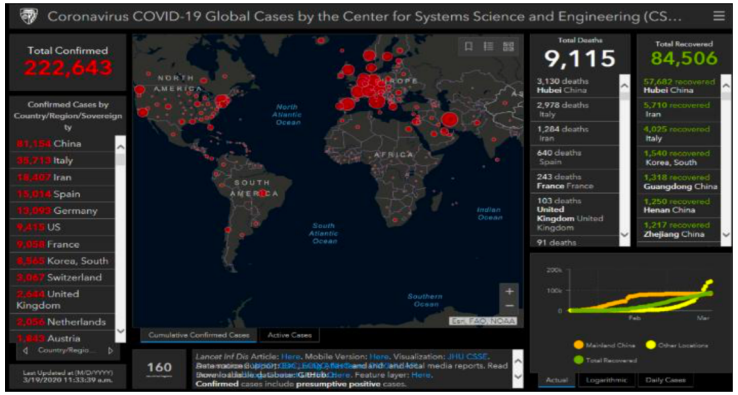
인공지능스타트업: Generated Photos

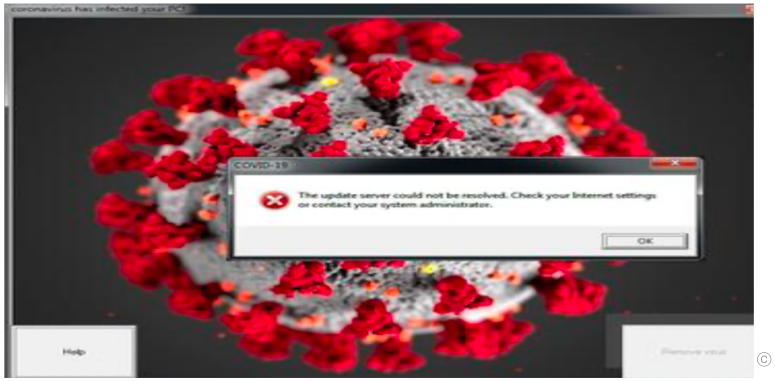
(2) COVID-19 키워드 악용 공격 위협 증가

- 피싱 메일 공격, 스미싱 공격, 악성 코드/악성앱 유포 (랜섬웨어 등)
- 코로나19를 주제로 한 피싱 공격 캠페인으로 정부 및 의료 기관을 대상으로 악의적인 공격 출현
- 국내도 2020년 1Q는 전 분기 대비 36%이상 증가했다는 통계

코로나19: 구글 하루 1천8백만 피싱 메일 삭제

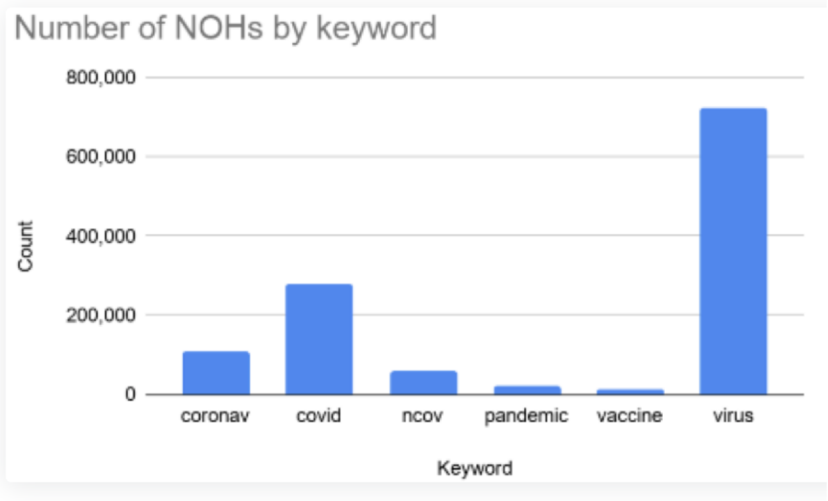
2020년 4월 18일



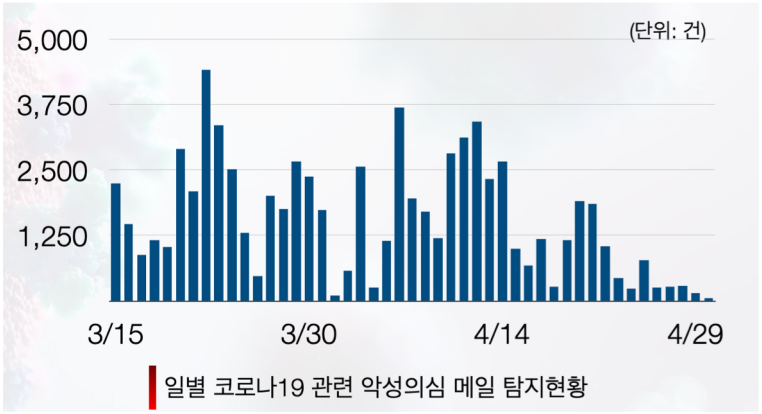


COVID-19를 키워드로 한 도메인들 생성이 급증하여, 대다수가 피싱 메일 공격 등에 활용됨

신규 등록된 도메인 중 COVID-19 관련 키워드 도메인이 40％ 이상 차지

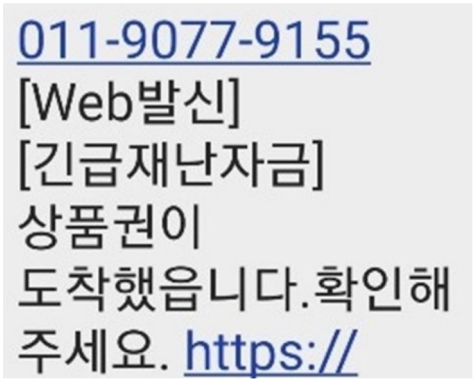


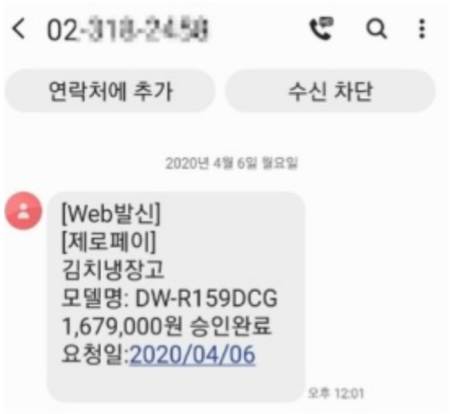
출처: paloalto (2020/03/09~2020/4/26)

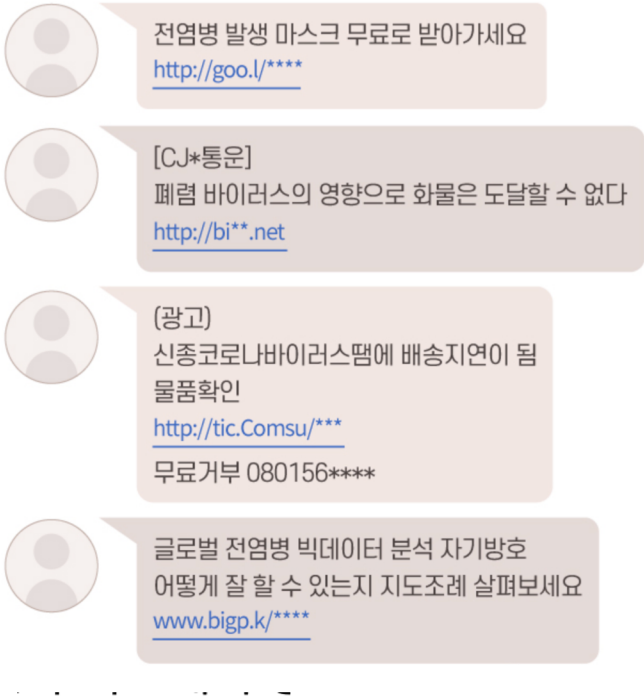


출처: 금융보안원

피싱 사이트 방문 및 악성(가짜) 앱 설치 유도







가짜 국세청 앱

사이버 허드렛일 확산

컴퓨터 사기 범죄자들, 자동화 봇이 아니라 값싼 노동력 선호

자동화 봇 사용했을 때보다 인간 고용하는 것이 공격 성공율 높아

비용 절감도 되고 공격 효율도 높아지고...유행하면 추적이 힘들어지기도

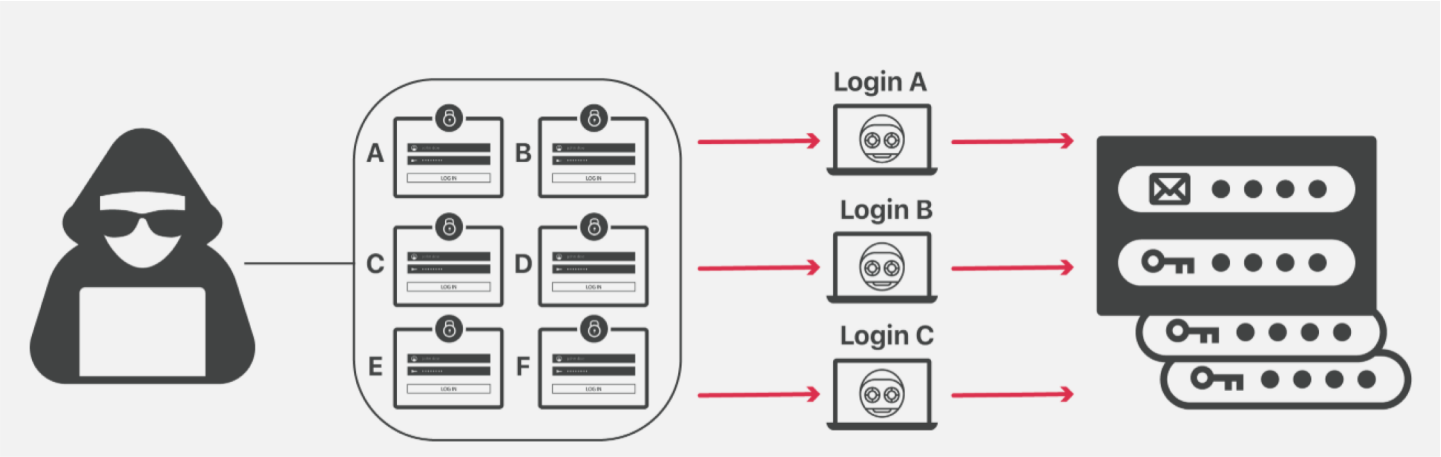
[이미지 = iclickart]

출처 : 보안뉴스 (19/11)

(3) 크리덴셜 스터핑 (Credential Suffing) 피해 급증

- 한 서비스에서 유출된 자격증명(크리덴셜)을 다른 서비스 로그인에 활용 시도하는 공격
- 약 0.1%는 성공한다는 이야기도 있지만…
- 2017년 11월부터 2019년 4월까지 세계 금융 업계를 대상으로 한 크리덴셜스터핑 공격은 35억 건 (출처: Akamai)
  “Akamai의 금융 서비스 고객 중 한 명에게 5천 5백만건의 악성 로그인 시도를 가했다”

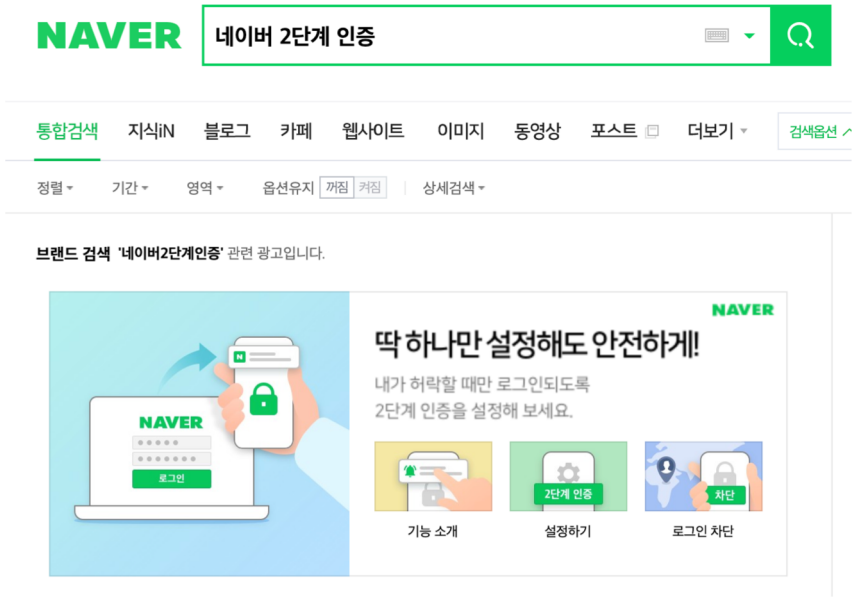
연예인 폰 해킹 주범 '크리덴셜스터핑'…해킹 배후도 밝혀지나

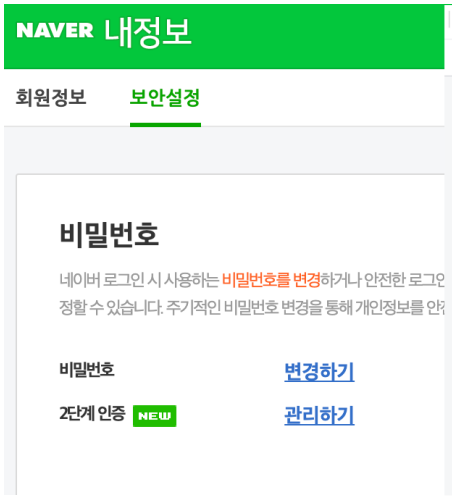


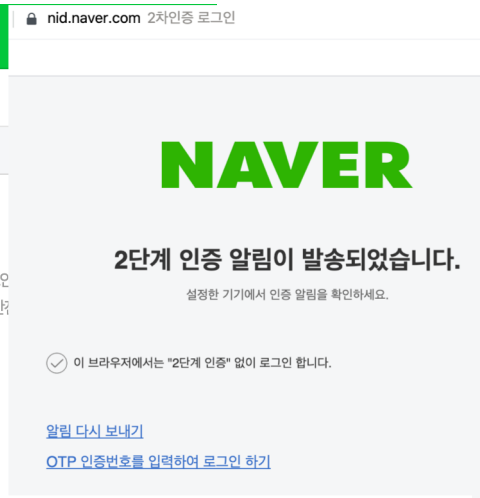
공격자 훔친 아이디와 비밀번호 매크로(봇) 공격 목표 서비스

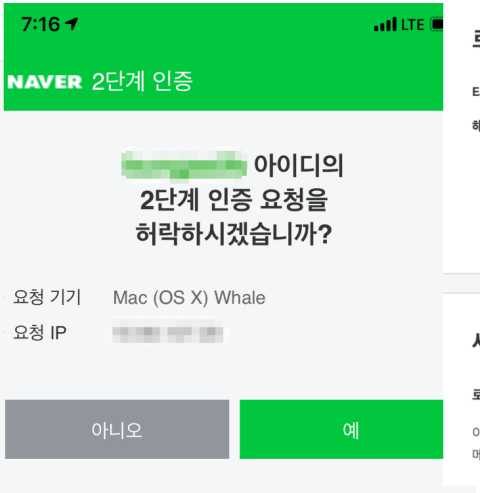
크리덴셜 스터핑 예방 방법

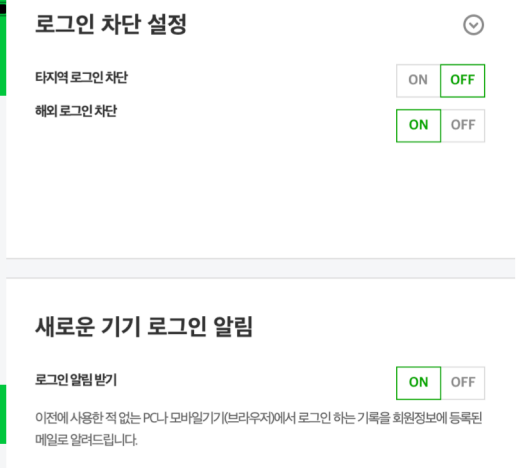
- 2차 인증 활성화
- 서비스 마다 유일한 아이디와 비밀번호 만들기
- 비밀번호는 더 길게 길게 만들기



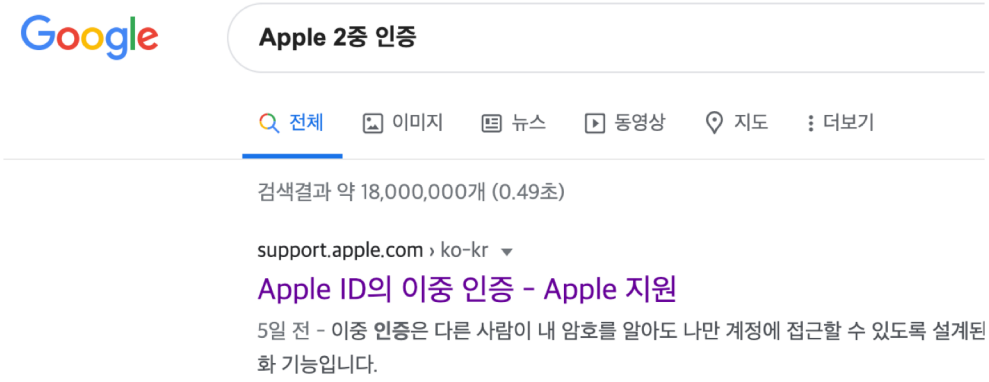


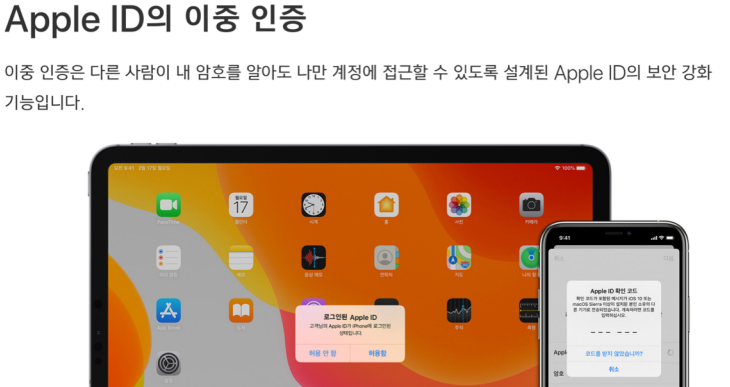






크리덴셜 스터핑 예방 방법



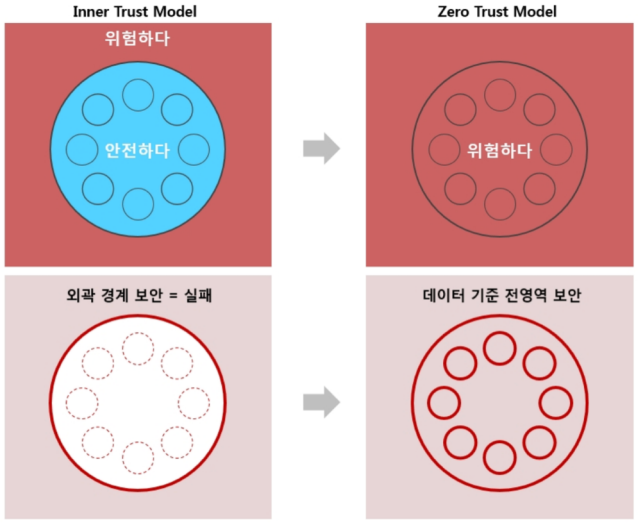


(4) 재택(원격) 근무 환경 보안 위협 증가

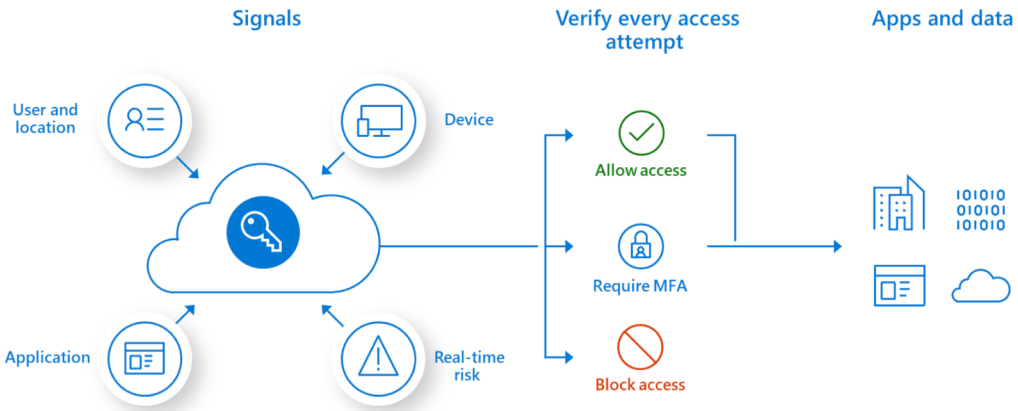
- ❖ 회사와 같은 보안 정책의 연속성을 유지하기 어려운 환경
- ❖ 상대적으로 안전하지 않는 네트워크/PC 환경
- ❖ 가정(공공 PC) 에서의 악성코드 감염/ 외부 침입으로 인한 정보 유출
- ❖ 위험 사이트 접근 제한 및 정보 유출 모니터링 차단 한계

제로트러스트(Zero Trust) 보안 전략의 전환 필요

- 아무도 믿지 마라
- 시스템 외부와 내부를 따로 나누지 않고 모든 곳이 위험하다고 가정
- 누구든 시스템에 접근하려면 권한을 부여하기 전에 한번 더 인증
- 특히 접근하려는 데이터에 따라 보안 강도(추가 권한 확인 등)을 차별화



출처 : Pentasecurity



출처 : Microsoft

맺음말

1. 주기적으로 안전하게 중요한 데이터를 온라인/오프라인에 백업하기
2. 가정 내 정보 보안에도 신경 쓰기 (예. 공유기 보안 관리)
3. 비밀번호 안전하게 관리하기
4. 의심스러운 이메일, SMS, 메신저 주의하기
5. 항상 최신 소프트웨어로 업데이트
6. 소셜 미디어 프로파일 관리
7. 프라이버시 및 보안 설정 확인
8. 공공 PC 사용 조심하기

https://www.kisa.or.kr/covid19/main.jsp