과학기술정보통신부
Ministry of Science and ICT
www.msit.go.kr

보도자료

4차산업혁명의 큰길로 대한민국이 달려갑니다

보도일시	2020. 3. 30.(월) 배포시점부터 보도해 주시기 바랍니다.		
배포일시	2020. 3. 30.(월)	담당부서	정보보호기획과
담당과장	최동원(044-202-6440)	담 당 자	신홍순 사무관(044-202-6441)

재택·원격근무 시 지켜야 할 정보보호 수칙 발표

- 랜섬웨어 감염 및 정보유출 방지를 위한 실천 수칙 권고 -

□ 과학기술정보통신부(장관 최기영, 이하 '과기정통부')는 재택·원격근무 시 기업의 해킹 피해를 예방하기 위하여 사용자와 보안관리자가 지켜야할 사항을 담은 정보보호 실천 수칙을 권고하였다.

o 이번 보안 권고는 최근 코로나19 발생 이후 감염병 예방을 위한 사회적 거리 두기의 일환으로 기업·기관의 재택·원격근무와 원격교육이 사회 전반으로 확산됨에 따라 보안위협 증가에 대비하기 위해 마련되었다.

□ 최근 코로나19 이슈를 악용하여 사용자 계정 탈취와 스마트폰·PC 해킹을 노리는 스미싱 문자가 지속적으로 유포되고 있고, 국내외에서 해킹메일 사례도 발견되고 있다.(스미싱 탐지: 2월~3월 9,886건)

o 또한, 코로나19로 인한 기업·기관의 약화된 보안관리 체계를 노린 랜섬웨어 공격 피해도 13건이 발생하는 등 민간부문의 보안위협이 증가하고 있는 상황이다.(랜섬웨어 피해 신고: 2월 1건 → 3월 13건)

□ 이에 따라, 과기정통부는 재택·원격근무에 이용되는 원격단말의 해킹 등 보안위험이 기업의 랜섬웨어 감염이나 정보유출로 전이되지 않도록 사용자와 보안관리자가 지켜야할 사항을 구분하여 6대 실천 수칙을 제정·권고하였다.

□ 먼저, 사용자 보안권고 사항에는 ▲개인 PC 보안 최신 업데이트 ▲백신 프로그램 최신화 및 정기검사 ▲가정용 공유기 보안설정(SW 업데이트, 비밀번호 설정) 및 사설 와이파이·공용PC 사용 자제 ▲회사 메일 이용 권장 및 개인 메일 사용주의 ▲불필요한 웹사이트 이용 자제 ▲파일 다운로드 주의(랜섬웨어 감염 주의) 등이 있으며,

o 기업의 보안관리자 권고에는 ▲원격근무시스템(VPN) 사용 권장 ▲재택근무자 대상 보안 지침 마련 및 인식제고 ▲재택근무자의 사용자 계정 및 접근권한 관리 ▲일정시간 부재 시 네트워크 차단 ▲원격 접속 모니터링 강화 ▲개인정보, 기업정보 등 데이터 보안(랜섬웨어 감염 주의) 등이 포함되어 있다.

□ 또한, 코로나19 상황이 마무리될 때까지 정부 및 기업의 안전 대책과 수칙, 팁 등을 한눈에 볼 수 있는 '코로나19 안심 정보'를 한국인터넷진흥원 홈페이지(www.kisa.or.kr/covid19) 및 전화(☎118)를 통해 운영할 방침이다.

o '코로나19 안심 정보'에는 '정보보호 6대 실천 수칙' 뿐만 아니라, 코로나19와 관련한 다양한 보안정책, 일반현황, 코로나19 관련 유용한 앱 등의 정보를 함께 제공하며, 정기적으로 업데이트할 예정이다.

□ 과기정통부 허성욱 정보보호네트워크정책관은 "코로나19로 인한 보안사고 예방을 위해서는 국민과 기업의 정보보호 수칙 준수에 대한 적극적인 동참이 필요하다."라고 말하며 "과기정통부는 앞으로도 코로나19와 관련한 각종 보안사고 및 사이버 공격 대응에 최선을 다하겠다."라고 말했다.

붙임 : 재택·원격근무 정보보호 6대 실천 수칙

이 자료에 대하여 더욱 자세한 내용을 원하시면
과학기술정보통신부 신홍순 사무관(☎ 044-202-6441)에게 연락주시기 바랍니다.

붙임1 코로나19 정보보호 6대 실천 수칙

<코로나19 재택근무 시 지켜야 할 정보보호 6대 실천 수칙>

사용자 실천 수칙		보안관리자 실천 수칙	
1	**개인 PC 최신 보안 업데이트** - 재택근무 시 개인 PC를 업무에 사용하는 경우 운영체제 및 응용프로그램 최신 상태 유지	1	**원격근무시스템(VPN) 사용 권장** - 사내 보안정책에 따른 VPN 사용 권장 - 미보유 기업의 경우 사내망 접속PC 백신 최신화 및 수시점검 정책 시행
2	**백신 프로그램 업데이트 및 검사** - 백신 보안패치 최신 업데이트 및 주기적 바이러스 검사 수행(원격근무 접속 전 및 일일 1회 이상) - 백신 자동 업데이트 설정 및 실시간 검사 기능 해제 금지	2	**재택근무자 대상 보안지침 마련 및 보안인식 제고** - PC 운영체제 및 소프트웨어 백신 최신화, 공유기 패스워드 설정, 업무 목적 외 웹사이트 이용 자제 등 보안지침 마련 및 교육 실시
3	**가정용 공유기 보안설정(비밀번호) 및 사설 와이파이·공용PC 사용 자제** - 가정 인터넷 공유기를 최신 소프트웨어로 업데이트하고, 공유기 비밀번호 설정 ※ 비밀번호는 유추가 어렵도록 특수문자 등 포함 - 개인 영업장(카페, 식당 등)에 설치된 사설 와이파이, 공용 PC를 이용한 재택근무 자제	3	**재택근무자의 사용자 계정 및 접근권한 관리** - 재택근무자의 비밀번호 설정 강화 및 재택근무 시 접근권한 최소화 방안 마련 - 원격근무시스템 접근 시 비밀번호 외 OTP 등 2차 인증수단 적용 필요
4	**회사 메일 권장, 개인 메일 사용주의** - 회사에서 제공하는 메일서비스 사용 권장 - 상용 메일서비스 사용 시 목적 외 메일 열람 자제 및 링크·파일 실행 주의 ※ 공용PC에서 메일열람 후 반드시 접속 종료	4	**일정 시간 부재 시 네트워크 차단** - 재택근무자가 사내 네트워크 접속 후 부재 시 네트워크 접속 차단 설정 ※ 10분~30분 동안 부재 시 차단 권장
5	**불필요한 웹사이트 이용 자제** - 업무 목적 외 웹사이트 접속 자제	5	**원격 접속 모니터링 강화** - 재택근무자의 사내 네트워크 접속 현황에 대한 관리 및 우회 접속 모니터링 실시
6	**파일 다운로드 주의(랜섬웨어 감염 주의)** - 메일 및 웹브라우저를 통해 파일 다운로드 시 랜섬웨어 감염 가능성이 있으므로 출처가 의심스러운 파일 다운로드 금지 - 업무 파일은 별도의 저장장치에 주기적 백업 실시	6	**개인정보, 기업정보 등 데이터 보안** **(랜섬웨어 감염 주의)** - 기업 중요 문서 및 데이터 활용 시 DRM 설정 등 데이터 유출 방지 대책 마련 ※ 데이터 외부 유출 시 관리자의 승인 절차 등 - 재택근무자의 작업 및 업무 파일을 기업 내부에 반입할 경우 랜섬웨어 감염 여부 등 파일 검사 필요 - 중요 기업 데이터 백업 권장