
 금융위원회	<div> <div>  </div> <div> 보 도 자 료 </div> </div>			
	보도	2020.3.9.(월) 조간	배포	2020.3.6.(금)
책 임 자	금융위 전자금융과장 이 한 진(02-2100-2970)	담 당 자	금 종 의 서기관(2811) 김 영 진 사무관(2973)	
	금감원 IT·핀테크전략국 선임국장 전 길 수(02-3145-7420)		장 성 옥 부국장(7415)	
	금융보안원 사이버대응본부장 임 재 옥(02-3495-9002)		임 형 옥 부장(9400)	

제 목 : 코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방수칙을 마련하였습니다.

1 배 경

- 정부는 금융회사에 맡겨진 국민의 재산을 충실하게 보호함과 동시에, 시스템 리스크를 방지하여야 할 금융분야의 특수성을 고려하여,
- 다른 분야에 비해 강화된 금융보안체계를 운영함으로써 해킹·악성코드 등 ‘사이버 공격’에 선제적으로 대응해 왔습니다.**[별첨1]**

※ (참고1) 사이버 공격(Cyber Attack)의 유형

- ① **(전산시스템·전산망 해킹)** 정당한 접근권한 없이 전산시스템·전산망에 불법적으로 접근하여 데이터를 조작·파괴·은닉 또는 유출
- ② **(악성코드 감염)** 전산망을 통해 컴퓨터 바이러스 등 악성 프로그램을 시스템에 감염시켜 전산시스템·전산망의 운영을 방해하거나 데이터를 파괴
- ③ **(서비스거부 공격)** 일시에 대량 신호를 보내거나 부정한 명령의 처리 등을 통해 서비스의 정상적 운영을 방해(DDoS : Distributed Denial of Service)

- 그런데, 최근 코로나19와 관련, 금융회사의 재택근무가 확대되고 인터넷·모바일 banking 등 비대면 금융거래가 증가하는 등의 상황에서
- 국민들의 불안감을 악용한 해커들의 이메일·문자 발송 등 사이버 공격의 우려가 제기되고 있습니다.

2 최근 코로나19 관련 사이버 공격의 특징

- 금융분야는 금융보안원을 통한 24시간 보안관제 조치 등에 따라 현재까지 사이버 공격 피해 사례는 발생하고 있지 않으나,
 - 다른 분야에서 악성코드를 첨부한 이메일 유포 등의 사례가 나타나고 있어, 향후 공격 확산 가능성 등에 유의할 필요가 있습니다.
- 특히, 코로나19와 관련한 최근 사이버 공격은 다음과 같은 특징이 있습니다.

- ① 코로나19와 관련한 이슈로 주의를 환기시키는 이메일·문자를 발송해 PC, 스마트폰 등에 악성코드를 감염시키고 정보 탈취를 시도하고 있으며,
- ② 해커들이 개인이나 특정 기관의 관련 정보·특성 등을 미리 파악하여, 그 대상이 관심을 가질만한 주제로 이메일등을 발송하는 이른바 ‘스피어피싱’ 공격도 두드러지고 있습니다.

* **Spear Phishing** : 잡을 물고기를 노려서 작살(Spear)로 낚시하는 것에 빗대어, 해커들이 특정 대상에 집중하여 최적화된 공격을 수행하는 사이버 공격 기법

※ (참고2) 코로나19 관련 사이버 공격 사례

악성앱 설치 유도 문자	악성코드를 포함한 이메일 유포
<p>전염병 발생 마스크 무료로 받아주세요.<URL></p> <p>(광고)신종코로나 바이러스팩에배송지연 물품확인<URL> 무료거부 0801567165</p>	

- 코로나19 이슈를 이용해 ‘**마스크 무료 배포**’, ‘**코로나로 인한 배송지연**’ 등 내용으로 문자메시지를 발송, 취약한 사이트 접속 및 악성앱 설치 유도(2.2일)
- ‘**Coronavirus Update: China Operation**’ 제목으로 악성코드가 포함된 이메일을 불특정 다수 기업에 유포(2.6일)
- 질병관리본부를 사칭하여 불특정 다수 사용자에게 이메일을 보내 특정 사이트 접속 유도 및 계정 정보 탈취를 시도(2.24일)
- 특정 해킹그룹* 등이 회사직원을 사칭해 ‘**코로나 바이러스 대응**’을 주제로 악성코드를 포함한 이메일을 발송(2.26일)

* `14년, 한국수력원자력을 해킹한 배후로 지목된 사이버공격 집단으로 악성코드 內 특정단어 ("Kimsuky")를 포함하고 있어 해당 해킹그룹을 "김수키"로 명명

3 조치사항

[1] 그간의 조치사항

□ 정부는 코로나19 관련 상황에 대응하여 그간 다음과 같은 조치를 하였습니다.

① 코로나19 관련 사이버공격 유의사항을 금융회사 등에 전파(2.7일)

* 금융전산 위기경보 발령('관심'), 코로나19 관련 금융보안 유의사항 전파 등

② 코로나19 관련 금융회사가 원격 접속 등 재택근무를 활용하는 경우에도 금융보안대책을 수립토록 조치(2.7일, 2.27일)

* 재택근무시 내부통제절차, 가상사설망(VPN) 활용 등 자체 보안대책 수립 필요

③ 사이버 공격 외에 보이스피싱 모니터링·대응체계를 강화하고, 대국민 유의사항을 안내(3.2일, 관계 부처 공동 보도자료 참고)

[2] 금융회사 등의 사이버 보안 유의사항

□ 앞으로 금융회사·전자금융업자 등은 일상적인 업무처리 과정에서 뿐만 아니라, 임직원 등에게 재택 근무 등을 하도록 하는 경우에도

○ 다음과 같은 보안 유의사항을 숙지하여, 해킹·정보유출 등 사고가 발생하지 않도록 금융보안에 만전을 기하여 주시기 바랍니다.

① 원칙적으로 금융회사의 보안대책이 적용된 업무용 단말기를 사용

② 재택 근무 과정에서 원격 접속시 내부 보안대책 등을 준수


③ 금융회사는 임직원 원격 접속시 상시 모니터링을 수행

④ 발신자 정보 등을 통해 수신된 이메일의 정상 여부를 한번 더 확인

⑤ 불특정 다수가 이용하는 PC(예: PC방 등) 등에서 업무용 이메일 열람 금지

⑥ 비대면 전자금융거래 증가 현황 등을 모니터링 → 서비스 지연 또는 거래 중단 등의 사고가 발생하지 않도록 유의

[3] 금융이용자를 위한 해킹 등 피해예방 수칙

- 금융이용자인 국민들께서도 다음과 같은 피해예방 수칙을 적극 참고하여, 해킹 등으로부터 재산을 보호하고 소중한 개인정보를 지키시길 바랍니다. [상세내용  별첨2, 3]

- ❶ 백신 프로그램 설치 및 최신 버전 유지
- ❷ 모르는 사람이 보낸 문자메시지 및 이메일 열람 주의
- ❸ 출처가 불분명한 파일 다운로드 및 실행 금지
- ❹ 정부, 금융 유관기관, 기업 등을 사칭하는 이메일 열람 주의
- ❺ 스마트폰 공식 앱스토어(애플앱스토어, 구글 플레이스토어 등) 이외에서의 앱 설치 주의

4 향후 대응방향

- 최근 국경 없는 사이버 공격은 지속적으로 진화중이며, 신기술 활용에 따른 디지털 금융 리스크는 확대되고 있습니다.
 - 과거 IT리스크 차원에서만 관리되던 금융보안은 금융안정에 까지 영향을 미칠 수 있는 중요 고려사항*으로 부각되고 있습니다.
- * 사이버 리스크가 금융 시스템의 안정성에 위협 요인이 되고 있으며, 사이버 보안 강화는 금융안정을 위해 우선 고려할 과제(IMF, "Cybersecurity Risk Supervision", '19.9월)
- 정부는 코로나19와 관련한 사이버 공격 동향을 지속 모니터링하고, 필요시 쏜금융회사에 보안 유의사항을 신속 전파하는 등 철저히 대응하겠습니다.
- 앞으로, 이번과 같은 비상 상황 뿐만 아니라, 금융회사의 근무환경 변화 등에 맞추어 금융보안을 강화할 수 있도록
 - 금융회사·전자금융업자, 금융인프라 기관 등의 업무연속성 계획(BCP: Business Continuity Plan) 등을 포함한 디지털 금융보안 체계를 전반적으로 개선하는 노력도 지속해 나가겠습니다.

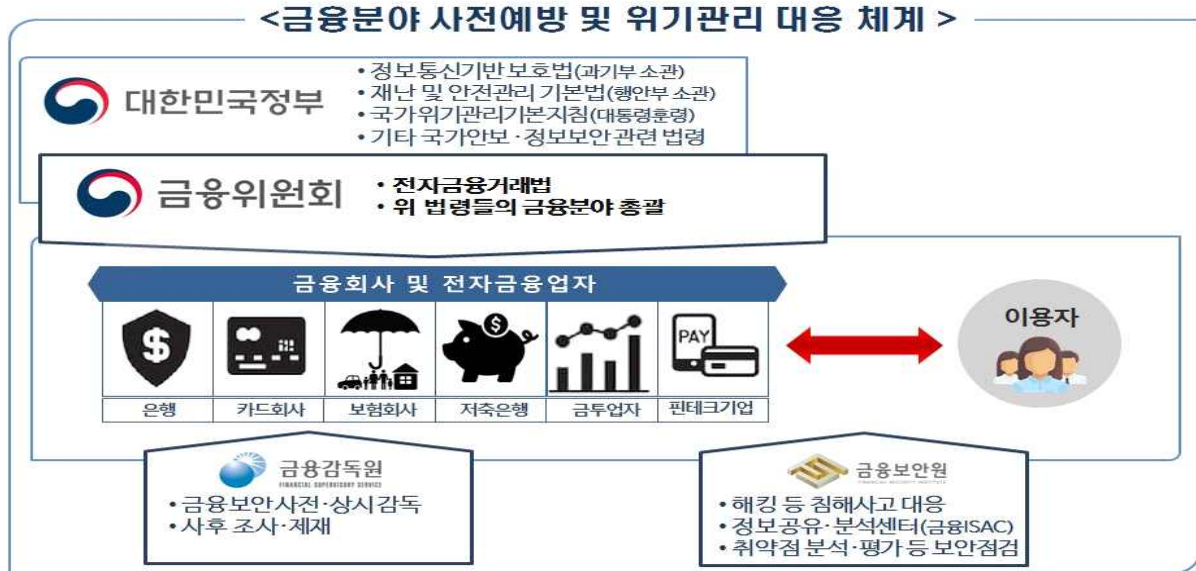
- ※ 별 첨 1 : 금융분야 사이버 공격 대응체계
 2 : 코로나19 관련 해킹 등 피해예방 수칙(상세)
 3 : 악성코드 감염예방 및 안전이용 수칙(그림)

  공공누리 공공저작물 자유이용허락	본 자료를 인용 보도 할 경우 출처를 표기 해 주십시오. http://www.fsc.go.kr	금융위원회 대 변 인 prfsc@korea.kr	 질병관리본부 콜센터	
--	--	---	---	---

“혁신금융, 더 많은 기회 함께하는 성장”

별 첨1

금융분야 사이버 공격 대응 체계



- 금융분야는 금융공동망 기반의 실시간 거래* 등으로 인해 사고 즉시 이용자의 재산상 피해 발생 가능 → Systemic Risk 우려

* 미국 등 주요국은 국내와 같이 금융공동망이 발전되어 있지 않음(영국은 '08년, 일본은 '18년말부터 24시간 실시간 이체가 가능, 그 외 주요국은 도입 추진 중)

- 이에 「전자금융거래법」 및 감독규정을 통해 금융사고·해킹 등의 예방 노력 등을 지속해 옴

- 특히, '13.3월 전산사고, '14.1월 카드정보 유출사고 등을 계기로 금융권의 보안인식을 제고하고 보안시스템을 대폭 강화

- ❶ 금융보안 상시 감독·검사를 수행하는 '금융감독원'과 함께 침해 대응·금융보안 전문기구인 '금융보안원'을 설립·운영중('15년~)

* 금융보안원의 정보공유·분석센터(ISAC, Information Sharing & Analysis Center)는 침해시도 및 발생 여부 등을 24시간 365일 모니터링·대응중

- ❷ 금융회사에게 사이버 공격 요인을 제거하고 안전성 확보 의무*를 부과하여 외부 사이버공격 시도를 사전에 차단토록 조치

* (i) 업무지속성 확보 방안(BCP)을 비롯한 비상대책 수립, (ii) 시스템 취약점 분석·평가, (iii) 비상대응훈련 실시, (iv) 재해복구센터(DR:Disaster Recovery) 설치·운영, (v) 망분리 등

- ❸ 정보보호최고책임자(임원급) 지정을 의무화함으로써 내부통제를 강화하고, 타 분야 유관기관과 사이버공격 정보 공유·대응

⇒ 최근 국내 금융권은 각종 사이버 공격에 선제적으로 대응함으로써 대형 전산사고로 이어진 사례는 없는 상황

1. 백신 프로그램 설치 및 최신버전 유지

- 바이러스 백신 소프트웨어 설치 및 최신버전 유지
- 백신 실시간 감시기능 활성화 및 주기적인 검사 실행
- 운영체제 및 응용 프로그램 최신버전 유지

2. 모르는 사람이 보낸 문자메시지 및 이메일* 열람 주의

* “코로나19 대응”, “코로나 감염자접촉자 신분정보 확인” 등의 문자이메일을 특히 주의

- 메일주소가 이상하지 않은지 우선 확인
예) @naver.com→naver-com.cc / @google.com→@goog1e.com / @daum.net→dauum.net
- 예정되지 않은 업무메일, 스팸메일 등 열람 금지
- 자극적인 주제의 이메일 및 SMS는 한번 더 의심
- 의심메일 수신시 발신자에게 유선 및 문자 등 다른 통신수단으로 재확인

3. 출처가 불분명한 파일 다운로드 및 실행 금지

- 신뢰할 수 없는 사이트 방문 자제
- 이메일 첨부파일은 보안메일 또는 출처가 확실한 경우에만 실행

4. 정부, 금융 유관기관, 기업 등을 사칭*하는 이메일 열람 주의

* 질병관리본부, 검찰·경찰, 금융감독원, 마스크·체온계 제조판매 업체 등 사칭에 유의

- 이메일, 문자 내에 포함된 의심스러운 링크(URL) 클릭을 주의
- 특정 사이트 접속 유도시 아이디, 패스워드 등 개인정보 입력에 주의

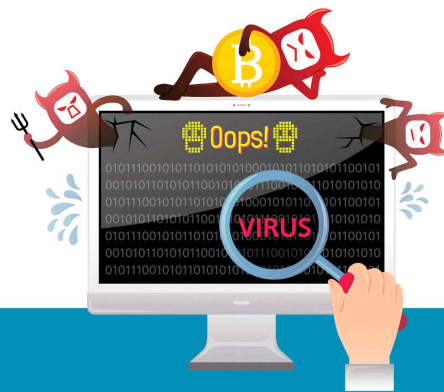
5. 스마트폰 공식 앱 스토어 이외에서의 앱 설치 주의

* 애플앱스토어, 구글플레이스토어 등 공식 앱 스토어를 이용

- 문자메시지 등을 통한 악성앱 설치 유도 주의

악성코드 감염예방 및 안전이용 수칙

보안수칙 생활화로 악성코드 감염 및 피해를 최소화 할 수 있다



감염예방 5대 수칙

- 1 운영체제 및 사용 프로그램을 최신 버전으로 유지
- 2 최신 버전의 백신 프로그램 설치 및 주기적 업데이트
- 3 백신 실시간 탐지 활성화 및 주기적 검사 실행
- 4 웹브라우저 팝업 차단 기능 설정
- 5 신뢰할 수 있는 정품 소프트웨어 사용

안전이용 5대 수칙

- 1 모르는 사람이 보낸 이메일 첨부파일 실행 및 링크된 이미지 클릭 주의
- 2 인터넷에서 출처가 불분명한 파일 다운로드 및 실행 금지
- 3 금융당국 및 정부기관을 사칭하는 협박성 이메일 주의
- 4 신뢰할 수 없는 사이트 방문 자제 및 확인되지 않은 URL 클릭 주의
- 5 공식 스토어(애플앱스토어, 구글 플레이스토어) 이외 앱 설치 주의