포스트 코로나 시대의 사회공학적 해킹과 대응방안

지도교수 : 한 상 훈
연 구 자 : 전 민 석

< 목 차 >

요 약

2020년 코로나19 바이러스가 전 세계적으로 퍼지면서 확진자 수는 나날이 늘어나고 있다. 코로나19는 우리의 삶을 180도 바꾸었고 사람들은 기존에 누렸던 일상이 얼마나 소중한지 피부로 느끼고 있다. “코로나 19 발병 이전의 삶으로 돌아가기는 힘들뿐더러 새로운 시대에 대한 대비를 해야 한다.”는 전문가의 말에 따라 우리는 실질적인 대책을 세워야 할 것이다. 코로나19 발병 이후 사람들의 불안 심리를 악용한 보이스 피싱, 스미싱 등의 사회공학적 해킹 기법으로 개인정보를 탈취하는 일이 빈번해지고 있다. 이에 따라 본 논문에서는 먼저 코로나19가 사회적으로 어떠한 변화를 가져왔는지, 또 사회공학적 해킹에는 어떠한 기법이 있는지 사례를 통해 알아볼 것이다. 또한, 코로나19 발병 이전과 이후에 사회공학적 해킹이 얼마나 증가했는지 알아보고 이에 대한 사람들의 인식에 대해 조사하고 분석할 것이다. 이를 토대로 사회공학적 해킹에 대한 대응방안을 알아보고자 한다.

주요어 : 포스트 코로나, 사회공학적 해킹, 피싱, 스미싱, 파밍

1. 서론

2020년 전 세계가 코로나19(COVID-19) 바이러스의 대유행으로 사회가 급변하였고 그로 인해 큰 혼란이 초래됐다. 코로나19 발병 초기에는 중국부터 시작해 일본, 한국 등 아시아 국가 뿐 아니라 서양권 국가까지 확산되었다. 현재는 전 세계적으로 확산되고 있다.

코로나 19의 강한 전염성에 따라 각국의 보건단체에서는 사회적 거리 두기와 위생관리 등을 철저하게 할 것을 당부하고 있으며 각국의 정부는 경제 지원 정책으로 경제위기를 극복하려 하고 있다. 또한, 코로나19는 언택트(Untact), 즉 비대면 사회로의 변화를 가속하고 있다.

재택근무, 온라인 강의 등이 일상화되어 가고 있다. 이러한 코로나 19로 인한 사회현상 극복 후 다가올 새로운 시대를 포스트 코로나라고 한다. 포스트(Post)와 코로나 19의 합성어로 지금처럼 언택트(Untact) 문화의 확산, 원격 교육 및 재택근무 급증 등 사회 전반의 큰 변화들이 우리 사회를 주도하게 된다는 것이다.

한편 코로나 19의 대유행을 악용한 사이버범죄의 빈도가 증가하여 인터넷상에서의 위협이 대두되고 있다. 특히나 코로나 19를 주제로 한 피싱, 스미싱, 파밍 등의 사람들의 불안 심리를 일으켜 개인정보를 탈취해가는 사회공학적 기법을 이용한 해킹이 증가하고 있다.

이에 따라 본 논문에서는 코로나 19로 초래된 사회적 변화 속에서 나타나는 사회공학적 해킹과 그에 따른 대응방안을 알아보고자 한다.

2. 포스트 코로나 시대의 사회공학적 해킹의 정의 및 사례

2.1 사회공학적 해킹의 정의

사회공학, 소셜 엔지니어링(Social Engineering)이라고도 불리는 이것은 사람들의 심리적 사회적 관계를 이용하여 사기를 치는 오래된 수법으로 새로운 기술이 아닌 오래전부터 존재해 온 기술로 우리 주변에서 흔히 일어나고 있는 현상이다.

정보보안에서의 사회공학, 사회공학적 해킹이란, 앞서 말한 개념과는 조금 다르다. 정보보안에서의 사회공학은 시스템이 아닌 사람들의 심리적, 사회적 관계, 사회적 요인과 심리적 요인, 즉 사람의 취약점을 공략하여 해킹에 필요한 정보 등을 얻어내는 공격 기법을 말한다.

비 기술적인 방식으로 시스템의 취약점을 공격하는 DDos 공격 등과 같은 기술적인 해킹과는 구분된다.

해커들은 온라인 및 오프라인 상에서 공격의 타겟으로 삼은 사람의 성향 등을 파악하여 정보를 수집하여 그것을 토대로 회사나 정부기관 등을 사칭하여 악성코드가 담긴 파일을 작성한다. 그렇게 작성된 내용을 피싱 메일, 스미싱 등으로 퍼뜨려 사람들은 의심 없이 파일을 열게 되어 퍼져나가게 된다.

위와 같은 접근 방식을 통해, 키로깅 프로그램을 이용해 공격 대상의 계정 패스워드를 가로채거나 사용자를 위장 웹사이트로 유인하여 입력한 개인정보를 탈취하는 파밍 수법 등이 시도되어지고 있다.

2.2 사회공학적 해킹 사례와 공격 기법 소개

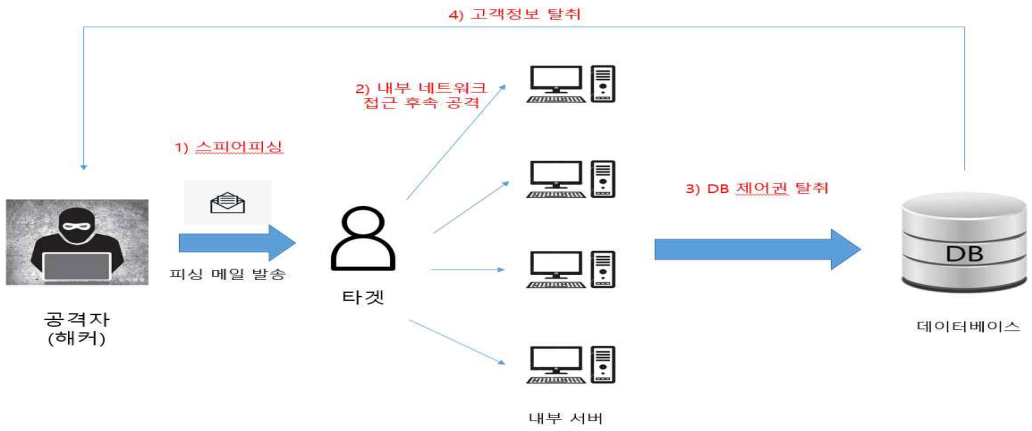
1990년대 미국의 가장 유명한 해커였던 케빈 미트닉(Kevin Mitnick)은 사회공학 기법을 가장 잘 사용한 사람으로 그는 이렇게 말했다. “정보보안의 가장 큰 위협은 컴퓨터 바이러스, 패치가 적용되지 않은 중요한 프로그램, 잘못 설정된 방화벽이 아니다. 바로 당신이다.”

실제로 그는 12세 때 사회공학 기법을 사용해 그 때 당시 LA의 버스 시스템에 사용되는 펀치 카드 시스템을 우회하여 LA지역의 모든 버스를 타고 다녔다고 한다. 그 후로도 모토로라, 썬마이크로시스템즈, 노벨 등 많은 회사들을 해킹을 했다. 그 중 모토로라사의 사건이 유명한데 그는 전화 몇 통만으로 모토로라사의 최신 핸드폰의 핵심 소스코드를 탈취했을 정도로 사회공학 기법에 능숙했다. 10여년이 지난 현재까지도 사회공학 기법이 많은 해커들이 사용하는 가장 효과적인 해킹 방법으로 해커들 사이에서 인식되어지고 있으며 최근에는 고도의 해킹 기술과 통합되어 많이 활용되어지고 있다.

이제부터 사회공학 해킹 기법에는 무엇이 있는지 사례를 통해 알아보자.

2.2.1 피싱

피싱은 사회공학 기법의 가장 대표적인 기술로 개인정보(private data)와 낚시(fishing)의 합성어이다. 전화, 문자, 메신저, 가짜 사이트 등 전기통신수단을 이용해 피해자를 기망, 공갈함으로써 이용자의 개인정보나 금융 정보를 빼낸 후, 금품을 갈취하는 사기 수법을 말한다.



[사진 1] 피싱 흐름도

2016년 유명했던 인터파크 회원정보 유출 사건이 있었다. 이 때 당시 약 2,000만 명이 넘는 고객 정보가 유출되었는데 사건의 발단은 인터파크 직원 1명을 표적으로 삼은 스피어피싱 공격이었다. 여기서 스피어피싱은 특정한 개인이나 회사들을 대상으로 시도하는 피싱 기법을 말한다.

민관협동조사단의 조사 결과에 따르면, 해커는 경영관리 직원인 A씨가 개인적으로 사용하는 국내의 한 포털사이트 메일의 ID와 PW를 먼저 가로챘다고 한다. 그 후 해커는 A씨가 평소 가족들과 이메일로 사진을 많이 주고받는다는 사실을 알아내 ‘우리 가족사진으로 PC의 화면 보호기를 만들었으니 열어봐라’라는 내용과 함께 파일을 여는 즉시 악성코드가 설치되는 압축파일을 넣어 가짜 이메일을 만들어 전송했다. A씨는 그 첨부파일을 열어보았고, 그 즉시 회사 PC에 침투한 악성코드는 인터파크 사내 전산망을 돌며 여러 PC를 감염시켰다. 수 일이 지난 후

고객 정보가 저장되어 있는 데이터베이스(DB) 서버를 관리하는 '개인정보 취급자PC' 제어권 탈취에 성공하고 개인정보를 유출했다. 이 때 해커는 PW관리 및 서버 접근통제 관리 등의 취약점을 이용해 인터파크 회원정보 2,665만 8,753건이 보관된 파일을 16개로 분할하고 직원PC를 경유해 외부로 유출한 것으로 조사됐다.

해당 사례에서 주요 이벤트를 보면 해커는 타겟이 이메일로 가족들과 사진을 주고받는다는 사실을 알아냈다. 그 후

1) 스피어피싱 메일을 보냈고
2) 첨부파일을 열어본 타겟의 PC는 악성코드에 감염이 되었고 그 즉시 내부 전산망을 타고 다른 PC까지 감염시켰다.
3) 그로부터 수 일이 지난 후 데이터베이스를 장악하여 고객 정보를 유출했다.

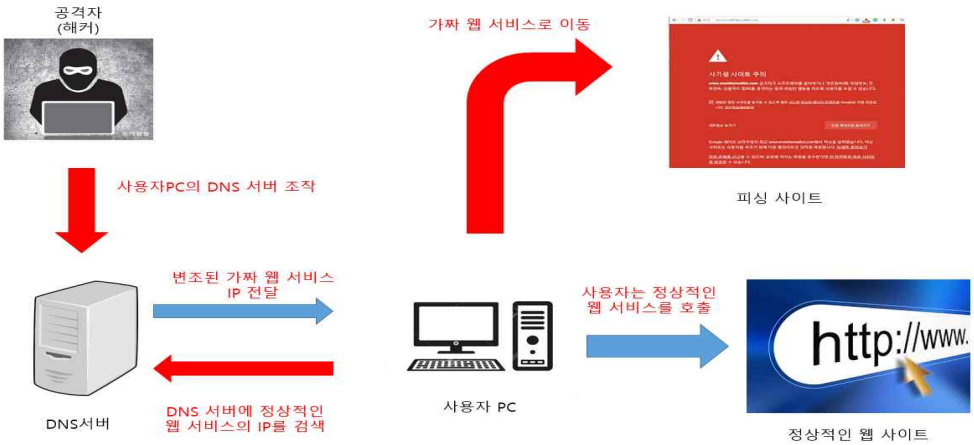
2.2.2 파밍

파밍(Pharming)은 넓은 의미에서 피싱(Phishing)의 한 유형으로 분류할 수 있다.

정확한 명칭은 'DNS Spoofing'이라고도 한다. 파밍은 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시켜 타겟의 정보를 탈취하는 공격 기법이다.

피싱과 파밍의 큰 차이점은, 먼저 피싱은 금융기관 등의 웹 사이트에서 보낸 이메일, 문자 메시지 등으로 위장해 사용자로 하여금 접속을 유도한 뒤 개인정보를 빼내는 방식이다.

다음으로 파밍은 해당 사이트가 공식적으로 운영하고 있는 사이트의 도메인 자체를 해커가 미리 준비해둔 개인정보탈취용 가짜 사이트로 중간에서 바꿔치기하여 개인정보를 빼내는 방식에서 피싱과 파밍은 차이가 있다.

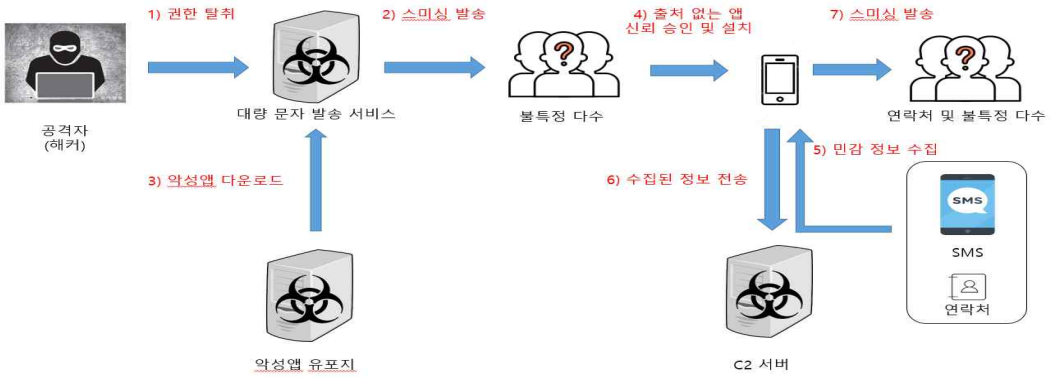


[그림 2] 파밍 흐름도

서울시 관악구에 거주하는 40대 초반의 주부 A(여)씨는 평소 자주 사용하는 본인 컴퓨터에서 인터넷 포털 사이트 검색을 통해 S은행에 접속했다. 그러나 A씨가 접속한 사이트는 해커가 만든 피싱 사이트였다. A씨는 피싱 사이트라는 것을 알아차리지 못한 채 팝업창에서 지시하는 대로 본인의 개인정보 및 계좌 정보와 보안카드 번호 등을 입력했다. 해커는 그 정보를 이용해 A씨의 이름으로 공인인증서를 발급받고 인터넷 뱅킹을 통해 A씨의 계좌에서 약 2000만원 가량을 이체했다.

2.2.3 스미싱

스미싱(Smishing)은 문자메시지 피싱(SMS Phishing)이라고도 하며, 문자메시지(SMS)와 피싱(Phishing)의 합성어이다. 이름에서도 알 수 있다시피 문자메시지를 이용한 피싱이다.



[사진 3] 스미싱 흐름도

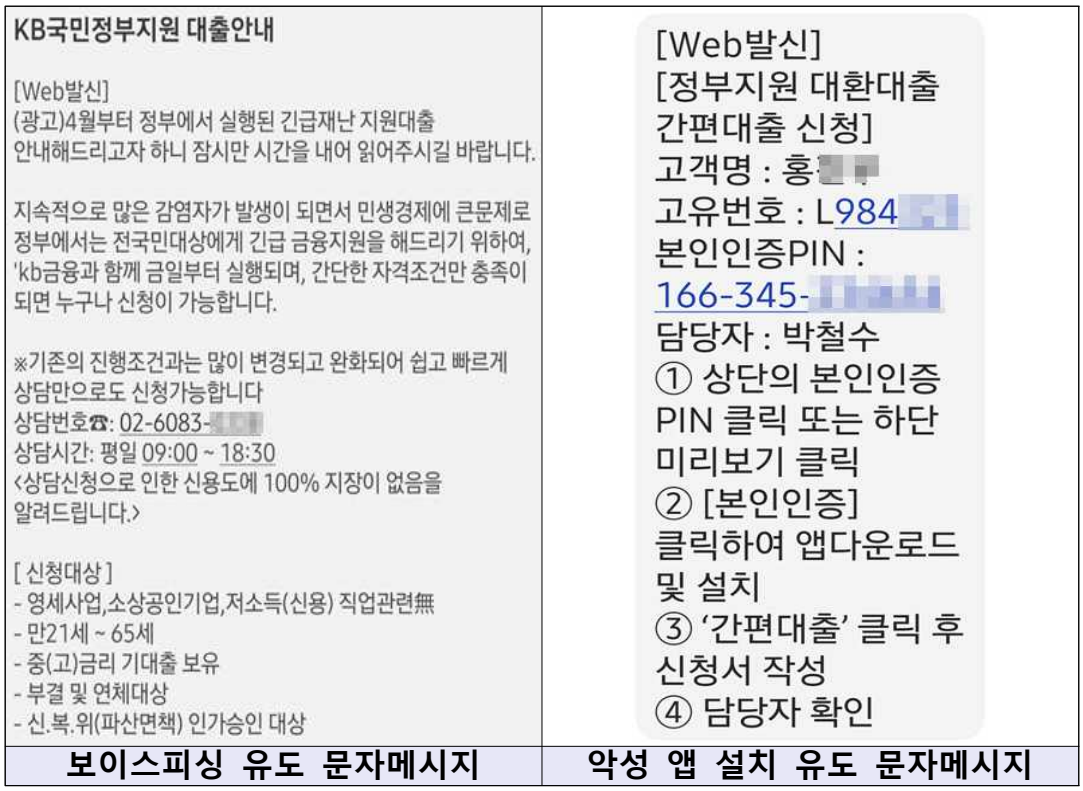
사례 1) 대출금리비교 앱(App)을 사칭하여 돈을 송금하게 한 사례

피해자 A씨는 캐피탈을 사칭한 공격자로부터 '스마트폰에 특정 앱(App)을 설치하면 본인의 신원 확인 및 대출이 가능하다'는 내용의 전화를 받은 후 해당 프로그램을 설치하였고, 앱을 실행하자 여러 금융기관의 전화번호 목록이 확인되었으며 피해자 A씨가 대출을 이용 중인 대부업체에 상환방법을 문의하고자 전화통화를 시도(앱 상에서의 통화 연결 기능)를 하였으나 피해자 A씨가 설치한 앱은 통화 연결 시 자동으로 특정번호(공격자)에게 전화가 연결되었고 공격자가 알려준 상환계좌로 돈을 송금하여 피해를 입었다.

(출처 : 미래창조과학부 등 보도자료, "신·변종 전자금융사기 합동 경보 발령 !", 2013. 8. 29. 참조)

사례 2) 코로나19 관련 스미싱

코로나19로 인해 경기침체가 장기화됨에 따라 많은 국민들이 곤경에 처했다. 정부는 이를 극복하고자 긴급재난지원금 제도를 편성하였다. 많은 사람들은 긴급재난지원금에 관심을 갖고 신청하거나 순번을 기다리고 있다. 무서운 사실은 이러한 사회적 현상을 악용하여 해커들이 공격을 시도하고 있다는 것이다.



[표 1] 실제 스미싱 문자

(출처 : 금융감독원 – http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp?seqno=23092)

위 사진은 실제 스미싱 문자 사진이다. 이를 읽어보면 전혀 의심이 가지 않을 뿐만 아니라 납득이 가는 내용이다. 일반적인 상황에 놓인 사람에 비해 경제적으로 어려움을 겪고 있는 사람이라면 평소와 달리 이성적인 판단이 흐려져 현혹될 위험이 높다. 해커들의 기술은 그와 더불어 사회적 현상까지도 이용하여 고도로 발전되어가고 있다.

3. 코로나와 사회공학적 해킹의 관계

3.1 코로나 관련 주요 키워드의 악용

최근 국내, 국외 할 것 없이 코로나19 바이러스에 대한 사람들의 불안감에 편승하여 마스크 무료 배포, 긴급재난 지원금 등을 사칭한 스미싱 문자, 코로나19 관련 키워드를 악용한 도메인이 증가하고 있다. 국내에 한국인터넷진흥원(KISA)에 따르면 코로나19 사칭 악성앱 유포지가 35건, 유출지 24건으로 조사되었다.

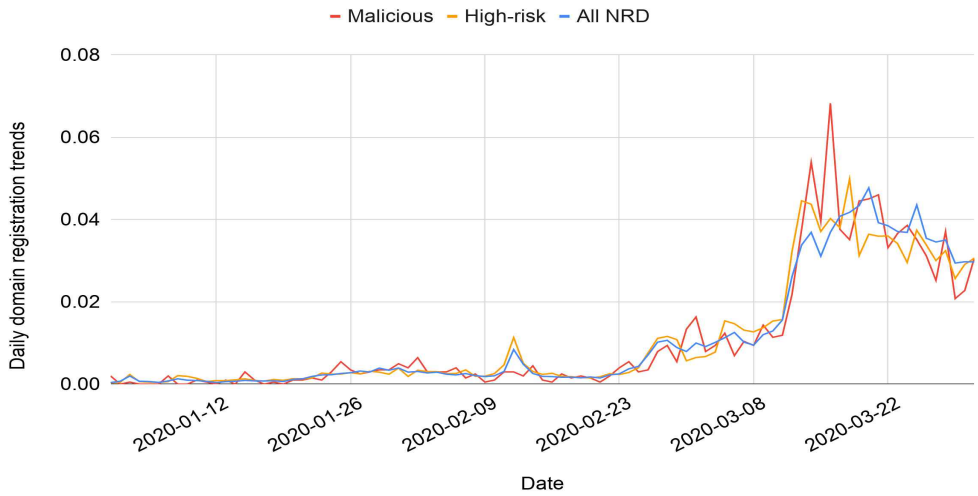
또한 국외에서는 보안업체인 팔로알토(Palo Alto)에서 최근 코로나19를 주제로 한 도메인이 증가하고 있음을 발표하였다. 2020년 올해 1~3월 사이에 신규 등록된 도메인을 분석한 결과, 약 2,000개 이상의 악성 도메인과, 약 40,000개 이상의 고위험군의 도메인이 있었으며, 2~3월 사이에는 신규 도메인 등록이 569% 증강한 것으로 나타났다고 한다. 이 중에서 주요 키워드 ('covid', 'covidvirus', 'covid19'등)의 비율이 약 40% 되는 것으로 조사되었다.

언택트(Untact) 사회가 앞당겨져 오면서 네트워크상에서의 작업이 증가했다. 많은 사람들이 일상의 많은 것(금융거래, 인터넷 쇼핑 등)을 인터넷으로 해결하고 있다. 또한 코로나19가 지속되면서 사람들의 불안감이 고조되고 있다. 이러한 사회적 변화를 감지한 해커들로부터 앞서 언급한

키워드를 미끼로 피싱 공격, 스미싱, 파밍 등 사회공학 기법을 사용한 사이버범죄를 시도되어지고 있다.

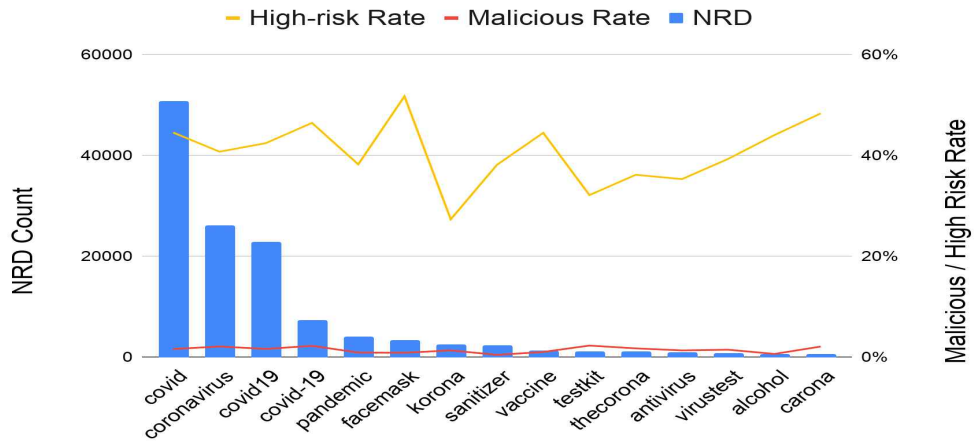
구분	내용	상세
Domain	sd23s[.]xyz	유포지
Domain	sdge3[.]xyz	유포지
Domain	mshue[.]xyz	유포지
Domain	hanjumsu[.]com[.]cn	유포지
Domain	psigz[.]xyz	유포지
Domain	directsend[.]pro	유포지
Domain	sefss[.]xyz	유포지
Domain	sdx3g[.]xyz	유포지
Domain	swusy[.]xyz	유포지
Domain	htwes[.]xyz	유포지
Domain	prves[.]cc	유포지
Domain	nsbve[.]xyz	유포지
Domain	wsgxc[.]xyz	유포지
Domain	nhueg[.]xyz	유포지
Domain	mnseg[.]xyz	유포지
Domain	ywuhg[.]com	유포지
Domain	muwht[.]xyz	유포지
Domain	uwygs[.]xyz	유포지
Domain	gnwzw[.]com	유포지
Domain	cnxw[.]com[.]cn	유포지
Domain	qpw85d8g[.]cn	유포지
Domain	qpw85ndm[.]cn	유포지
Domain	qpw85ec3[.]cn	유포지
Domain	eobua[.]com	유포지
Domain	uerfh[.]cn	유포지
Domain	zqbsi[.]xyz	유포지
Domain	deoimnb[.]xyz	유포지
Domain	hh59hf[.]com	유포지
Domain	sywhe[.]cn	유포지
Domain	boxcloud[.]com(미국의 정상파일공유서비스, 2개 계정 조치 요청)*	유포지
Domain	sxssz[.]xyz	유포지
Domain	dfcvz[.]xyz	유포지
Domain	y-t[.]top	유포지
Domain	y-w[.]top	유포지
Domain	foenapp[.]com	유출지
Domain	wambiq[.]com	유출지
Domain	gxquf[.]net	유출지
IP Address	103[.]126[.]160[.]33	유출지
IP Address	103[.]126[.]160[.]34	유출지
IP Address	114[.]25[.]68[.]120	유출지
IP Address	171[.]244[.]19[.]177	유출지
IP Address	171[.]244[.]19[.]183	유출지
IP Address	171[.]244[.]19[.]185	유출지
IP Address	171[.]244[.]19[.]167	유출지
IP Address	1[.]164[.]168[.]19	유출지
IP Address	171[.]244[.]19[.]239	유출지
IP Address	171[.]244[.]19[.]135	유출지
IP Address	171[.]244[.]19[.]250	유출지
IP Address	171[.]244[.]19[.]241	유출지
IP Address	45[.]145[.]81[.]76	유출지
IP Address	193[.]47[.]61[.]59	유출지
IP Address	36[.]239[.]253[.]168	유출지
IP Address	45[.]135[.]117[.]175	유출지
IP Address	45[.]128[.]145[.]12	유출지
IP Address	103[.]80[.]26[.]218	유출지
IP Address	36[.]110[.]236[.]114	유출지
IP Address	58[.]82[.]243[.]78	유출지

[사진 4] 코로나 19 사칭 악성 앱 유포지(35건) 및 유출지(24건)
(출처 : 한국인터넷진흥원 :
https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=35290)



[사진 5] 일일 코로나 바이러스 관련 도메인 등록 동향

(출처 :Palo Alto https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/)

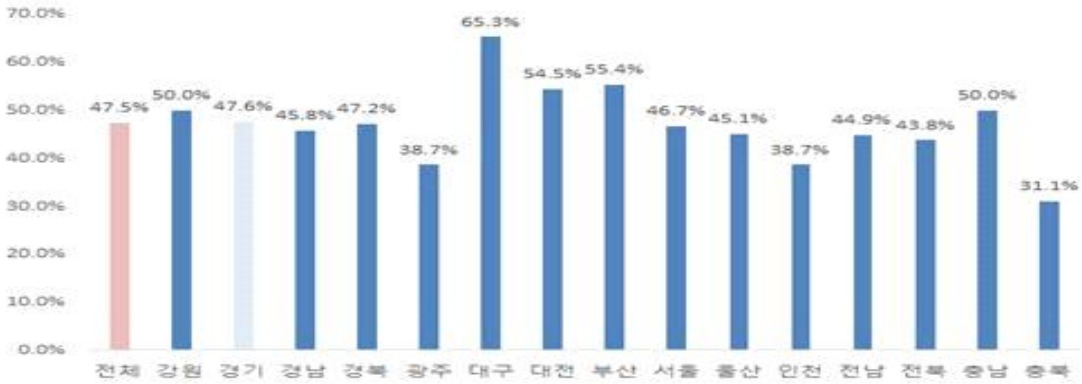


[사진 6] 신규 등록 도메인에서 가장 많이 사용되는 주요 키워드

(출처 : Palo Alto https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/)

3.2 코로나로 인한 정신건강 피해

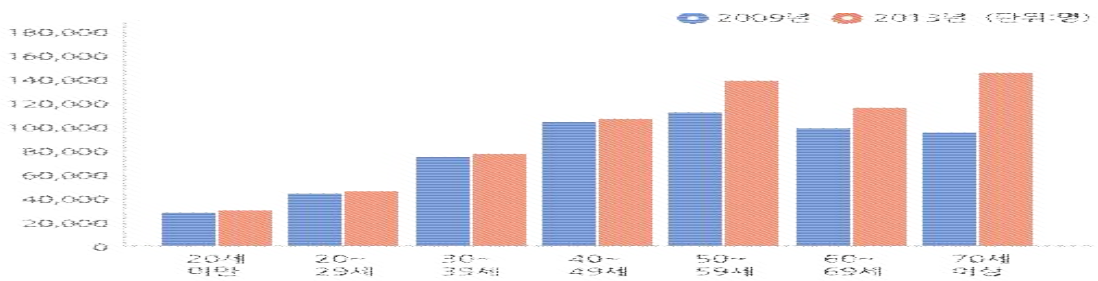
코로나19의 장기화로 사람들의 정신 건강도 악화되고 있는 실정이다. 실제로 우리나라 국민의 47.5%는 불안/우울감을 경험하고 있다고 보도되었다.[1] 경기연구원에서 지난 4월, 전국 17개 광역시도 15세 이상, 약 1500명을 대상으로 실시한 바 있다. '코로나19로 인한 국민 정신건강 설문조사'에서 특히 대구시민이 전국 평균보다 약 20% 높은 65.3%로 나타났다.



[사진 7] 지역별 불안/우울감 수치
(자료 : 경기연구원(2020), 코로나19로 인한 국민 정신건강 실태조사)

이와 같은 현상을 악용한 사례들도 많이 보인다. 대표적으로 코로나 블루[2]로 사람들의 외로움을 이용한 로맨스 스캠이 대두되고 있다. 로맨스 스캠은 SNS와 메일 등 온라인으로 피해자에게 접근하여 이성적 관심을 가장해 재력, 외모 등으로 신뢰를 형성한 후 각종 이유로 금전을 요구하는 방법의 사기이다. 특히 장년층(50~60) 이상이 당하는 경우가 많다.

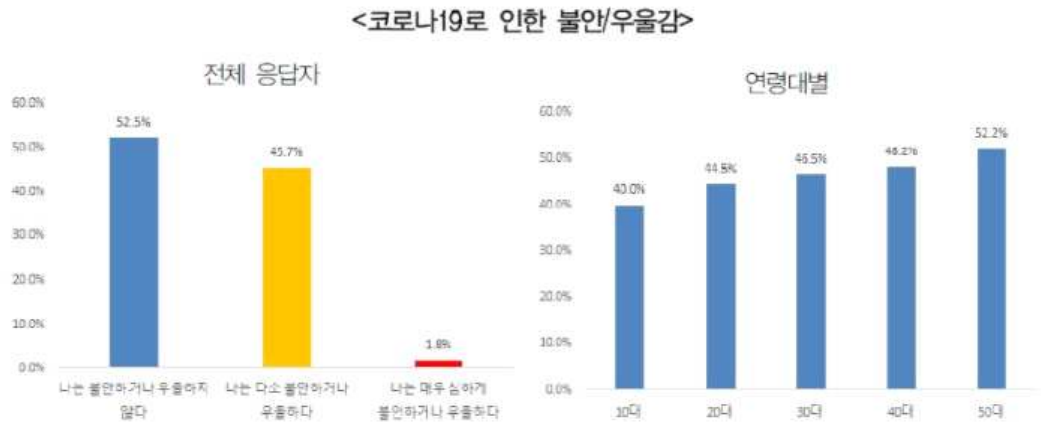
장년층(50~60)의 경우 많은 회사나 일자리에서 은퇴를 하는 연령대이며 그로 인해 사회경제적 박탈감을 다른 연령층에 비해 많이 경험해 우울감이 높아진다. 공격자들이 그러한 장년층의 심리를 악용해 피해자로 많이 선정하게 되는 것이다. 하지만 2020년 현재 코로나19 바이러스의 장기화로 사람들의 불안/우울감은 날이 갈수록 증가하고 있다. 이제는 청년층, 장년층에 관계없이 누구에게나 일어날 수 있는 현실이다.



[사진 8] 연령별 우울증 진료인원
(출처 : 건강보험심사평가원
http://www.hira.or.kr/re/stcIlnsInfm/stcIlnsInfmView.do?pgmid=HIRAA030502000000&sortSno=179)

---

1) 비전21뉴스 (https://www.vision21.kr/news/article.html?no=97322)
2) 코로나19와 우울감(Blue)이 합쳐진 신조어로 코로나19의 확산으로 일상에 큰 변화가 닥치면서 생긴 우울감이나 무기력증을 뜻한다.



[사진 9] 코로나19로 인한 불안/우울감
(출처 : 경기연구원(2020), 코로나19로 안한 국민 정신건강 실태조사)

4. 사회공학적 해킹의 대응방안

4.1 피싱에 대한 대응방안

피싱 대응방안은 크게 사용자 측면과 서버 측면 두 가지로 볼 수 있다.

4.1.1 사용자 측면에서의 피싱 대응방안

일반 사용자의 측면에서 봤을 때, 피싱 공격에 대한 대응은 사회공학적인 공격을 어떻게 대응 할 것인가에 초점이 맞춰진다.

가장 중요한 것은 어떤 형태로든 수신된 메시지에 대해 꼼꼼한 검토를 통해 피싱 공격의 여부를 확인하는 것이다. 특히, 그 내용이 중요정보를 요구하는 경우에는 더욱 그러하다.

일단, 문자 수신시 출처가 불분명한 사이트의 주소는 클릭을 자제하고 바로 삭제한다. 또한 잘 알지 못하는 사용자로부터 온 이메일은 피싱임을 의심할 필요가 있다. 첨부된 파일은 바이러스 혹은 악성코드임을 의심할 필요가 있다.

의심되는 사이트 주소의 경우 정상 사이트와 일치여부를 확인하여 피해를 예방하며, 휴대폰번호, 아이디, 패스워드 등 개인정보는 신뢰된 사이트에만 입력하고 인증번호의 경우 모바일 결제로 연계될 수 있으므로 한 번 더 확인하는 노력이 필요하다.

- 인터넷 브라우저에서의 차단 기능 활용
- 광고 홍보성 메일 차단 기능 활용
- 이메일 전자서명 첨부 기능 활용
- 일반적 보안 준수 사항 고지

4.1.2 서버 측면에서의 피싱 대응방안

서버 측면에서의 피싱 대응방안은 클라이언트가 해당 사이트에 접근하기 위해 스마트카드와 같은 물리적 토큰을 같이 사용하게 함으로써 웹 사이트로부터 강력한 인증을 받도록 한다. 또한 자원에 대한 피싱 방어기술 구현을 위해 피싱 위협에 대한 교육과 피싱의 원인을 제거하는 내부적 업무 지침 및 기술 개발에 대한 노력이 필요하다.

- 피싱 피해 사례 및 교육자료 배포

- 전자서명 및 이메일 검증
- 보안을 고려한 웹 응용프로그램 개발
- 강력한 인증 시스템 구축
- 라우터 및 게이트웨이 보호
- 도메인 관리

4.2 파밍에 대한 대응방안

파밍에 대한 대응방안으로 사용자들이 할 수 있는 것은 실제로 피싱에 대한 대응방안을 잘 준수하는 것이다. 또한 웹 사이트의 스푸핑을 막을 수 있는 장치를 적용하고 웹브라우저의 보안 레벨을 높여야 한다. 이 외 파밍에 의한 피해를 방지하기 위한 방법으로 사이트 관리자는 자신의 도메인이 변경되지 않도록 도메인 등록기관에 도메인 잠금 기능을 신청하여 사용하도록 한다. DNS 서버 관리자는 DNS에 관련된 취약점을 제거하여 해당 시스템이 침해를 당하지 않도록 해야 한다.

호스트 파일의 임의 변경을 막고, DNS 정보, Proxy 설정 변경 등 악성코드에 의해 시스템이 변조되는 것을 막고 이미 감염된 PC에서 악성코드의 기능이 발휘되지 못하도록 제어해야 한다.

혹여 파밍으로 인해 금융피해를 본 경우 신속히 경찰서나 금융회사 콜센터를 통해 지급정지 요청을 한 후 해당 은행에 경찰이 발급한 '사건 사고 사실 확인원'을 제출하여 피해 금액 환급 신청을 한다. 악성프로그램에 감염이 된 경우 한국인터넷진흥원 보호나라의 PC원격 점검 서비스 또는 '파밍캅'프로그램을 다운로드 받아 치료하는 것이 좋다.

4.3 스미싱에 대한 대응방안

스미싱에 대한 대응방안으로 스미싱 메시지가 왔을 때 인터넷주소를 클릭하여 사이트 접속을 통해 특정 애플리케이션을 설치했다면 악성코드의 감염을 의심해야한다. 악성 앱 감염이 의심이 된다면 모바일 백신으로 악성 앱을 삭제하거나 수동으로 악성 앱을 삭제한다. 그 후 서비스 센터를 방문하는 것이 좋다.

스미싱 악성 앱에 감염되면 모바일 결제 피해가 발생할 수 있다. 따라서 이동통신사에 모바일 결제 내역이 있는지 확인해야한다. 모바일 결제 피해가 확인이 되면 피해 의심 스미싱 문자를 캡쳐하여 통신사 고객센터를 통해 스미싱 피해 신고 및 '소액결제확인서'를 발급 받는다.

소액결제 확인서를 지참하여 관할 경찰서 사이버수사대 또는 민원실 방문하여 사고 내역을 신고한다. 사고 내역을 확인 받고 '사건사고 사실 확인서'를 발급 받는다. 사건사고 사실 확인서 등 필요서류를 지참하여 통신사 고객센터 방문 또는 온라인으로 서류를 발송한다. 그 후 통신사나 결제대행 업체에 사실 및 피해 내역 확인 후 피해보상을 요구한다.

스미싱 2차 피해를 막기 위해서 주변 지인들에게 스미싱 피해 사실을 알리고 특정 악성 앱 삭제 방법을 확인 후 삭제를 꼭 해준다.

5. 결론

코로나19로 인해 온라인, 비대면 상황이 지속되면서 인터넷 사용 빈도가 급증했고, 중요 정보들이 인터넷을 통해 송수신 되는 양 또한 많아졌다. 뿐만 아니라 심리적인 고립감, 우울감 등으로 인한 정신질환을 앓고 있는 사람들이 늘어났다. 이를 악용해 공격자(해커)들은 쉽게 정보를 얻기 위해 기술적인 해킹 기법보다 사람들의 심리적 요인을 이용하는 비 기술적 해킹 기법인 사회공학적 해킹을 많이 사용하게 되었다. 사회공학적 해킹 공격의 수법으로 본 논문에서는 피싱, 파밍, 스미싱을 알아보고 대응방안에 대해 이야기를 했다.

코로나19라는 범지구적 재난으로 많은 사람들이 힘들어 하고 있다. 공격자(해커)들은 이러한 상황마저도 이용해 자신들의 이익을 챙기려 하고 있다. 본 논문에서 알아본 사회공학적 해킹과 그 종류, 그리고 그에 따른 대응방안을 잘 준수하여 공격자(해커)들에게서 피해를 받지 않도록 주의해야 하며, 취미활동, 여가생활을 즐기며 정신건강 또한 함께 챙기는 것이 포스트 코로나 시대에 살아갈 우리들의 자세일 것이다.

참고문헌

1) 이정민 - 사회공학적 해킹 위협 대응방안에 대한 연구, 건국대학교 정보통신대학원 정보통신학과, 2013

2) 최준성, 국광호 - 국내방산업계 사회공학적 공격 동향과 대응 방안, 한국방위산업학회지, 2012

3) 김준석, 강현재, 김진수, 김휘강 - 보안 위험 평가를 위한 사회공학 공격 그래프, 한국컴퓨터정보학회, 2018

4) 김정훈, 고준영, 이근호 - 빅데이터 기반의 융합 보이스피싱을 이용한 사회공학적 공격 기법과 대응방안, 백석대학교 정보통신학부, 2015

5) 이동휘, 최경호, 이동춘, 김귀남, 박상민 - 사회공학기법을 이용한 피싱 공격 분석 및 대응기술, 융합보안논문지, 2006

6) 최양서, 서동일 - 사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석, 한국정보보호학회, 2006

7) 김도우, 이규범 - 사회공학적 공격기법의 유형분류, 한국산업보안연구, 2019

8) 박재혁, 이재우 - 인간의 감정 상태를 이용한 사회공학 기법 연구, 한국정보보호학회, 2015

9) 인터넷침해대응센터 침해사고분석단 종합분석팀 - 피싱 메일 공격 사례 분석 및 대응방안, 한국인터넷진흥원, 2018

10) 강지윤, 윤지혜, 김윤정 - 피싱/파밍 사례 및 대응방안 분석, 한국정보과학회, 2013

11) 이응용 - 코로나19(COVID-19)를 이용한 사이버공격 및 대응 동향, 한국인터넷진흥원, 2020

12) 전효제 - 팬데믹(Pandemic)시대의 개인정보보호, 한국인터넷진흥원, 2020

13) 이진규 - 코로나 바이러스와 개인정보 활용에 대한 소고, 한국인터넷진흥원, 2020

14) 네이버 블로그 (https://blog.naver.com/gowit_sps/221560575171)

15) 보안뉴스 권 준 기자 - 코로나19 악용 사이버공격 급증... 자가격리하듯 '망분리'로 원천 차단해야 (https://www.boannews.com/media/view.asp?idx=87716), 2020

16) pplus news - 코로나19로 인해 변화된 사이버 위협과 보안 솔루션의 필요성 (https://pplus.co.kr/news/?uid=307&mod=document), 2020

17) 국민대학교 신문방송사 - 포스트 코로나 시대의 정보보기술 (http://press.kookmin.ac.kr/news/articleView.html?idxno=101487), 2020

18) 중앙일보 김창우 기자 - 개인정보 유출, 사람 속여 빼돌리는 '사회공학'에 당한다 (https://news.joins.com/article/23712554), 2020

19) ddaily 이종현 기자 - 코로나19가 불러온 언택트 시대, 해킹 공격도 늘었다. (http://www.ddaily.co.kr/news/article/?no=196950), 2020

20) 오미애(정보통계연구실 빅데이터, 정보연구센터장), 전진아(보건정책연구실 건강정책연구센터장) - 코로나바이러스감염증-19 소셜 빅데이터 기반 주요 이슈 분석, 한국보건사회연구원, 2020.03.17.

21) 비전21뉴스 - 국민 절반 코로나19 우울감 호소, 2020.05.19. (http://www.vision21.kr/news/article.html?no=97322)

22) Palo Alto https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/