언택트 시대의 보안 위협 및 대응 솔루션

지도교수 : 김 윤
연 구 자 : 김 나 영

< 목 차 >

요 약

2019년 갑작스럽게 닥쳐온 코로나바이러스감염증-19로 인해 우리의 일상은 많은 부분이 변화하였다. 그 중에서도 최대한 사람과 접촉하지 않는 언택트(Untact)시대가 도래 했다는 점이 가장 큰 변화일 것이다. 이러한 시대는 우리에게 많은 편리함과 유용함을 가져다주었다. 하지만 편리한 일상 속 보안을 위협하는 상황 또한 생겨났다. 이에, 본 논문은 언택트 시대를 살아가는 우리의 일상 속에 어떠한 보안 위협이 존재하는지, 그러한 위협을 어떻게 예방하고 대비하는 지에 대한 대비책을 알아보고자 한다.

주요어 : 코로나19, 언택트, 비대면, 일상, 보안, 공격, 대응 방법

1. 서론

1.1 언택트 시대의 정의

기존 의미의 언택트(Untact)란 '콘택트(contact: 접촉하다)'에서 부정의 의미인 '언(un-)을 합성한 말로, 기술의 발전을 통해 점원과의 접촉 없이 물건을 구매하는 등의 새로운 소비 경향을 의미하였다.

하지만 코로나 바이러스 이후 사회적 거리 두기 확산에 따라, 언택트 소비가 일상화되면서 언택트 시대는 새로운 패러다임으로 등장하였다. 대표적으로 언택트 금융, 언택트 근무, 언택트 수업 등의 방식들이 사회 전반으로 확산되고 있다.

이런 방식으로 '언택트'라는 단어는 시대의 흐름에 따라 의미가 확장되어지고 있는 추세이다. 단어의 의미가 확장됨에 따라 우리의 일상에도 넓은 영향을 끼치고 있는데, 구체적인 예시와 이에 대한 보안 위협 및 대응 방안에 대해서는 다시 자세히 다루도록 하겠다.

1.2 언택트 시대의 동향

구분	개요	플랫폼
재택근무 (화상회의)	▶현황 : SK텔레콤, KT 등 통신회사와 삼성, LG, 네이버 등 IT 기업들을 선두로 재택근무 추진 ▶예시 : PC 로그온 → 클라우드 시스템 접속 → 사내 이메일 체크 → 화상회의 → 사내 메신저로 채팅 → 업무시간 종료(로그오프) ▶활용기술 : 그룹메신저, 원격회의 시스템, 원격 PC제어 등	·ZOOM ·MS 팀즈 ·Remote Meeting ·Webex ·TeamViewer
온라인 개학	▶현황: 한 달 만에 초중고 전원 온라인 개학 ▶특징: 학교별 온라인 학습 플랫폼과 진행방식 (실시간, 동영상 녹화, EBS 콘텐츠 이용 등)이 상이함 ▶문제점: 서버 마비, 해킹 등 보안 문제, 부정 수강 등	·EBS 온라인 클래스 ·e학습터 ·구글 클래스룸 ·네이버 밴드 ·위두랑 ·리로스쿨
원격 의료	▶현황: 2/24일 코로나19 의료기관 감염 방지를 위해 전화 상담 및 처방을 한시적으로 특례 인정 (보건의료기본법 근거) ▶원격 의료 추진 실적: 2/24~4/12일까지 3,072곳 참여, 진료 건수 10만 3,998회, 진료금액 12억 8,813만원(중앙재난안전대책본부)	·메디히어 ·굿닥 ·코로나119

[표 1] 언택트 서비스 사례

[표 1]을 보면 알다시피 다양한 종류의 언택트 서비스가 늘어나면서 진정한 언택트 시대의 포문을 연 것을 볼 수 있다. 언제 어디서나 시간과 장소의 구애를 받지 않고 편리한 서비스를 이용할 수 있다는 점이 언택트 서비스의 가장 큰 장점이라고 볼 수 있다.

이외에도 배달앱, 키오스크 주문, 셀프 계산대 등 우리의 일상 속에 조그마하게 자리 잡은 비대면 서비스도 언택트 서비스라고 할 수 있다.

하지만 너무 갑작스러운 변화에 따라가기 벅찼던 것일까, 특히 고령 연령층에서는 언택트 서비스에 적응하지 못하여 많은 서비스 이용에 제한을 받고 있고, 무엇보다 이번 논문의 쟁점인 보안 쪽으로도 악의적인 해커들 또한 언제 어디서나 시간과 장소에 구애를 받지 않고 쉬운 방식으로 이용자들의 보안을 위협하고 있다.

따라서 이번 논문에서는 언택트 시대가 가져온 보안위협 및 보안 솔루션에 대해 알아보고자 한다.

2. 본론

2.1. 일상 속의 언택트

2.1.1 언택트 금융거래

비대면 금융생활서비스 중 가장 보편화 된 것은 삼성페이와 같은 간편결제 서비스와 오픈 뱅킹 서비스이다. 먼저 간편결제 서비스는 플라스틱 카드 대신 어플을 이용하여 온/오프라인 결제에 이용하는 방식으로, 앱카드 결제 서비스로 확장되어가고 있다. 그리고 오픈 뱅킹은 카카오, 네이버와 같은 대기업이나 토스, 뱅크샐러드 등의 핀테크 기업들이 모든 은행의 자금을 조회하여 사용자의 전재산을 비롯해 이체 및 조회 서비스를 제공한다.

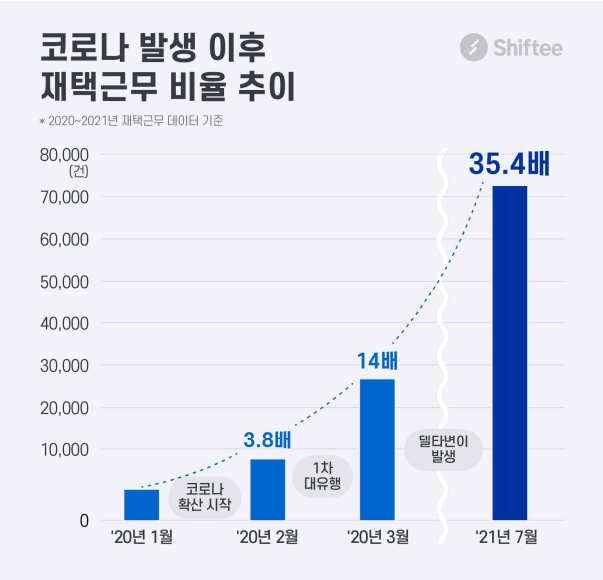
20년 2월 23일 기준	
총 가입자수	2,060명
은행	533만명
핀테크	1,507만명
총 등록 계좌 수	3,586만 계좌
은행	1,479만 계좌
핀테크	2,107만 계좌

[표 2] 핀테크 금융서비스

2.1.2 언택트 근무

전 세계적으로 코로나가 확산되면서 국내에서 감염접촉의 가능성을 감소시키기 위한 사회적 거리두기의 일환으로 다수의 기업에서 비대면 근무체계를 추진하였다.

동일공간에서 대면방식으로 수행되던 근무체계를 비대면 방식으로 전환하기 위해서는 직원들 간의 커뮤니케이션이나 업무 이력관리, 정보유출 가능성 등 생각보다 많은 조건들을 고려해야 한다.



[사진 1] 코로나 발생 이후 재택근무 비율 추이

최근 정보통신 기술의 발달로 일반 사무직 등 재택근무가 가능한 직무가 더욱 많아지는 추세이다.

통합 인력관리 솔루션 Shiftee에서는 지난 2년간 사업장의 근무 형태 변화에 대한 설문을 진행하여 분석한 결과, 코로나19 발생 이후 재택근무 비율이 크게 증가했다고 밝혔다.

정부에서는 상대적으로 재택근무가 쉽지 않은 환경에 놓여 진 중소기업을 위해 재택근무 컨설팅 사업을 지원하는 등의 방법으로 적극적으로 재택근무를 권장하는 행보를 보이고 있다.

2.1.3 언택트 수업

직장인들은 언택트 근무를 한다면, 학생들은 언택트 수업을 진행한다. 수업은 녹화 수업과 실시간 수업으로 나뉜다.

녹화 수업은 강의자가 미리 녹화해둔 영상을 학생들이 조회하는 방식으로 진행한다. 이와 같은 경우에는 서로의 카메라와 마이크를 공유하지 않고 개인적으로 녹화 영상만 보기 때문에 보다 안전한 방법이라고도 볼 수 있다.

실시간 수업은 ZOOM, Webex 등과 같은 비대면 회의 프로그램을 이용하여 언택트 수업을 실시한다. 한 명의 대표가 회의 방을 만들어서 다수의 인원에게 초대 코드를 보내는 방식으로 진행되며, 웹 캠과 마이크 기능을 이용하여 회의실 안의 인원들끼리 서로의 화면을 공유한다.

따라서 실시간 수업은 녹화 수업에 비해 개인의 사생활 노출이 가능한 환경이 만들어지고, 언제 어디서 어떠한 변수가 생길지 모른다는 단점이 존재한다. 특히 비대면 회의 프로그램이 활성화되면서 많은 보안 문제를 일으키고 있는데 밑의 내용에서 이와 같은 문제점에 대한 자세한 분석을 해보고자 한다.

3.1. 언택트 시대의 보안 위협

3.1.1. 줌바밍 (Zoombombing)

최근 Zoom 회의 도중 제 3자가 회의 방에 무단 참석하여 인종차별이나 종교 비하발언, 음란영상 공유 등의 행위로 인해 정상적인 회의 진행을 방해하는'줌바밍(Zoombombing)'공격으로 인해 화상회의 솔루션의 안전성에 대한 논란이 끊이지 않고 있다.

```
while isture == 'true':
    rand=random.uniform(0,1)

    // 9~10자리의 숫자로 이루어진 랜덤 ID 생성
    if rand > 0.5:
        id=random.randrange(10000000, 999999999, 6)
    else
        id=random.randrange(10000000, 999999999, 6)

    // 회의방 UPL에 랜덤 ID를 추가
    joinid ='https://zoom.us/wc/join/' + str(id)
    print("typing code " + str(id))

    // 위에서 조합한 URL을 가지고 회의방에 접근 시도
    browser.get((joinid))

    // 회의방에 접근이 가능한지 체크
    if len(browser.find_elements_by_id('inputname')) > 0:
        print('Code ' + str(id) + 'works!')
```

[사진 2] 줌바밍(Zoombombing) 공격 코드

줌바밍 공격이 가능한 것은 Zoom 가입 시 주어지는 9~10자리의 숫자로 구성된 ID를 이용하여 회의 방이 생성되는 구조를 이용하여 무작위 대입공격을 통해 랜덤으로 ID를 생성해 활성화된 회의 방을 발견하면 임의의 사용자도 활성화된 회의 방에 참석이 가능하게 된다.

그리고 회의방 참석 URL 주소인 https://zoom/us/wc/join/[사용자ID]에서 사용자 ID 부분에 랜덤 함수를 만들어서 숫자를 입력하고, 응답 값이 존재하면 그에 상응하는 회의에 참석하면 된다.

[사진 3] 공격 결과

3.1.2. 스미싱 (Smishing)

스미싱(smishing)은 문자메시지(SMS)와 피싱(Phising)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량으로 전송 후 이용자가 악성 앱을 설치하도록 유도하여 금융정보 등을 탈취하는 신종 사이버 공격이다.

스미싱은 1990년대부터 있었던 이메일 기반 피싱(Phishing)의 변형인 문자 메시지 중심의 사기 행위다. 그러나 보통의 사람들은 컴퓨터보다 휴대폰에서 의심스러운 메시지에 노출이 되기에 이메일 메시지보다 의심스러운 문자 메시지를 열어볼 가능성이 더 높다. 그리고 개인 기기에는 일반적으로 회사에서 사용할 수 있는 보안 조치가 부족하다. 이 오래된 속임수에 대한 악명은 점점 더 널리 퍼지고 있다

스미싱은 보통 악성코드를 클릭하도록 유도하는 공격의 형태가 가장 보편적이다. 한 가지 예시를 들자면, 체코에서 공격자가 사용자에게 해당 국가의 우편 서비스에서 제공되는 앱을 다운로드하도록 유도했던 사례가 있다. 실제로 이는 스마트폰의 다른 앱에 입력된 신용카드 정보를 수집할 수 있는 트로이목마 관련 악성코드였다.

이 외에도 사용자를 속여 자격 증명을 공개하도록 유도하는 공격과 같이 공격자는 사용자가 온라인 계정 가운데 하나에 로그인할 때 사용할 수 있는 사용자 이름과 비밀번호 또는 기타 기밀 정보를 드러내도록 유도한다. 특히 계좌번호나 폰뱅킹을 이용한 뱅킹 스미싱(bank smishing)은 가장 공격 성공률이 높고 흔한 공격 유형 가운데 하나다.

마지막으로 송금 사기 또한 굉장히 보편적인 공격의 형태 중 하나이다. 이런 유형의 스미싱은 기술적인 해킹보다 사기에 가깝지만, 성별과 나이에 무관하게 가장 피해가 극심한 공격이기에 보다 많은 사람들이 주의해야할 필요가 있다.

[사진 4] 스미싱 문자 사례

3.2 보안 취약점 대응 솔루션

3.2.1 원격협업도구 및 VPN 취약점 셀프 점검

원활한 재택근무 및 온라인 수업을 위해 원격협업도구를 사용하는 사람들이 많아졌다. 이에 따라 원격협업도구의 보안 취약점이 잘 드러나 줌바밍(Zoombombing) 공격과 같은 여러 피해가 급증하고 있다.

몇몇 기업들과 사람들은 외부에 보안 취약점이 드러나는 것을 대비하기 위해 VPN이라는 가상 사설 네트워크를 통해 내부적으로 업무를 처리하며 나름의 보안을 지키려는 노력을 하고 있다.

하지만 많은 사람들이 사용할수록 많은 취약점 또한 널리 퍼지게 될 수밖에 없다. 보안을 지키기 위한 여러 노력들이 무색하게 되기 전에 셀프 체크리스트를 통하여 본인의 보안 취약점은 어떤 부분에서 드러나고 있는지, 어떤 행동을 취해야 보안을 지킬 수 있는지를 알아보길 바란다.

구분	체크리스트	여부
원격협업도구	1. 회사 내 화상회의 보안 정책 마련	
	2. 화상회의 사용 시 대기방 기능 사용	
	3. 회의에 필요한 인원만 회의방 접근코드 공유	
	4. 인증된 단말기를 이용하여 화상회의 참여	
	5. 필요한 경우가 아닐 시 회의 내용 녹화 금지	
	6. 회의 시 민감한 정보가 화면에 노출되지 않도록 유의	
	7. 채팅, 파일 공유, URL 공유 등의 기능이 불필요할 시 비활성화	
	8. 메신저 이용 시 알 수 없는 사용자의 파일 공유 및 URL 클릭 금지	
	9. 업무 공유 솔루션 이용 시 프로젝트 공개 범위 설정 필요	
	10. 업무 공유 솔루션 이용 시 민감한 정보 게시 금지	

[표 3] 원격협업도구 셀프 체크리스트

구분	대상	체크리스트	여부
VPN	관리자	1. 사용자는 VPN 장비 버전 관리를 통해 패치 정책 수립	
		2. 최대 접속자 수를 고려해 용량, 라이선스 확장 필요	
		3. VPN 접속 시 비밀번호 이외 2차 인증 수단 적용	
		4. VPN 사용자에 대한 세션 만료 설정 필요	
		5. 기업 내 비대면 근무 체계 대응안 수립 후 배포	
		6. 다양한 OS 환경의 VPN 사용 매뉴얼 배포	
	사용자	1. PC 업데이트 및 백신 프로그램 업데이트	
		2. 사설 Wi-Fi, 공용 PC을 통한 업무 수행 자제	
		3. 업무 수행 시 불필요한 웹사이트 접근 자제	
		4. 업무에 불필요한 파일 다운로드 시 주의	

[표 4] VPN 셀프 체크리스트

3.2.2 보안 취약점 대응 솔루션

최근 다양한 서비스가 원격으로 전환되면서 비대면 서비스를 통한 해킹, 개인정보 유출 등의 보안사고 우려도 함께 증가함에 따라 보안 수준 강화가 필요해지고 있다. 본 논문에서는 보안 전문가보다는 비전문가인 개개인이 일상 속 실천할 수 있는 보안 취약점 대응 솔루션에 대해 다루려한다.

첫 번째로는 모바일 앱 점검이다. 특히 비대면 서비스 모바일 앱 대상으로 안전하지 않은 데이터 저장, 통신, 인증 등의 점검을 시행해야한다. 이때 모바일 백신과 같은 도구를 활용한다면 모바일 앱 뿐만이 아닌 디바이스까지 비전문가라도 편리하게 전문적인 점검이 가능하다.

두 번째는 유/무선 공유기 취약점 점검이다. IT 강국인 대한민국에서는 공유기가 없는 장소를 찾아보기 매우 힘들다. 여러 장소 중에서도 특히 공공장소인 카페, 지하철역, 버스 등에서 보안 설정이 미흡한 공유기를 통한 피해가 많이 발생하고 있다.

따라서 사용자는 되도록 공공장소 무선 인터넷을 사용하지 않거나, 인터넷 이용 시 단말기 DNS/IP주소를 수동으로 설정하며 최대한 보안을 유지해야 한다. 자택이나 회사와 같이 특정 이용자만이 사용하는 공유기에 비밀번호를 필수로 설정하는 등의 방법 또한 보안 취약점에 대응할 수 있는 방법들 중 하나이다.

마지막으로 스미싱 예방이다. 최근 비대면 서비스가 급증하면서 중요한 사무절차를 메신저로 진행함과 동시에 스미싱 피해 또한 급증하는 추세이다. 가장 좋은 예방방법은 의심스러운 문구 및 URL이 포함된 메시지는 클릭조차 하지 않는 것이다. 또는 통신사에서 제공하는 스미싱 예방 서비스를 가입하는 것도 하나의 좋은 대응 방법이다.

4. 결론

위의 내용들에서 살펴보았듯이, 언택트와 함께 살아가는 일상 속에는 기술을 이용한 해킹뿐 만 아니라 사회 공학적 해킹까지 다양한 방식과 종류의 방법으로 우리의 보안을 위협하는 공격들이 증가하고 있다. 따라서 우리의 개인정보와 보안 취약점은 상당히 위험에 처해있는 상황이다.

단기간에 많은 것들이 비대면화가 된 우리의 일상에 대해 너무나 빠른 변화라고 생각하여 시대를 따라가기 힘들다는 사람들도 많아지고 있다. 그러나 아무리 급변하는 세상이어도 우리의 개인정보에 대한 보안은 절대 소홀히 해서는 안 되는 부분이다. 또한, 앞으로 코로나19와 같이 우리의 일상을 완전히 뒤집어 놓을만한 일들이 생겨날 가능성이 충분하다.

앞으로 더 많은 사람들은 더 많은 개인정보를 더 많은 장소에 저장할 수밖에 없는 시대를 살아가게 될 것이다. 이에 따라 갈수록 더 다양한 보안 취약점이 생겨나며 보안 위협이 증가할 것이다.

이에 대해 예방하고 피해를 입지 않으려면 현재 본인의 정보가 어느 곳에 보관되어있는지, 보안이 취약하진 않은지, 혹여나 나도 모르는 사이에 보안 취약점이 드러나 있지 않는지 등을 제대로 파악하고 그에 따른 보안 취약점에 대한 대비를 단단하게 해두는 것이 현대 사회를 영리하게 살아가는 방법이다.

참고문헌

[1] “일은 집에서, 점심은 배달, 코로나가 바꾼 경제활동”, 머니투데이 2020.03.23.
[2] “코로나19가 앞당긴 일상의 확산”, KOTRA 해외시장뉴스 2020.04.21
[3] 비대면 근무체계로 인한 보안이슈 및 대응방안 - IGLOO 2020.05.29.
[4] SK인포섹, 보안서비스 '비대면 원격'으로 확대 2020.06.23.
http://news.heraldcorp.com/view.php?ud=20200623000079
[5] 비대면 업무환경 도입·운영 보안 가이드 배포 2020.06.25.
http://www.epnc.co.kr/news/articleView.html?idxno=98715
[6] KISA, 비대면 서비스 보안 점검 지원 2021.04.01.
https://www.koit.co.kr/news/articleView.html?idxno=81534
[7] 고용노동부, 코로나19 관련 “재택근무 가이드라인” 마련, 배포 2020.04.02.
https://www.moel.go.kr/news/enews/report/enewsView.do?news_seq=10851
[8] 직장인 78.3% “코로나로 재택근무했다” 2021.06.01.
https://www.koit.co.kr/news/articleView.html?idxno=85106
[9] 시프티, 2020~2021년 재택근무 관련 기업 빅데이터 분석 결과 발표 2022.02.10.
https://shiftee.io/ko/blog/article/shifteeWorkFromHomeBigData
[10] [데이터로 본 한국인] 금융에 있어서도 커지는 언택트 영향력 2020.04.10.
https://www.hankookilbo.com/News/Read/202004091456042133
[11] 코로나19, 언택트 사회를 가속화하다 [경기연구원 이슈&진단] 2020.05.28.
https://m.blog.naver.com/gri_blog/221980273335
[12] 계속해서 대학의 골칫거리가 되고 있는 줌바밍(Zoomboming) 2021.05.16.
https://www.unipress.co.kr/news/articleView.html?idxno=3636
[13] 줌의 보안 취약점 분석과 보안 업데이트 결과 비교, 김규형, 최윤성 2020.12.
https://koreascience.kr/article/JAKO202007552826477.pdf
[14] 비대면 근무체계로 인한 보안이슈 및 대응방안 2020.05.29.
https://www.igloo.co.kr/security-information/%EB%B9%84%EB%8C%80%EB%A9%B4-%EA%B7%BC%EB%AC%B4%EC%B2%B4%EA%B3%84%EB%A1%9C-%EC%9D%B8%ED%95%9C-%EB%B3%B4%EC%95%88%EC%9D%B4%EC%8A%88-%EB%B0%8F-%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88/
[15] 스미싱이란, 대표적인 사례 및 예방.신고 방법 2021.09.14.
https://daystudy.tistory.com/1732
[16] 님아, 그 파일을 열지 마오...카카오 혼란 틈새 노린 '스미싱', 2022.10.18.
https://m.ytn.co.kr/news_view.php?s_mcd=0103&key=202210181558506243&pos=#return
[17]스미싱 | 사이버위협 - KISA 인터넷 보호나라&KrCERT
https://www.boho.or.kr/cyber/smishing.do