사이버 보안과 인터넷 안전

front porch

피어스 프로젝트
도구 및 자료 안내 (2019년 판)

Front Porch Center for Innovation and Wellbeing의 계획

추가 후원 단체

California Lutheran Homes

나이 들며 변화하는 개개인의 필요를 충족시키는 혁신적인 커뮤니티와 프로그램에 중점을 둔 비영리 봉사 단체인 Front Porch 는 은퇴자 커뮤니티 거주자였던 Ellie Piers 의 가족으로부터 넉넉한 기부금을 받았습니다.

Ellie Piers

Front Porch Center for Innovation and Wellbeing's (FPCIW's)가 수행하고 있는 기술을 이용한 노인들의 안녕 증진이라는 임무는 이 기부금의 혜택을 받고 있습니다. Piers는 Front Porch의 은퇴자 커뮤니티인 캘리포니아 주 칼스배드 소재 Carlsbad By The Sea에 살았습니다. Piers의 공헌 덕분에 CIW는 정보 기술을 이용한 노인 안전 문제에 집중하여 샌디에고 및 인근지역 노인들의 온라인 안전 계획을 개발했는데, 이는 인터넷을 통해 먼 곳에 있는 광범위한 커뮤니티들에서도 이용될 수 있습니다.

Piers는 기술에 관한 호기심과 모험심이 강한 사람으로 기술의 도움을 받아 노인들이 건강하고 안전하게 살 수 있다고 믿었습니다. Piers는 가족 및 친구들과 연락을 유지하는데 기술의 힘을 이용할 기회를 받아들이는 한편, 기술의 사용에 수반되는 안전 문제에 대해서도 익히 알고 유념했습니다. 기술 사용시 발생되는 취약점에 대해 예리하게 인식하고 있던 Piers는 각 "웹 서핑"의 목표로 본인을 안내하는데 도움이 되는 웹사이트에 접속하기 전에 철저히 질문하는 버릇이 있었습니다. 다른 사람들을 도우려는 Piers의 정신을 기리기 위해 FPCIW는 노인 안전 문제를 알리고 계몽하는 다음과 같은 내용의 **Piers Project (피어스 프로젝트)**를 개발했습니다:

- 노인 안전과 관련한 새로운 기술의 시험 및 노인들의 온라인 보안과 관련된 콘텐트 개발;
- 노인들의 온라인 안전 문제에 대한 영향력 확대를 목표로 한 기부금 활용을 위한 협력 기구 설립을 위해 샌디에고 및 인근 지역에 전문성이 있는 단체들과 접촉;
- 샌디에고 및 인근 지역 노인들의 삶을 개선시킬 수 있는 기술에 대한 인식을 높여 줄 매체들에 대한 탐구;
- 노인 복지라는 중요한 분야에 변화를 주려는 Piers의 기부와 관심에 경의를 표시하는 온라인 및 소셜 미디어 캠페인 벌이기

FPCIW가 제작한 이 도구는 보다 많은 언어로 더 많은 지역사회에 본 자료를 제공하기 위해 California Lutheran Homes Foundation에서 추가로 후원하였습니다. 이 도구는 개개인이 온라인 세계에 존재하는 일부 위험들에 대해 더 잘 이해하고, 인터넷의 혜택을 누리면서 그러한 위험은 사전에 자신 있게 피하도록 안내하는 길잡이입니다 .

사이버 보안 도구

목차

알고 계셨습니까....

- 2016년에 65세 이상 **미국인 중 67%** 가 인터넷을 사용하고 있었습니다[1].
- **노인이 당한 학대는 24건 중 1건만** 신고됩니다[2].
- 2017년에 노인들은 **금전 사기로 17억 달러를** 잃었습니다[3].
- **금전 사기의 45%는** 인터넷 사용에서 시작됩니다[4].
- 미디어에서 보는 것의 진실 여부에 대해 확신이 없다는 **사람이 59%**입니다[5].

오늘날 기술은 우리 일상 생활의 필수적인 도구가 되었습니다. 인터넷을 통해 사랑하는 사람과 대화하고, 온라인으로 은행 업무와 쇼핑을 하며, Facebook과 Twitter 같은 플랫폼에서 사람을 사귀고, 좋아하는 분야에 대한 탐구도 합니다. 인터넷에서 얻는 혜택은 아주 많지만 어떻게 하면 안전하게 광범위한 디지털 세계를 이용할 수 있을까요?

디지털 사회의 활동적 구성원인 우리에게는 인터넷 위생을 잘 실천하는 것이 중요합니다. 개인적, 사회적, 아울러 금전적 손상까지 끼치게 할 수 있는 우리의 개인 정보를 캐내려는 사람들이 사용하는 흉측한 계략들에 대해서도 알아야 할 필요가 있습니다. 여느 유익한 기술과 마찬가지로 위험을 줄여서 편하고 안전하고 평화롭게 인터넷의 혜택을 누리도록 위험을 줄이는데 도움이 되는 예방 조처를 취하는 것이 중요합니다: 우리의 힘과 통제는 지식과 경험의 공유에서 나오는 것입니다.

이 도구는 노인들의 안전한 컴퓨터 사용을 위한 자료들을 안내하기 위해 만들어진 것입니다. 이 도구에 담긴 가르침은 모두 안전하고 성공적인 온라인 경험을 위한 3개의 단순하지만 중요한 규칙에 기반을 두고 있습니다.

1) 인터넷에서 보는 콘텐츠에 **의문을 가지십시오.**

2) 유효성과 신빙성을 **확인하십시오.**

3) 친구, 이웃, 동료에게 도움을 **요청하고,** 당신 주위 사람들에게도 가르쳐 주십시오.

사이버 보안과 사기의 대상인 노인들

사이버 보안이란 일반적인 인터넷 안전을 말하는 것으로, 컴퓨터에 저장되어 있거나 인터넷을 통해 얻을 수 있는 정보의 보호에 중점을 두고 있습니다. 컴퓨터와 인터넷을 포함한 다양한 방식의 기술을 이용한 사기는 계속 발전하고 있습니다.

인터넷 사용자는 모두 사이버 범죄자들의 목표물이 될 수 있는데 어째서 노인들이 가장 흔하게 당하는 것일까요? 노인들은 금전적으로 더 안정적일 확률이 높고, 사기를 당하고도 신고를 잘 하지 않거나 사건을 어디에 어떻게 신고해야 하는지조차 모를 수 있습니다. 노인들은 기억력, 수명, 신체 건강의 향상을 거짓으로 약속하는 제품들에 큰 돈을 투자하기도 합니다.

노인들은 수치심이나 두려움 때문에 범죄 피해를 덜 신고하는 경향이 있어 금전 사기는 지속되고, 추가 피해자를 계속 발생시킵니다[9]. 과거 당신이 사이버 범죄의 피해자였다면 **혼자만 당한 것이 아니며** 많은 사람들이 똑같은 어려움에 처했었다는 사실을 아는 것이 도움이 될 것입니다.

소비자용으로 출시돼 있는 기술들을 사용하는데 익숙하지 못할 수도 있는 사람들이라면 사이버 사기를 적극적으로 피하는 기법들을 배우는 것이 중요합니다. 피어스 프로젝트의 도구는 노인들이 온라인에서 홀대 당하는 것을 방지하고, 노인들이 온라인에서 안전하게 처신하면서 정보 기술의 훌륭한 혜택을 누리도록 돕는 것입니다.

누구를 믿나? 사기꾼들을 식별하라!

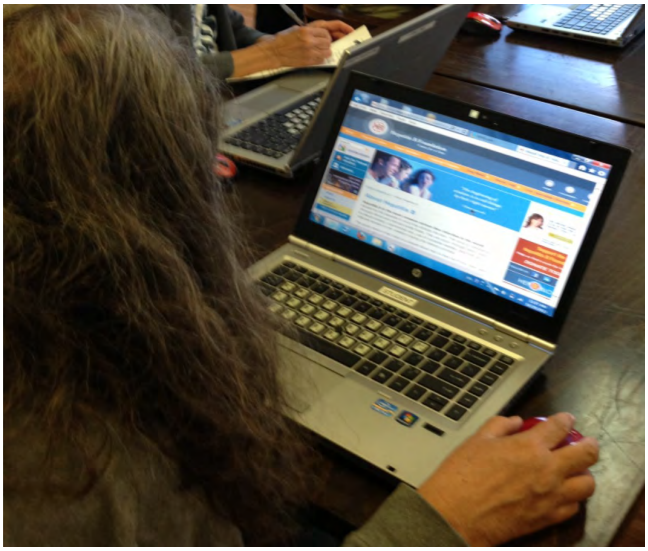
인터넷의 많은 장점 중 하나가 건강, 세금, 금전 관리 등 우리 삶을 다방면으로 관리하게 해주는 편리함 입니다. 필요한 정보를 쉽게 찾을 수 있고 도움이 필요할 때 적절한 사람과 신속히 연결될 수 있습니다. 인터넷을 사용할 때는 사기꾼과 속임수들을 식별하고 걸러낼 수 있는 것이 중요합니다.

허락이나 동의 없이 어떤 사람이 당신의 개인 신원 정보를 취득하거나 사용하는 것이 신분 도용입니다. 그 정보가 물건을 주문/구매하고, 소셜 시큐리티 혜택을 받고, 당신의 개인 재산을 빼돌리거나, 다른 범죄를 저지르는데 사용될 수 있습니다. 신분 도용을 당하면 해로운 결과가 초래될 수 있습니다. 불법 복제 여권, 신용 손상, 메디케어/ 메디케이드 사기 같은 것이 포함되기도 합니다. 다음은 알고 있어야 할 흔한 사기 행위들과 거기 걸려들지 않고 안전하게 지내기 위해 할 수 있는 예방 조치입니다:

의료 사기. 이런 유형의 사기에는 다양한 형태가 있습니다. 허위 텔리비전 광고, 새로 제정된 법이 요구할 수 있는 건강 보험 카드 추가 발급 조항의 악용, 건강 보험료 대폭 할인을 약속하는 전화 같은 것도 포함됩니다.

1) 인터넷에서 보는 콘텐츠에 **의문을 가지십시오.**
2) 유효성과 신빙성을 **확인하십시오.**
3) 친구, 이웃, 동료들에게 도움을 **요청하고,** 주위 사람들에게도 가르쳐 주십시오.

다른 사람으로 가장하고 벌이는 사기들도 있습니다. 공무원을 사칭하며 새로 나온 수혜자 카드를 보내주려면 메디케어 번호가 필요하다고 말하기도 합니다.



이렇게 해 보십시오!

- ✓ **최근 시사를 파악하고 계십시오.** 사기꾼들은 메디케어와 기타 건강 관련 프로그램들이 바뀌면서 미디어에서 널리 논의되고 있는 기간에 공격을 계획하는 경우가 많습니다[6]. 메디케어 자유 등록 기간에는 마음을 단단히 먹고 조심하십시오. Social Security Number Removal Initiative (SSNRI) (소셜 시큐리티 번호 제거 발의안)의 일환으로 2018년 4월부터 Centers for Medicare and Medicaid Services 는 소셜 시큐리티 번호가 들어 있는 구형 메디케어 카드를 대체하는 새 카드를 발행하여 우송하고 있습니다.
- ✓ **진술의 사실 여부를 조사하십시오.** 당신의 개인 정보를 공유하기 전에 안전을 기하기 위해 메디케어(1-800-MEDICARE)에 문의하십시오. 메디케어는 개인에게 전화하는 일이 절대 없다는 것을 알고 계시고, 만약 그런 전화를 받는다면 당신의 개인 정보는 아무 것도 주지 마십시오.

세금 관련 사기. 최근 W-2 피싱 사기가 사이버 보안의 관심사가 되었습니다. 사기꾼들이 회사의 대표나 임원이 직원의 W-2 납세 정보를 묻는 것처럼 보이는 가짜 이메일을 보내는 방법들을 찾아내고 있는 것입니다. 사이버 범죄자들은 이렇게 얻어 낸 W-2 정보를 가지고 허위 세금 보고를 하거나 신분을 도용합니다[7].

이렇게 해 보십시오!

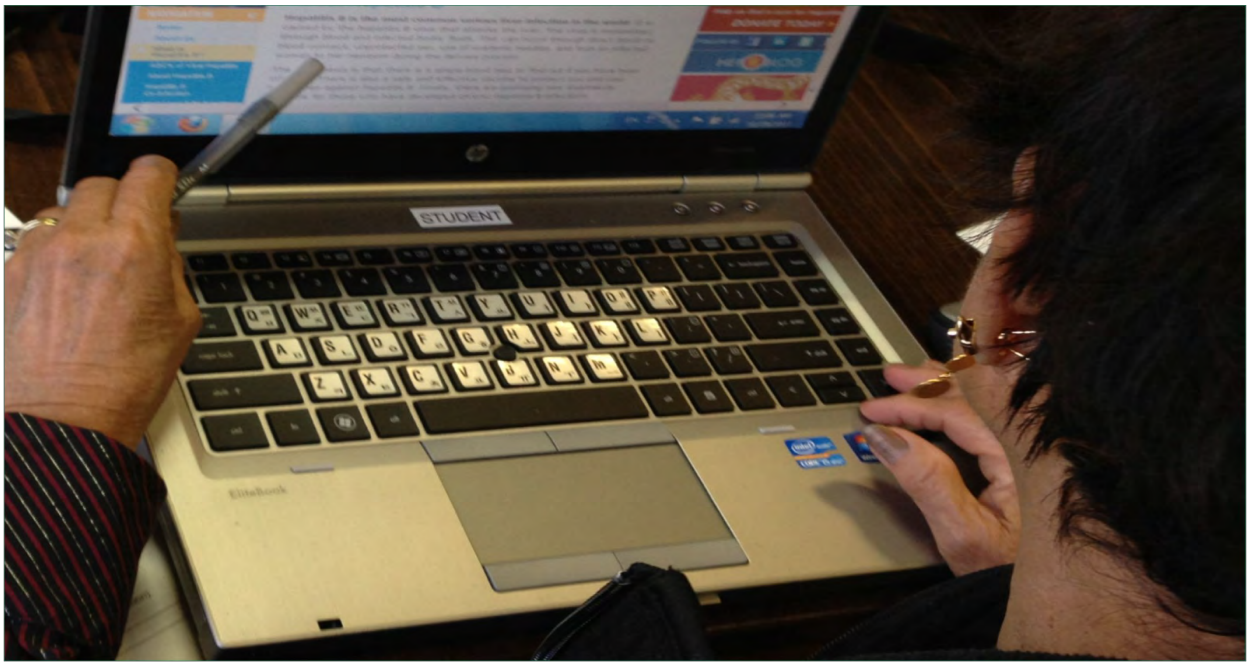
- ✓ **전화를 거십시오.** W-2 납세 정보를 요구하는 이메일을 받으면 어떤 정보도 보내기 전에 본인의 직장에 전화해 진위 여부를 확인하십시오.
- ✓ **세금 보고를 일찍 하십시오.** 세금 보고를 일찌감치 해버리면 사이버 범죄자들이 허위 보고를 할 수 없게 됩니다.
- ✓ **정기적으로 당신의 신용 점수를 확인하십시오.** AnnualCreditReport.com에서 1년에 한번씩 무료로 당신의 신용 점수를 확인하고 의심스러운 거래 내역이 있는 계좌는 동결시키십시오.

복권 사기. 이러한 유형의 불법 행위 중에는 당신이 복권에 당첨되었다는 허위 주장을 하면서 첫번째 처리 수수료 지불을 요구하는 것도 있습니다. 이메일을 통한 복권 사기는 합법적인 복권 관리 기관이나 기타 합법적인 기업의 이름을 사용합니다. 서두르지 마시고 조사해 보십시오. 믿어지지 않을 정도로 좋다면 아마도 사기일 것입니다.

투자 사기. 이런 사기는 신규 및/또는 기존 자금에 대한 투자와 관련됩니다. 광산, 석유, 개스나 신 기술 회사 등에 투자하라는 요청을 받을 것입니다. "Prime Bank" (프라임 뱅크) 사기가 전형적인 시나리오입니다. 사기꾼들은 투자자들로부터 모은 자금을 가지고 U.S. Federal Reserve 같은 공공 기관이 발행했거나 보장하는 "Prime Bank" 증서를 구입하고 거래할 것이라고 주장 합니다. 또 자주 이런 방식의 투자 기회는 오로지 초대로만 얻을 수 있으며 엄선된 일부 고객에게만 제한된 것이라고 덧붙입니다[8]. 게다가 해외 투자는 국내 규정과 감독으로 인해 추가 실사가 요구되므로 심각하게 검토되어야 합니다.

이렇게 해 보십시오!

- ✓ **외형으로 회사를 판단하지 마십시오.** 어떤 웹사이트는 매력적이고 합법적으로 보이지만 그렇다고 항상 믿을만한 회사인 것은 아닙니다.
- ✓ **계약 약관에 관하여 문의하십시오.** 일반인들은 중요한 세부사항을 무시하는 경향이 있으니, 계약서를 주의 깊게 검토하십시오.
- ✓ **거액의 약속을 믿지 마십시오.** 이것은 이메일 받는 사람에게 던지는 흔한 미끼입니다.



이메일

이메일은 인터넷의 대표적 통신 수단이지만 어떤 것은 열어도 안전하고, 어떤 것은 삭제해야 할 것인지를 어떻게 알 수 있을까요? 주의해서 살펴봐야 할 단서들은 무엇일까요? 다음은 알아둘 용어 및 이메일 수신함에서 잠재적 위협을 식별할 수 있는 방법들입니다.

피싱 (Phishing). 사기꾼이 가짜 이메일이나 문자를 이용해서 당신의 소중한 개인 정보를 빼내는 것을 "피싱"이라고 합니다. "낚시"와 비슷하게 사기꾼들은 합법적이고 안전한 웹사이트처럼 가장한 링크나 가짜 웹사이트를 피해자들에게 미끼로 던집니다. 그렇게 해서 비밀번호, 소셜 시큐리티 번호, 은행 계좌 정보 같은 것들을 수집합니다.

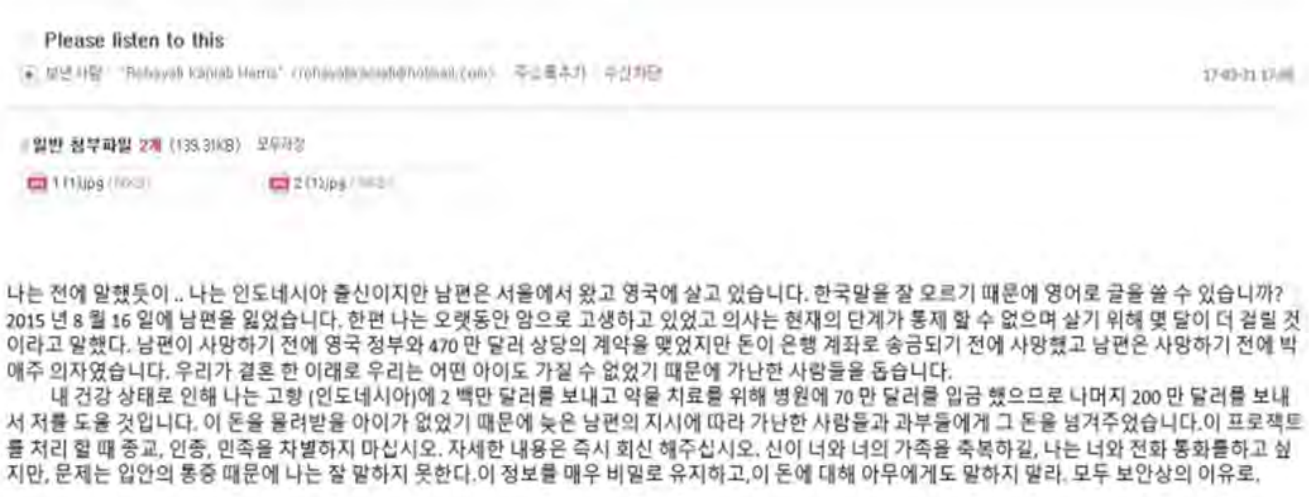
스팸 (Spam). 다양한 온라인 사기에 이용될 수 있는 원하지 않는 다량의 이메일을 말합니다. 대부분의 스팸은 해롭지 않고 그저 귀찮은 광고들이지만, 어떤 것은 허가 없이 컴퓨터와 서버에 들어와서 바이러스를 퍼뜨릴 수 있습니다. 이 방법으로도 당신의 개인 정보를 불법 취득하여 판매할 수 있습니다.

해킹 (Hacking). 컴퓨터나 개인 계좌에 허가없이 원격으로 접속하는 자를 해커라고 합니다. 컴퓨터 시스템이나 컴퓨터 네트웍의 취약점을 부당하게 이용하는 해킹은 어떤 형태라도 불법이며 범죄 행위로 여겨집니다.

나이지리아 편지 사기/ 419 사기(Nigerian Letter Fraud / 419 Fraud). 수수료 선불 사기로도 알려진 이 사기는 발신자가 외국 정부 관료이거나 금전적 도움이 필요한 외국인임을 자처하면서 이메일로 당신의 개인 정보나 은행 관련 정보를 요구합니다. 발신자는 수신자에게 (편지 안에 제공된) 팩스 번호를 통해서도 볼 수 있는 은행 이름(들)과 계좌 번호(들) 및 기타 비밀 정보를 적은 빈 레터헤드(윗 부분에 개인, 회사, 단체의 이름과 주소 등이 적혀있는 편지 용지) 같은 것을 보내달라고 요청합니다[9]. 외국 정부가 보낸 이메일은 의심하십시오. 그것들은 대개 외국에 소재한 은행에 거액을 입금해서 도와달라고 요청합니다. 이런 사기꾼들은 긴급하다고 호소하며 즉각적인 금전 원조를 요구합니다. 아울러 Social Security Administration Office 직원이라며 당신의 소셜 시큐리티 번호를 묻는 것과 같은 미국 정부의 이메일도 의심하십시오. 한번 더 생각하십시오! 이런 종류의 기관들은 당신의 개인 정보를 인터넷을 통해 묻지 않는 것이 정상입니다.

자세히 살피기

피싱 사기는 나이지리아에서만 오는 것이 아닙니다: 거액을 송금해 도와달라는 이메일은 무엇이든 의심하십시오. 납득이 가지 않는 긴급 상황에 처한 친구나 가족들이 보낸 것 같아 보이는 요청도 마찬가지로 의심하십시오.


Please listen to this

일반 첨부파일 2개 (139.31KB) 모두저장

1 (1).jpg 2 (1).jpg

나는 전에 말했듯이 .. 나는 인도네시아 출신이지만 남편은 서울에서 왔고 영국에 살고 있습니다. 한국말을 잘 모르기 때문에 영어로 글을 쓸 수 있습니까? 2015 년 8 월 16 일에 남편을 잃었습니다. 한편 나는 오랫동안 암으로 고생하고 있었고 의사는 현재의 단계가 통제 할 수 없으며 살기 위해 몇 달이 더 걸릴 것이라고 말했다. 남편이 사망하기 전에 영국 정부와 470 만 달러 상당의 계약을 맺었지만 돈이 은행 계좌로 송금되기 전에 사망했고 남편은 사망하기 전에 박애주 의자였습니다. 우리가 결혼 한 이래로 우리는 어떤 아이도 가질 수 없었기 때문에 가난한 사람들을 돕습니다.

내 건강 상태로 인해 나는 고향 (인도네시아)에 2 백만 달러를 보내고 약물 치료를 위해 병원에 70 만 달러를 입금 했으므로 나머지 200 만 달러를 보내서 저를 도울 것입니다. 이 돈을 물려받을 아이가 없었기 때문에 늦은 남편의 지시에 따라 가난한 사람들과 과부들에게 그 돈을 넘겨주었습니다.이 프로젝트를 처리 할 때 종교, 인종, 민족을 차별하지 마십시오. 자세한 내용은 즉시 회신 해주십시오. 신이 너와 너의 가족을 축복하길, 나는 너와 전화 통화를하고 싶지만, 문제는 입안의 통증 때문에 나는 잘 말하지 못한다.이 정보를 매우 비밀로 유지하고,이 돈에 대해 아무에게도 말하지 말라. 모두 보안상의 이유로.

이렇게 해 보십시오!

✓ **이메일의 철자법과 문법에 유의하십시오.** URL(웹페이지 주소), 이메일 주소, 이메일 내용의 철자를 확인하십시오. 피싱 이메일에서는 보통 미묘한 철자법 오류들을 찾아볼 수 있습니다. 발신자 이름이 보이면 그 메시지를 보낸 이메일 주소가 있는지 다시 한번 보십시오. 또한 마우스를 링크 위로 가져 가면 그 링크가 데려 가겠다고 약속한 것과는 다른 의심스러운 웹사이트로 데려가는 것을 발견하게 될 수도 있습니다.

✓ **모르는 곳에서 온 이메일은 열지 마십시오.** 낯선 사람에게서 온 이메일, 문자나 소셜 미디어 메시지는 삭제하거나 무시하십시오. 당신에게 돈, 선물을 찾아 가라거나 휴가를 제안하는 이메일도 똑같이 조심스럽게 대하십시오: 이런 이메일은 당신을 악성소프트웨어나 바이러스에 감염될 수 있는 다른 웹사이트로 데려갈 가능성이 큽니다. 의심스러우면 바로 삭제하십시오!

✓ **이메일이나 문자에 포함된 링크는 의심하십시오.** 아는 사람에게서 이메일을 받았는데 내용이 달랑 링크 하나 뿐이면 그 링크는 클릭하지 마십시오. 이는 당신에게 이메일을 보낸 사람이 해킹을 당했다는 흔한 징후입니다. 그럴 때는 전화나 다른 방법으로 그 사람과 연락하고 그 이메일은 삭제하십시오.

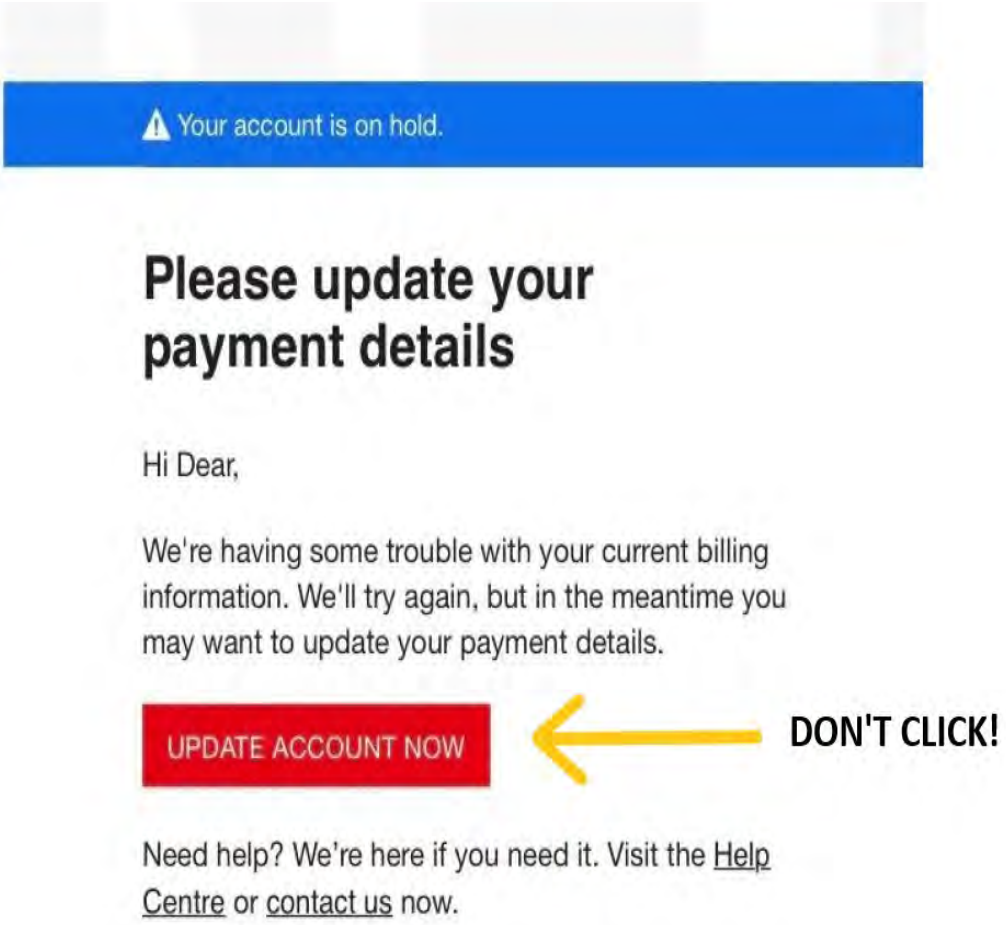
✓ **은행 계좌나 개인 정보는 절대 이메일로 보내지 마십시오.** 은행이나 보험회사 같은 합법적인 회사들은 절대 이메일로 개인 정보를 보내라는 요청을 하지 않는다는 것을 알고 계십시오. 안전한 웹사이트에서 자기 계좌에 로그인해 메시지나 공지사항을 확인하십시오.

1) 인터넷에서 보는 콘텐츠에 대해 **의문을 갖고,**
2) 유효성과 신빙성을 **확인하고,**
3) 친구, 이웃, 동료들에게 도움을 **요청하고,** 주위 사람들에게도 가르쳐 주십시오.

자세히 살피기

사기꾼들은 이메일을 보낼 때 받는 사람들이 안심하고 거기 끼워 넣어진 링크를 클릭하게 만들기 위해서 **익숙한 회사 이름들을 자주 사용합니다.** 아래에 있는 이메일을 보십시오. 2018년 12월에 오하이오 경찰에 신고된 실제 "피싱" 이메일 사례로 마치 Netflix에서 발송된 것 *같아 보입니다.*

어떤 회사에서 온 이메일에 들어 있는 링크가 안전한지 확신이 없을 경우에는 브라우저 창을 새로 열고 직접 그 회사의 웹사이트로 가서 당신 계좌에 로그인하는 것이 가장 안전한 방법입니다. 만일 당신 계좌와 관련된 중요한 공지사항이나 메시지가 있다면 안전한 웹사이트의 당신 계좌 안에도 있을 것입니다.



넷플릭스를 사칭한 사기: 현재 본인의 결제 시스템에 문제가 있어 계정이 보류되었으니 이메일상의 링크를 통해 결제 정보를 업데이트 하라는 내용. 빨간색의 계정 업데이트 버튼을 누르면 개인 정보와 크레딧 카드 정보가 유출되어 도용될 수 있다. 의심스러운 경우에는 넷플릭스 웹사이트를 통해서만 로그인 할 것.

재정 보호

인터넷을 이용하여 재정 관리를 하면 많은 이점이 있습니다: 온라인으로 편리하게 물건을 구입하고, 각종 청구서의 일정 관리와 지불도 하며, 즉각적인 자금 이체도 가능합니다.

온라인 금융사기는 여러 형태가 있는데 가장 흔한 사기 유형은 크레딧 카드나 은행 계좌 정보를 이용한 사기로 구매, 투자, 세금과 관련된 복잡한 문제에 악용되는 일이 빈번합니다. 이런 사기를 치는 사람들은 가짜 웹사이트나 이메일 메시지를 통해 정보를 얻어 냅니다.

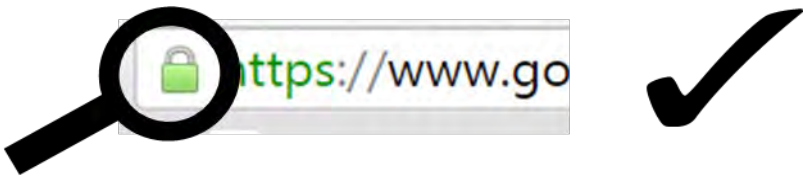
온라인 쇼핑. 데빗/ 크레딧 카드를 이용한 사기 행위들이 포함됩니다. 실제로 카드를 훔치거나 카드 번호, 카드 보안 번호, 카드 소지자의 이름과 주소 같은 카드 소지자 계좌와 개인 정보를 불법 취득해서 저지릅니다.

이렇게 해 보십시오!

- ✓ **가능하면 대체 서비스를 이용해 지불하십시오.** 어떤 사이트에 직접 지불하는 대신 보안 단계가 추가되는 PayPal, Amazon, and Google Check Out 같은 대체 지불 서비스를 이용하십시오[10]. 또 가능하면 "손님" 자격으로 지불하고 계좌에 카드를 저장하지 않기를 선택하십시오.
- ✓ **명세서를 잘 살피십시오.** 사용 중인 크레딧 카드 목록을 정리해두고 은행의 지불 내역서를 정기적으로 확인하십시오. 잘못되었거나 낯설어 보이는 것이 눈에 띄면 카드 발급 기관과 즉각 접촉하십시오.
- ✓ **가능하면 크레딧 카드를 사용하십시오.** 데빗 카드보다는 크레딧 카드를 사용하는 것이 일반적으로 더 안전합니다. 왜냐하면 주문한 제품이 배달되지 않거나 주문한 것과 다를 경우 구매자가 카드 발행자에게 크레딧을 요청할 수 있기 때문입니다[11].
- ✓ **가장 강력한 인증 도구를 사용하십시오.** 생체 인식, 보안 키, 또는 스마트폰 같은 모바일 장치의 앱을 통해 받는 독특한 일회용 암호 같은 가장 강력한 인증 도구를 이용하면 온라인 쇼핑 계좌를 보호할 수 있습니다[11].

자세히 살피기

자물쇠 아이콘을 확인하십시오. 웹사이트에 접속했는데 주소 창에 작은 자물쇠 아이콘이 나타나면 그 웹사이트는 데이터를 전송할 때 *보다 높은* 보안 수준을 채택하고 있음을 뜻합니다. 이 아이콘은 일부 보호기능을 보여주는 것이긴 하지만 반드시 완벽한 보안을 보장하지는 않습니다!



링크의 주소를 확인하십시오. 외형적으로는 합법적으로 보이는 링크라도 진짜가 아닐 수 있으므로 링크는 매우 주의 깊게 읽어 보십시오. 예를 들어 "bankofamericacard.com" 이나 "B-of-America" 같은 링크는 합법적인 것으로 보이는데 도움 되는 "bank" 나 "America" 라는 단어가 주소에 들어 있지만 진짜 그 회사의 웹사이트로 연결되는 링크가 아닙니다.

Federal Trade Commission (연방 통상 위원회) 웹사이트 **www.ftc.gov** 에서 온라인 소비자를 위한 조언과 귀띔을 더 살펴보십시오!

온라인 뱅킹. 보안이 확실한 은행 웹사이트나 앱에 안전하게 접속했다면 온라인으로 은행 업무를 처리해도 안전합니다. 온라인 쇼핑을 할 때와 같은 보안 신호들(초록색 자물쇠, “https”, 웹사이트 주소의 철자법이 정확한지)을 찾아 보십시오. 다음은 안전한 온라인 뱅킹을 위한 몇가지 요령입니다.

이렇게 해 보십시오!

- ✓ **온라인 뱅킹을 할 때는 개인 와이파이를 사용하십시오.** 중요한 정보가 관련된 일을 할 때는 무료나 공용 와이파이를 사용하지 마십시오.
- ✓ **입출금 내역서를 정기적으로 확인하십시오.** 구매 내역이 모두 익숙해 보이는지 확인하십시오. 계좌 활동내역에서 의심스러운 점이 보이면 즉시 은행에 문의하십시오.
- ✓ **은행 사이트나 앱을 종료하기 전에 반드시 로그아웃 하십시오.** 로그아웃 한 다음에는 브라우저마저 완전히 닫으시면 더 좋습니다.
- ✓ **은행의 보험 규정에 관해 문의하십시오.** 사이버 범죄자들이 당신의 은행 정보를 입수할 경우에 대비하여 사기 사건이 발생했을 경우 변제에 관한 당신 은행의 보험 규정 및 절차를 미리 알아두는 것이 좋습니다. 청구액을 보고해야 하는 기간은 얼마이며 은행은 얼마까지 변제해 주나요?

1) 인터넷에서 보는 콘텐츠에 대해 **의문을 갖고,**
2) 유효성과 신빙성을 **확인하고,**
3) 친구, 이웃, 동료들에게 도움을 **요청하고,** 주위 사람들에게도 가르쳐 주십시오.

악성소프트웨어(Malware)

클릭해도 안전한 것과 아닌 것을 어떻게 아십니까? 믿을만한 곳에서 순전히 당신에게 보내려는 메시지만 받을 수 있기 원한다면 몇가지 중요한 점들을 알아둬야 합니다.

클릭베이트(Clickbait) 란 방문자의 관심을 끌어서 특정 웹 페이지로 가는 링크를 누르게 하려는 목적을 가진 인터넷 콘텐츠를 말합니다. 어떤 제목이나 광고는 정말로 당신을 흥미로운 기사나 물건을 사고 싶은 온라인 상점으로 데려다 주겠지만 클릭베이트 제목을 많이 사용하는 사이트에는 악성소프트웨어가 들어있을 가능성이 높습니다.

악성소프트웨어(Malware). 맬웨어(Malware)란 컴퓨터 시스템에 해를 끼치거나 못쓰게 하려고 만든 프로그램인 "malicious software"를 줄인 말입니다. 스마트폰 같은 모바일 기기들도 맬웨어와 바이러스 공격으로부터 자유롭지 않으니 조심해서 사용해야 합니다. wikipedia.org에 따르면 "맬웨어는 정보를 빼내려는 목적으로 잠복하거나 컴퓨터 사용자가 모르도록 장기간 감시하기도 한다."고 합니다. 악성소프트웨어에는 몇가지 종류가 있습니다:

랜섬웨어(Ransomware). 몸값을 뜻하는 '*랜섬 (ransom)*'과 '*소프트웨어(software)*'를 합성한 용어인 랜섬웨어는 원격으로 컴퓨터를 정지시키고 저장된 정보를 빼내거나, 도둑맞은 자금을 되돌려 받으려면 금전적 보상을 하라는 요구하기까지 합니다. 이런 악성소프트웨어를 퍼뜨리는 자들은 자신을 경찰처럼 권위있는 인물로 가장할 수도 있습니다. 이처럼 해로운 악성소프트웨어 공격은 스마트폰과 태블릿을 대상으로도 이루어질 수 있습니다.

바이러스(Viruses). 컴퓨터 속의 바이러스는 사람들 사이의 바이러스와 비슷합니다. 기술적으로 말하자면 바이러스는 컴퓨터를 생존을 위한 숙주로 사용합니다. 그렇게 하면서 바이러스는 당신의 컴퓨터 안에서 계속 증식하고 변형해 가면서 임무를 수행하는데 이 공격 중에 다른 컴퓨터에 악성소프트웨어를 퍼뜨리기도 합니다.

백신 프로그램(Vaccine programs). "바이러스 퇴치 소프트웨어"로도 알려진 백신은 악성소프트웨어의 공격을 예방하거나 반격하는 도구의 기능을 합니다. 악성소프트웨어 공격의 예방을 돕기 위해 당신의 컴퓨터에 바이러스 퇴치 프로그램(혹은 Windows FireWall)이 최소한 하나는 작동하고 있는지 확인하십시오. 특히 최근 컴퓨터의 처리 속도가 눈에 띄게 감소했다면 이런 프로그램이 필요할 수 있습니다.

백신 프로그램은 가격과 기능 면에서 다양한 제품이 있습니다. 대표적인 브랜드에는 이런 것들이 있습니다:

- Avast
- AVG
- Bitdefender Antivirus
- Kaspersky Anti-Virus
- McAfee AntiVirus
- Norton Security

악성소프트웨어 퇴치 프로그램 (Anti-Malware Program). Windows FireWall은 악성소프트웨어에 대하여 가장 기본적인 형태의 보호기능을 하며 Microsoft Windows 프로그램에 장착되어 있기도 합니다. 그러나 Apple Mac 사용자는 애플 메뉴에서 소프트웨어를 업데이트할 수 있는지 확인하는 것이 중요합니다. 또 Apple 컴퓨터 사용자는 정기적으로 예약된 업데이트가 "System Preferences" 옵션에서 실행되도록 해야합니다. uBlock Origin 같은 브라우저 확장 기능은 컴퓨터 사용자의 활동을 추적하고 악성소프트웨어를 설치하는 광고들을 차단할 수 있습니다.

자세히 살피기

컴퓨터에서 주시해야 할 위험 신호들은 아래와 같은 것들입니다:

- 컴퓨터가 멈추거나 속도가 느려짐
- 이상한 소리나 경고음
- 계속 튀어 나오는 팝업창
- 원하지 않는 사진들
- 사라지는 데이터

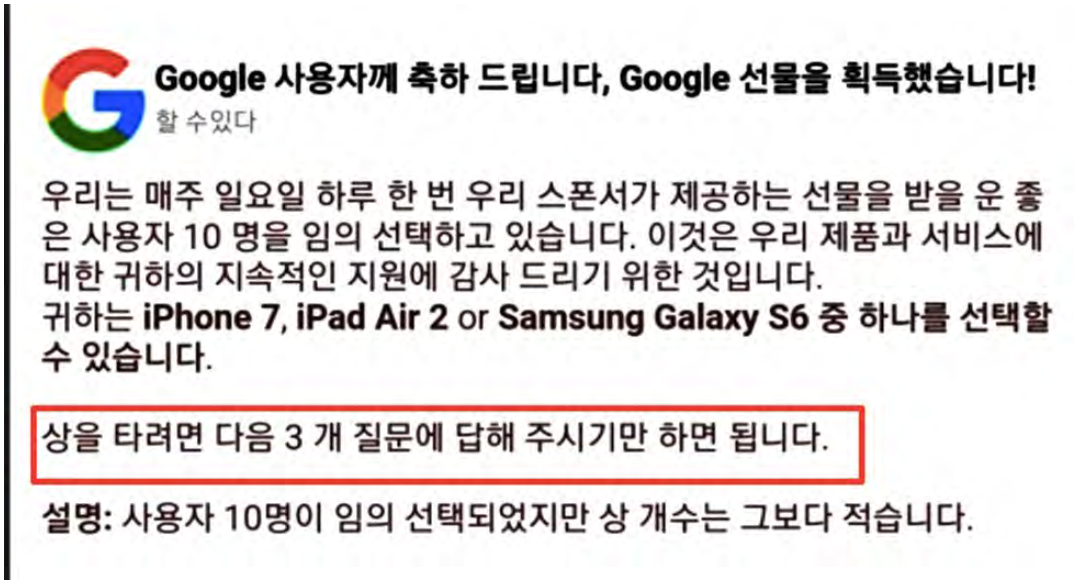
바이러스 퇴치 소프트웨어의 업데이트를 정기적으로 확인하시고 포괄적인 검사를 끝까지 마치고 확인하십시오[12]. 또한 새로운 공격에 대비하기 위하여 소프트웨어가 업데이트되도록 매년 계약을 갱신하는 것을 잊지 마십시오.

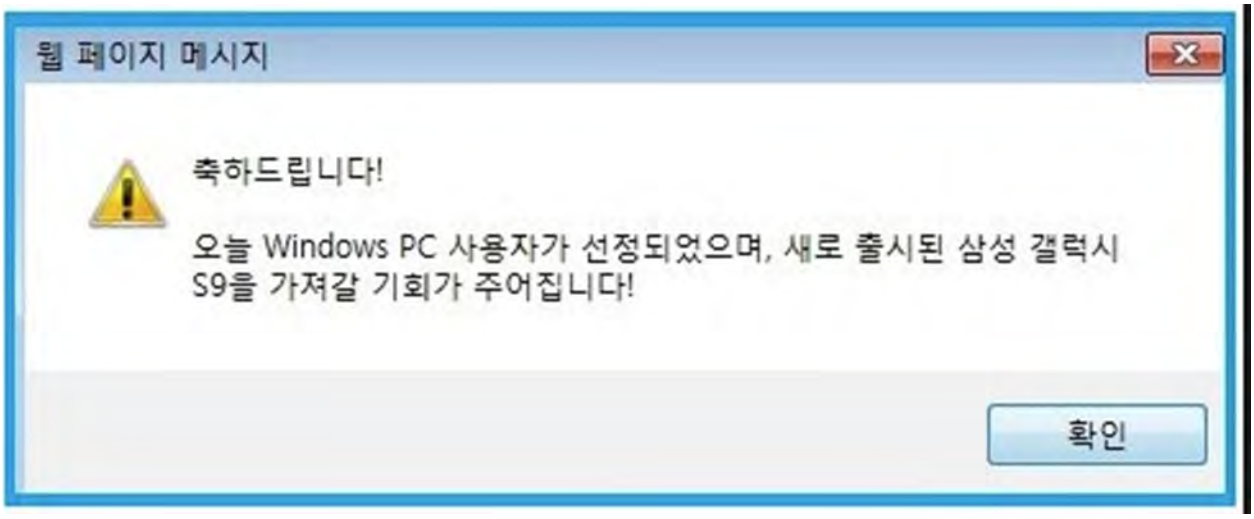
이렇게 해 보십시오!

✓ **닫으십시오.** 팝업 광고나 웹사이트가 수상해 보이면 그 창의 오른쪽 위에 있는 "X"를 클릭해 닫아 버리십시오. 브라우저나 바이러스 퇴치 프로그램이 안전에 의문을 표시하는 웹사이트는 접속하지 마십시오[11].

✓ 다운로드할 것이 무엇인지, 또 그 출처가 안전한지에 대한 확신이 없다면 아무것도 **다운로드하지 마십시오.**

✓ **광고와 팝업 창**들은 자주 시스템 진단 경고처럼 보이거나 당신이 무언가에 당첨됐다고 주장합니다. 그런 것들은 클릭하지 마십시오. 당장 닫아 버리고 컴퓨터나 기타 사용중인 기기에 늘 하는 바이러스 백신 검사를 하십시오. 다음은 피해야 하는 흔한 팝업 창들 중 일부입니다.





비밀 번호 안전

우리는 개인 정보를 돈처럼 다뤄야 합니다 – *그것을 소중히 여기고 보호해야 합니다.* 비밀 번호로 개인의 소중한 정보에 접속할 수 있기 때문에 비밀번호 안전은 매우 중요합니다 – 비밀 번호를 여러분 집의 열쇠처럼 생각하십시오. 다른 사람들이 알아내기 어려운 비밀번호를 만드는 것은 우리 자신을 지키는 중요한 방편입니다.

강력한 비밀번호 만들기.

✓ 길게 만드십시오. 6글자 이상이 바람직합니다.
✓ 모든 계좌에 같은 비밀번호를 사용하지 마십시오
✓ 글자, 숫자와 기호를 적절히 섞어서 쓰십시오.
✓ 자녀의 이름, 생년월일, 나이, 주소 같은 개인 정보는 사용하지 마십시오.
✓ 비밀번호를 정기적으로 바꾸십시오. 전문가들은 최소한 6개월마다 바꿀 것을 권장합니다.

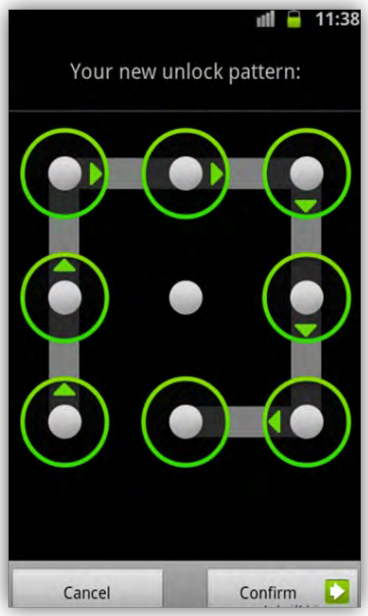
비밀번호 관리자. 비밀 번호 관리 프로그램을 사용하면 여러 계좌에 하나의 비밀번호를 사용할 수 있습니다. 당신이 미리 등록해 놓은 웹사이트에 로그인 정보를 자동으로 입력해 줍니다. 각 프로그램의 장단점을 조사하여 가장 적합한 프로그램을 찾으십시오. 유료 서비스를 옵션으로 제공하고 있는 무료 프로그램 몇 가지를 예로 들자면 다음과 같습니다:

- LastPass
- Keeper
- Dashlane

당신의 비밀 번호가 이 목록에 있습니까?

해커들은 비밀 번호를 추측해서 우리 계좌에 들어 옵니다. 그러니 다른 사람들이 짐작하기 쉽게 만들지 마십시오. 다음에 적힌 비밀번호들은 아무 것도 사용하지 않도록 하십시오: 이것들은 2018년에 가장 흔하게 사용되어서 해킹하기 쉬운 비밀 번호 25개 입니다*

순위	비밀번호
1	123456
2	password
3	123456789
4	12345678
5	12345
6	111111
7	1234567
8	sunshine
9	qwerty
10	iloveyou
11	princess
12	admin
13	welcome
14	666666
15	abc123
16	football
17	123123
18	monkey
19	654321
20	!@#$%^&*
21	charlie
22	aa123456
23	donald
24	password1
25	qwerty123



컴퓨터, 태블릿, 스마트폰 등 **모든 기기를 반드시 잠그십시오**. 비밀 번호를 설정하여 당신 혼자만 사용하십시오.

이중 인증. 이중 인증(2FA)을 하면 보안이 한 단계 더 추가되므로 당신 계좌에 들어가려는 사람을 단념 시키는데 도움이 될 수 있습니다. 누군가 당신의 비밀번호를 알아 냈어도 당신의 계좌에 접속하려면 당신의 전화기가 필요할 것이기 때문입니다. 이중 인증이란 당신이 아는 것(비밀 번호)와 당신이 소지한 것(당신의 휴대전화)의 두가지로 이뤄집니다[13]. 인증 도구는 생체정보, 보안 키, 또는 모바일 기기의 앱을 통해 받는 독특한 일회용 암호 같은 형태가 있습니다[14].

스마트 어시스턴트, 스마트 홈, 와이파이

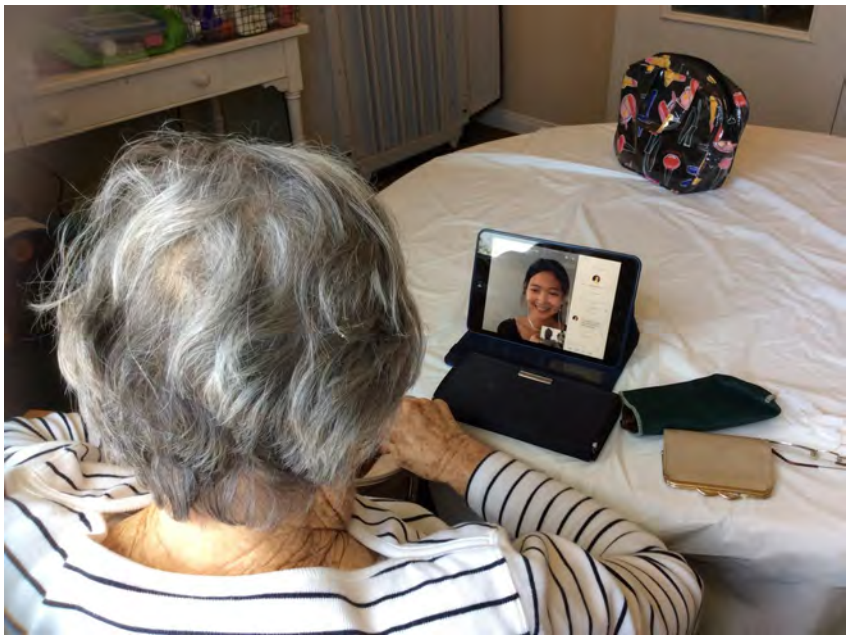
아마존 알렉사 (Amazon Alexa)

같은 음성 보조 장치들이 점점 더 가정에 보급되면서 자신의 사생활 보호를 위해 취할 수 있는 안전 조치들에 대해 알고 있는 것이 중요해졌습니다. **IoT** ("사물 인터넷"이라고도 알려져 있습니다)는 사물들과 기기들이 정보를 주고 받는 것이 가능해진 네트워킹 능력을 말합니다[15]. 모든 스마트 홈 장치들, 가전제품들, 스피커, 장난감, 착용형 기기 등이 모두 포함됩니다. 흔히 "Alexa가 내가 하는 모든 대화를 녹음하고 있을까?"라는 질문을 하는데 Amazon 웹사이트는 아니라고 대답하고 있습니다. 그 장치는 오로지 "음성 구동어" (Alexa)만을 감지하도록 만들어졌고, 그 음성 구동어와 일치하는 음향 패턴을 통해서 인식하지 다른 소리는 아무 것도 "클라우드"에 저장되거나 전송되지 않는다고 설명합니다[16]. 인터넷에 연결된 장치를 사용할 때는 나쁜 의도를 가진 사람이 들어와 정보를 가져갈 가능성이 내재되어 있다는 것을 언제나 명심하십시오. 그러므로 중요한 정보나 개인 정보는 무엇이건 인터넷에서 공유하거나 저장하지 말 것 또한 언제나 기억하십시오

마이크 "끄기" 단추와 전원 차단하기

Voice First (음성 우선) 장치에는 음 소거 단추가 딸려 나오므로 그것을 작동시키면 아무리 음성 구동어를 말해도 장치가 반응을 보이지 않습니다. 그 장치가 확실히 내가 하는 말을 듣거나 녹음하지 못하도록 하려면 그 장치의 전원 플러그를 빼거나 건전지를 제거하십시오.

와이파이 라우터 보호. 무선 라우터가 있으면 매우 자유롭게 노트북과 모바일 기기들을 사용할 수 있습니다. 와이파이 라우터를 구입하면 사람들이 찾아보거나 추측해 낼 수 있게 사전 설정된 경우가 많습니다. 비밀 번호를 바꾸고 무선 네트워크의 이름을 변경해서 당신의 스마트 장치들이 연결되어 있는 인터넷 공급원을 안전하게 해주는 것을 잊지 마십시오[11].



소셜 미디어와 가짜 뉴스

소셜 미디어 네트워크가 지난 3~4년 사이에 크게 대중화 되었습니다. 이들 네트워크는 당신을 언제 어디서나 가족 및 친지들과 연결시켜 주는데, 이 플랫폼을 통해 다른 사람들과 공유하는 것에 대해 주의하면 훨씬 안전해질 것입니다..

이렇게 해 보십시오!

- ✓ **모르는 사람의 친구 신청을 수락하지 마십시오.** 공짜 선물이나 입장권 같은 것을 주겠다며 미끼로 내세워 자기들의 링크를 클릭하거나 직접 만나게 하려는 메시지를 모르는 사용자로부터 받을 수 있습니다. 제품이나 서비스 광고에 포함되어 있는 게시물들도 조심하십시오. 아무리 친구나 당신이 아는 회사에서 온 것 같아 보이더라도 조금이라도 수상한 링크는 절대 클릭하지 마십시오.
- ✓ **당신이 얼마나 정보를 공유하고 있는지 알고 계십시오.** 당신의 온라인 소셜 미디어 프로필에는 당신에 관한 중요한 정보가 상당히 많이 들어 있을 수 있습니다. 이 정보에는 집 주소, 생년월일, 취향, 가족 등등이 포함될 수 있습니다. 당신이 게시하는 것에도 주의하십시오- 친구들을 염두에 두고 올린 정보지만 개인 정보 보호 설정에 따라 사기범들이 볼 수도 있습니다.
- ✓ **Facebook Messenger 나 이메일 대신 다른 것을 사용해 보십시오.** Signal, Whatsapp, 및 ProntonMail 같은 암호화된 앱은 추가된 보안을 제공합니다.

✓ **개인 정보 보호 설정을 확인하십시오.** Facebook 같은 소셜 미디어 플랫폼에서는 누가 당신의 프로필 정보, 게시물, 활동을 볼 수 있는지, 누가 당신의 타임라인에 게시할 수 있는지, 누가 사진에서 당신에게 태그를 붙일 수 있는지를 당신이 관리할 수 있습니다. 당신이 태그된 사진과 게시물을 다른 사람들이 당신 프로필에서 보기 전에 먼저 검토하고 게시할 수 있도록 개인 정보 보호 설정에서 제한을 많이 두는 것이 현명합니다.

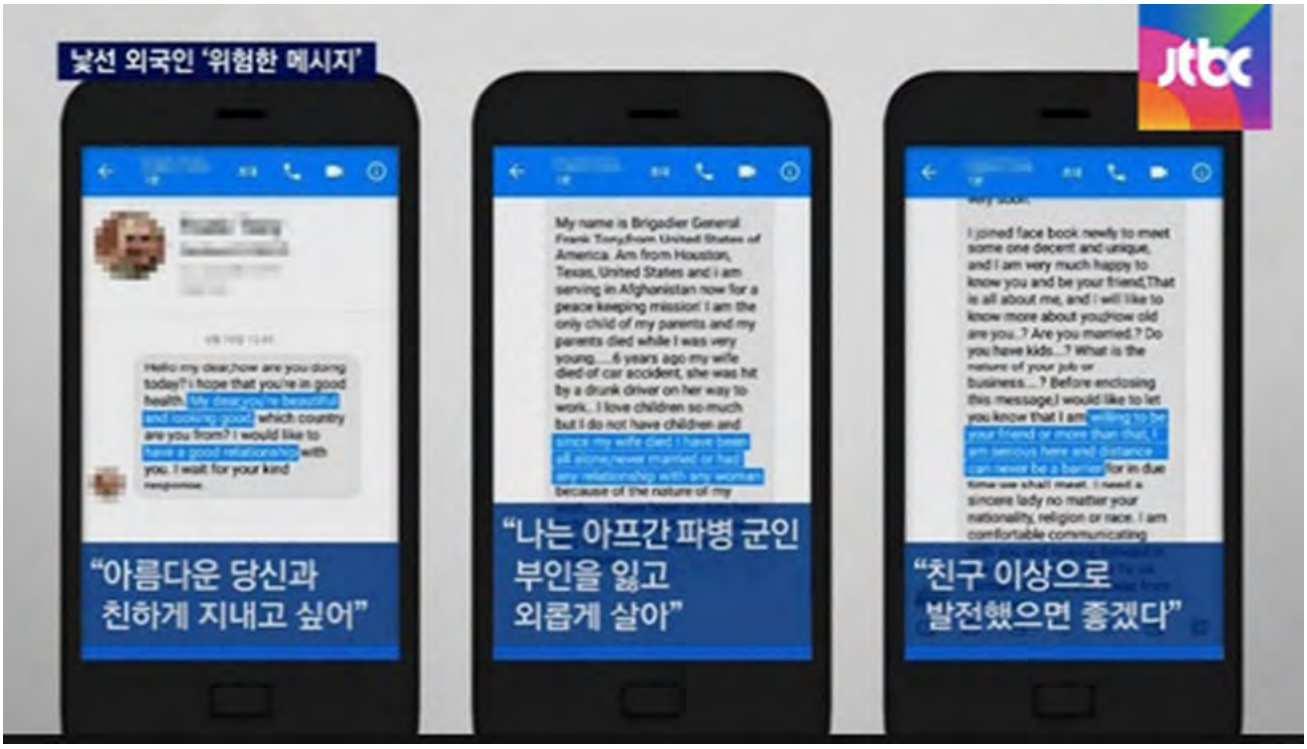
자세히 살피기

"Like(좋아요)"와 비슷합니까? Facebook의 "좋아요"와 비슷해 보이는 버튼이나 오도하는 이미지로 순식간에 당신의 주의를 끄는 비디오 스크린샷은 자기도 모르는 사이에 원하지 않는 쇼핑 웹사이트로 데리고 가거나 바이러스와 악성소프트웨어에 감염시키기까지 합니다

Facebook 게시물 아래쪽에 자리잡고 있는 진짜 "좋아요" 버튼 모양과 처음엔 비슷해 보이게 속이는 가짜 버튼을 구별할 줄 아는 것이 중요합니다. 사람들이 호기심에 특정 링크, 사진, 비디오나 기사를 클릭하고 싶도록 만드는 것을 "클릭베이팅"이라고 합니다. 이렇게 현혹하는 글이나 광고 중에는 그저 다른 웹사이트로 데려 가기만 하는 것도 있지만 일부 해로운 것도 있습니다. 그런데 이렇게 "좋아요" 속임수의 피해자가 되면 자기도 모르는 사이에 가짜 "좋아요" 버튼이 있는 거짓 비디오/이미지를 퍼뜨려 당신의 온라인 친구들까지 피해자로 만들 수 있습니다.

여러 플랫폼에서 당신의 개인 정보 보호 설정을 관리하는 National Cyber Security Alliance—Stay Safe Online 정책에 대한 이 참조 링크를 살펴보십시오. **https://bit.ly/2BYiFVh**

온라인 데이팅 사이트. 온라인 만남 주선 사이트들은 자신이 다른 사람들과 공유하기로 한 것에 대해 조심하고 잘 살피는 한 비슷한 관심사를 가진 사람들을 새로 만날 수 있는 훌륭한 도구입니다. 만남 주선 앱에는 당신을 남부끄러운 사이트로 끌고 갈 링크로 유도하려는 사람들이 올려 놓은 가짜 프로필들도 많다는 것을 알고 계십시오.



이렇게 해 보십시오!

✓ **상대방 프로필에 위험 요소가 있는지 찾아 보십시오**. 소셜 미디어나 만남 주선 앱에서 누군가와 연결될 때 뒤에 숫자가 길게 연결된 이름은 가짜 프로필이라는 신호일 수 있습니다. 제목이나 내용이 혹시 단지 육체적인 것만 찾고 있는 것처럼 보이지는 않습니까?

✓ **상대방이 보내는 링크는 아무 것도 클릭하지 마십시오.** 메시지를 몇 번 주고 받은 다음에 상대방을 알게 되었다 느낄 때는 만나기 위해 전화번호를 공유하는 것에 부담을 느끼지 않게 됩니다. 그러나 대화에 내용이 없이 그저 링크만 보내왔다면 악성소프트웨어와 바이러스가 가득한 웹사이트로 연결될 수도 있으니 그런 링크는 클릭하지 말고 그냥 지나치십시오.

가짜 뉴스. 오늘 날 뉴스와 미디어에서는 무엇이 진짜이고 무엇이 가짜인지 구별하기가 어려울 수 있습니다. 사람들은 이제 그 어느때보다도 많은 정보에 접하지만 누구나 무엇이건 인터넷에 올려 놓고 사실이라고 주장할 수 있기 때문에 무엇이 진실인지를 항상 분명하게 알 수 없습니다. 그렇다면 무엇이 신뢰할만한 뉴스 출처인지는 어떻게 알 수 있을까요?

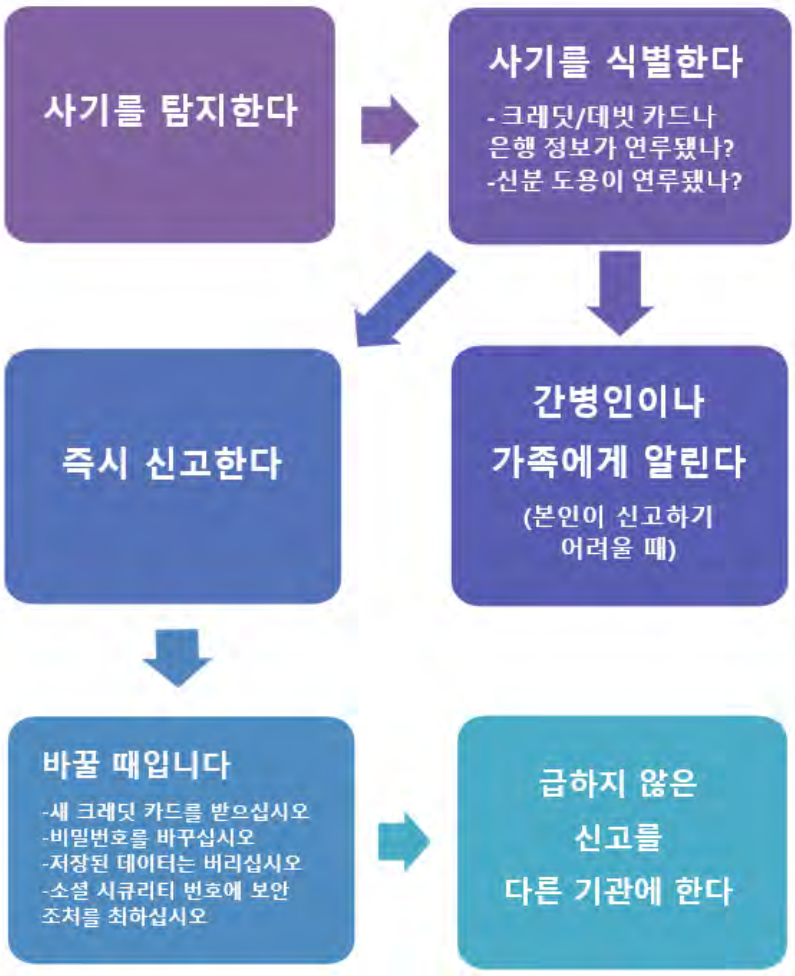
이렇게 해 보십시오!

✓ **출처를 감안하십시오.** 어떤 웹사이트를 방문하면 그 사이트 자체에 대한 정보를 수집하십시오. “About Us” (자기 소개)란을 들여다 보십시오. 누가 그 사이트를 운영하고 있습니까? 왜 그 사이트를 만들었습니까? 누가 사이트 유지비를 지불하며 후원자를 지지합니까? 거기 실린 정보들은 어디서 나온 것입니까? 웹사이트 주소의 맨 끝만 봐도 신뢰도의 수준이 다양함을 알 수 있습니다. 만일 **.gov** 로 끝났다면 그 사이트는 정부의 웹사이트로, 내용물은 게시되기 전에 여러 차례의 검토와 품질 보증 검사를 거친 것입니다. .edu 로 끝난 사이트들은 학교나 대학의 사이트로, 그 게시물들은 보통 학문적 기준을 고수합니다.

✓ **상호 참조.** 잘 알려져 있고 평판이 좋은 몇가지 서로 다른 뉴스 출처에 가보았을 때 각자의 편향이 있음에도 불구하고 사실에 대해서는 공통점들이 있습니까? 이상하거나 농담처럼 들립니까? 그 정보가 진실임을 확인해 줄 다른 출처가 있습니까?

✓ **조사해 보십시오.** 그 정보가 시사에 적합한지 날짜부터 확인하십시오. 가능하면 전문가에게 문의하거나 사실 확인 전문 사이트에 조회하십시오.

사이버 사기 대응 절차



신고 기관

사기 유형	기관 및 연락 방법
일반 사기 신고 (권장)	**각 지역 법 집행 당국** 경찰은 당신을 돕고 적절한 타 기관에 위탁할 의무가 있습니다.
일반 사기 신고 (권장)	**Federal Trade Commission** 전화: 1-877-382-4357 (TTY/TTD: 1-866-653-4261)
인터넷 범죄와 사기 (권장)	**Internet Crime Complaint Center** (IC3) 인터넷을 기반으로 한 모든 범죄와 사기 신고를 받는 곳으로 Federal Bureau of Investigation (FBI) 와 the National White Collar Crime Center (NW3C)가 공조합니다. http://www.ic3.gov/default.aspx
의료 사기 신고	**Federal Trade Commission (FTC)**로 전화하십시오. 1-877-FTC-HELP (1-877-382-4357) 또는 TTY 1-866-653-4261 또는 웹사이트를 방문하십시오: ftc.gov/complaint
메디케어 사기	**Department of Health and Human Services** 전화 : 1-800-633-4227 메디케어 및 메디케이드 사기, 낭비, 남용 신고 전화: 1-877-808-2468 **Senior Medicare Patrol** www.smpresource.org **Office of the Inspector General** 1-800-447-8477 또는 이메일 spoof@oig.hhs.gov
신분 도용 범죄	**Identity Theft Resource Center** 전화: 1- 888-400-5530 http://www.idtheftcenter.org/knowledge-base/
스페인어 사용자들의 건강 관련 문제	**Su Familia: The National Hispanic Family Health Helpline** 월요일-금요일, 오전9 시부터 오후 6 시까지 (동부시간) 전화 : 1-866-Su-Familia (1-866-783-2645)
IRS 및 세금 관련 사기	**IRS's Identity Protection Specialized Unit** 전화 : 1-800-908-4490 **Internal Revenue Service** 본인 또는 아는 사람이IRS 라 주장하며 개인 또는 재정 정보를 요구하는 이메일을 받았을 경우, 그 이메일을 다음 주소로Internal Revenue Service 에 전달하십시오phishing@irs.gov.

사기 유형	기관 및 연락 방법
IRS 및 세금 관련 사기	**IRS's Identity Protection Specialized Unit** 전화 : 1-800-908-4490 Internal Revenue Service 본인 또는 아는 사람이IRS 라 주장하며 개인 또는 재정 정보를 요구하는 이메일을 받았을 경우, 그 이메일을 다음 주소로Internal Revenue Service에 전달하십시오phishing@irs.gov.
복권 사기	**AARP Fraud Fight Call Center** 외국 복권 사기는 모두 신고하십시오. 전화: 1-800 646-2283 **U.S. Postal Inspection Service** 복권이나 우편 사기는 무엇이든 신고하십시오. 1-877-876-2455
소셜 시큐리티 사기	**Social Security Administration** 전화: 1-800-269-0271 (TTY: 1-866-501-2101) 오전 10시부터 오후 4시까지 (동부시간) http://oig.ssa.gov/report/
여권 사기	**Department of the State** 이메일: PassportVisaFraud@state.gov
비지니스 사기	**Better Business Bureau** 웹사이트에 신고하십시오 https://www.bbb.org/consumer-complaints/file-a-complaint/get-started
피싱 이메일 신고	**Department of Homeland Security, U.S. Computer Emergency Readiness Team** 이메일: phishing-report@us-cert.gov 또는 Federal Trade Commission에 이메일(spam@uce.gov)로 신고하거나, 피싱 이메일을 spam@uce.gov 로 전달해도 됩니다.
일반적인 성인 학대 신고	**Adult Protective Services** 는 California Department of Social Services 산하기관으로 노인과 피부양 성인에 대한 지원을 제공합니다. 신체적 학대, 성적 학대, 자기 방치, 유기, 재정적 학대, 심리적 학대, 타인에 의한 방치 등 학대가 의심되면 신고하십시오. 자세한 정보는 http://www.cdss.ca.gov/Adult-Protective-Services 를 방문하십시오. 전화번호는 캘리포니아의 카운티마다 다릅니다: http://www.cdss.ca.gov/inforesources/County-APS-Offices

자료

온라인 보안에 관하여 더 배우거나 다른 사람들을 가르치고 싶다면, 다음의 자료 목록이 도움이 될 것입니다.

명칭	웹사이트
AARP (American Association of Retired Persons) 는 노인을 표적으로 한 사기에 관한 최신 뉴스를 제공합니다.	http://www.aarp.org/money/scams-fraud/ 사기 상담 훈련을 받은 자원 봉사자들과 연결되는 전화 번호입니다. 1 (877) 908-3360.
CFTC (Commodity Futures Trading Commission) 는 미국 선물시장 사기에 관해 소비자들을 교육시킵니다 .	http://www.cftc.gov/ConsumerProtection/Resources/index.htm
Consumer Financial Protection Bureau 는 금전 사기 및 사기성 금융 제품에 관한 정보를 제공합니다.	http://www.consumerfinance.gov/
FBI (Federal Bureau of Investigations)는 대규모 마케팅을 이용하여 소비자들에게 사기를 치려는 계획들에 대한 정보를 제공합니다.	https://bit.ly/2rWBZOK
ElderCare.gov 는 노인을 위한 법률, 재정 지원 같은 서비스를 제공하는 커뮤니티 서비스에 연결시켜 줍니다.	https://eldercare.acl.gov/Public/Index.aspx
Federal Trade Commission 은 신종 및 기존 사기 수법에 대한 정보와 함께 자신을 보호하는 요령들을 제공합니다.	http://www.consumer.ftc.gov/scam-alerts FTC가 벌이는 이 온라인 사기 인식 캠페인도 살펴보십시오: http://www.consumer.ftc.gov/features/feature-0030-pass-it-on
Federal Housing Finance Agency 는 소비자들에게 모기지 구제 사기, 파산 사기, 역 모기지 사기 등 주거 관련 사기를 피할 요령을 알려줍니다.	https://www.fhfa.gov/
U.S. Bureau of Consular Affairs 는 외국에서 범죄 피해자가 된 미국인에게 정보를 제공합니다.	http://travel.state.gov/content/passports/english/go.html

명칭	웹사이트
Internet Crime Complaint Center 는FBI 와 National White Collar Crime Center 가 공조하여 연방, 주, 지역 및 국제적 법 집행 및 규제 기관들에 범죄 신고를 의뢰합니다.	http://www.ic3.gov/crimeschemes.aspx
Oasis 는 노인들에게 지속적인 학습을 권장하며 사이버 보안 관련 자료를 제공합니다	https://bit.ly/2RrFnQh
Elder Justice Initiative 는 노인 학대 및 금전 사기 피해자와 그 가족에게 U.S. Department of Justice 로부터 관련 정보를 제공합니다.	http://www.justice.gov/elderjustice/
Stay Safe Online by National Cyber Security Alliance 는 당신 자신과 가족을 보호할 요령과 자원을 제공합니다.	https://www.staysafeonline.org/stay-safe-online/resources/
GCF Global 은 인터넷 안전 관련 자원을 제공합니다.	https://edu.gcfglobal.org/en/internetsafety/
Medicare.gov 는 당신의 개인 정보를 보호하고 메디케어 사기를 예방하려면 어떻게 할 것인지에 관한 정보를 제공합니다.	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud

참조

[1] Anderson, Monica and Andrew Perrin. “Technology Use Among Seniors.” *Pew Internet Center*, 17 May. 2017. Web. 31 Dec. 2018. http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

[2] New York State Office of Children and Family Services “Under the Radar: The New York State Elder Abuse Prevalence Study.” *Self Reported Prevalence and Documented Case Surveys Final Report* 2011. Web. 31 Dec. 2018. https://ocfs.ny.gov/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf

[3] Office of Financial Protection for Older Adults “Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends.” *Consumer Financial Protection Bureau*, February 2019. Web. 12 March 2019. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

[4] Baig, Mehroz. “Elder Abuse and Technology.” *The Commonwealth Blog*, 6 Jun. 2013. Web. 4 Jan. 2016. http://www.commonwealthclub.org/blog/2013-06-06/elder-abuse-and-technology

[5] VanDeVelde, Amy. “Oasis YouTube video provides great guidance on how to navigate and trust what you hear on the news.” *Oasis Blog*, 14 March 2018. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/is-it-fake-news-find-out-how-to-know-for-sure-151661?utm_source=Center+0&utm_medium=email&utm_campaign=7585+March+2018+Discoveries&utm_term=620598

[6] Federal Trade Commission. "Health Care Scams." *Pass It On Resource Guide*, 2014. Web. 31 Dec. 2018. https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0183-health-care-scams.pdf

[7] Sjouwerman, Stu. “Scam Of The Week: New FBI and IRS Alerts Against W-2 Phishing.” *KnowB4 Security Awareness Training Blog*, 18 March. Web. 31 Dec. 2018. https://blog.knowbe4.com/scam-of-the-week-new-fbi-and-irs-alerts-against-w-2-phishing

[8] The Office of Investor Education and Advocacy (OIEA). “Investor Alert: Prime Bank Investments Are Scams.” U.S. Securities and Exchange Commission, 5 Feb. 2015. Web. 4 Jan. 2016. http://www.sec.gov/oiea/investor-alerts-bulletins/ia_primebankscam.html

[9] The Federal Bureau of Investigation. “Common Fraud Schemes.” *Scams & Safety*, 2010. Web. 4 Jan. 2016. https://www.fbi.gov/scams-safety/fraud

[10] AARP. “Prevention, Not Just Awareness, Key to Cyber Security.” Web. 31 Dec. 2018. https://states.aarp.org/prevention-awareness-cyber-security/

[11] Stay Safe Online. “Shopping Online.” *Online Safety Basics*. Web. 31 Dec. 2018. https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

[12] Kirchheimer, Sid. "Is Your Computer Infected." *AARP*, 9 Jan. 2012. Web. 31 Dec. 2018. https://www.aarp.org/money/scams-fraud/info-01-2012/computer-infected-scam-alert.html

[13] VanDeVelde, Amy. “Two factor authentication adds an essential layer of security.” *Oasis Blog*, 17 October 2017. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/want-more-protection-for-your-email-and-facebook-accounts-135523

[14] National Cyber Security Alliance. “Cheers to Safe Cybershopping!” *Stay Safe Online*. Web flyer. 31 Dec. 2018. https://staysafeonline.org/wp-content/uploads/2018/11/Online-shopping-tip-sheet-1118.pdf

https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230&pop-up=1

[15] “IOT.” *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

[16] Amazon.com. “Alexa and Alexa Device FAQS” Web. Feb. 2019. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

우리의 임무: 개개인이, 특히 나이를 먹으며 더 충만하게 살 수 있도록 돕기 위해 행복감과 자주성을 향상시키는데 있어 기술을 혁신적으로 사용할 방법을 탐구합니다.

우리의 비전: 기술 혁신은 개개인이 자기 집에서 "자기 식으로 삶을 사는" 능력을 향상시키는데 중요한 역할을 합니다. 우리의 목표는 우리 각자의 몸과 마음과 영혼이 더욱 성장하고 행복감이 유지되고 향상되도록 기술적 해결책들을 활용하는 것입니다.

우리의 프로젝트: 저희의 계획은 사회적 소속감 강화, 뜻있는 참여와 성장 및 전인적 건강의 권장, 주도적 참여로 건강과 행복에 대한 통제력 증대, 기동력, 시력, 청력 및 인지 능력에 대한 지원 확대, 응급 상황이나 심각한 사태 발생의 사전 방지, 보살핌을 제공하는 사람들에 대한 지원과 권한 부여, 건강하고 안전하고 접근이 용이하고 오랫동안 지속 가능한 환경 조성과 같은 주요 영역에 초점을 맞춘 다양한 범주의 기술 및 혁신을 말합니다.

더 자세히 알고 싶으시면 www.fpciw.org를 방문해 주십시오.

front porch

CENTER FOR INNOVATION AND WELLBEING