BIPT

BURNABY
INTERCULTURAL
PLANNING TABLE

스캠, ㅏ기, 인터넷 안전과 온라인 괴롭힘

청소년, 학부모, 시니어를 위한 팁

Funded by:

Immigration, Refugees and Citizenship Canada

Finance par :

Immigration, Refugies et Citoyennete Canada

스캠, 사기, 인터넷 안전과 온라인

청소년, 학부모, 시니어를 위한 팁

차 례:

소개:

Intercultural Connections Working Group

Andisheh Fard - SFU
Cindy Chang – City of Burnaby Recreation & Cultural Services
Darae Lee - MOSAIC
Deborah Baker – Squamish Nation
Duncan Olenick – Burnaby Public Library
Evelyn McGowan – Purpose Society / Burnaby Youth Hub
Gabriella Maio – Ministry of Children and Families Development
Heather McCain – Citizens for Accessible Neighbourhoods
Kimberly Barwich – Burnaby Neighbourhood House
Melody Monro – Fraser Health
Natalya Khan – Burnaby School District #41
Rebekah Mahaffey – City of Burnaby
Sangeeta Bhonsale – Burnaby Family Life
Shae Wiswanathan – SUCCESS
Tarana Sultan – PIRS
Thea Fiddick – ISS of BC

번역:

아랍어 Arabic:	Abeer Hattab
중국어 Chinese:	Derek Chen Tom Su
페르시아어 Farsi:	Sossan Kayoumi Nabila Akbari Zarif Akbarian
한국어 Korean:	Darae Lee
스페인어 Spanish:	Mary Blanca Battenberg Pilar Sain
티그리냐어 Tigrinya:	Tigist Dubus Tesfamarian Daniel Debesay Michael Tedros Gebrengus Enbakon Berhane Asmait Tekle

보호자를 위한 인터넷 안전 수칙

인터넷안전에 관해 이야기하기- 개인 정보 보호에서부터 신원 도용에 이르기까지, 인터넷사용에는 위험이 존재합니다. 어린이와 10 대 자녀들은 인터넷을 사용할때, 나이에 관계없이 보호자의 감독이 필요하며, 보호자는 주의를 기울여야합니다. 사진, 개인 정보, 현재 위치들을 공유하는 안전문제에 대한 지도가 필요합니다.

- 인터넷으로 해야하는 숙제와 온라인 시간 관리: https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- 보호자를 위한 10 가지 인터넷 안전 팁: https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- 인터넷 안전: https://www.webwise.ie/parents/advice-top-10-tips-for-parents/

지도 부재/이른 인터넷 노출- Shared Hope International 의 조사결과에 따르면, 보호자 8 명 중 1 명은 2 세인 자녀의 인터넷 사용을 허락하였고, 10 명 중 1 명만이 자녀가 10 세 이상이 되었을때 인터넷 사용을 허락하였습니다 (전문가 권고 나이). 결과적으로, 많은 어린이들이 적절한 지도가 부재한 상태로 인터넷을 사용하고 있습니다. 자녀를 해로운 인터넷사용에서 보호하는 방법은 아래와 같습니다.:

- https://protectkidsonline.ca/app/en/interests_and_risks-5_to_7
- https://protectkidsonline.ca/app/en/interests_and_risks-8_to_10
- https://protectkidsonline.ca/app/en/interests_and_risks-11_to_12
- https://protectkidsonline.ca/app/en/interests_and_risks-13_to_15

자녀의 인터넷 사용 관리하기- 불행히도, 보호자의 관심여부와 상관없이 많은 십대 자녀들이 보호자로부터 인터넷 사용기록을 숨기거나 삭제합니다. 그러므로 보호자의 더 큰 노력이 필요합니다. 십대 자녀들에게는 보호자가 모르는 이메일이나 소셜 미디어 계정이 있을 수 있고, 아이들은 이러한 계정을 만들기 위해 본인의 연령에 대해 거짓말을 하기도 합니다.

- https://protectkidsonline.ca/app/en/info_monitoring_online_activities
- 온라인 상 또래의 괴롭힘을 겪는 자녀가 있다면 아래 자료를 참고하세요: https://witsprogram.ca/pdfs/families/pyramid-of-support.pdf

휴대전화- 휴대전화는 연락을 유지하고 응급상황이 발생할 경우 유용하게 쓰일 수 있습니다. 대략 11 세에서 14 세의 69 퍼센트 가 휴대전화를 소지하고 있습니다. 휴대전화 사용자는

전화의 GPS 가 사용자의 정확한 실제 위치를 공개할 수 있음을 인식해야 합니다. 또한, 개인 휴대전화번호를 온라인에 게시하는 것에 대해 주의를 기울여야합니다.

- 자녀에게 전화를 줄때: https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- 휴대전화 안전사용 팁: https://protectkidsonline.ca/app/en/info_phone_safety
- 첫 휴대전화: 책임있게 사용하는 규칙: https://www.ahaparenting.com/Ages-stages/tweens/Cell-Phone-Rules-Safe-Responsible-Kids
- 보호자를 위한 휴대전화 모니터링 앱 정보: https://pumpic.com/parental-monitoring-app-canada.html

온라인 괴롭힘- 익명으로 다른사람에 대한 질문이나 정보를 올릴 수 있는 대화 앱 과 웹사이트들이 있습니다. 예를 들어 Whisper, Yik Yak, Ask.FM, 과 같은 앱들은 괴롭힘을 조장하는 것으로 알려져 있기때문에 위험합니다. 이러한 앱을 이용하여 익명으로 쉽게 다른 사람을 괴롭히고, 조롱하며 놀리게 됩니다. 그러므로 괴롭힘이 의심될 경우 바로 제보를 하는 것이 중요합니다.

- PREVNet: 괴롭힘 방지를 위한 연구 및 참고자료
- 자녀가 사이버 괴롭힘을 당했을 경우 대처 방법: https://needhelpnow.ca/app/en/resources_cyberbullying
- WITSProgram: 괴롭힘을 겪고 있는 아이들을 위한 지원 관련 정보
- RCMP's Centre for Youth Crime Prevention: 청소년 범죄와 희생을 막기위한 정보 자료
- Kids Help Line 보호자와 자녀를 위한 전화 상담
  도움이 필요하다면? 686868 번으로 'CONNECT' 라고 텍스트를 보내면 상담 봉사자와 연결 가능 (24 시간) https://kidshelpphone.ca/search/?keys=Cyberbullying

부적절한 사진-연구에 따르면 7 명 중 1 명의 10 대청소년은 자신의 나체 또는 반 나체 사진을 찍었고, 그 사진의 절반 이상이 인터넷을 통해 공유되었다고 합니다. 인터넷에 공유되는 것을 완전히 제거할 방법이 없다는 것을 인지하는 것은 매우 중요합니다.

- Cybertip.ca: 아동의 온라인 성학대 신고
- https://protectkidsonline.ca/app/en/info_self_peer_exploitation
- https://protectkidsonline.ca/app/en/info_online_extortion
- https://protectkidsonline.ca/app/en/info_online_luring

온라인 쇼핑, 신원 도용, 인터넷 서핑- 인터넷을 사용할때는 주의해야 합니다. 웹 활동 기록은 지속적으로 추적되기 때문입니다. 안전하지않거나 부적절한 웹사이트를 방문하면, 개인 및 금융정보가 노출되거나 컴퓨터가 손상될 수 있습니다. 모든 컴퓨터에는 적절한 보안 및

앤티바이러스 소프트웨어가 설치되어 있어야 합니다. 온라인으로 쇼핑을 하기 위해서는 항상 안전한 인터넷 연결을 사용하고, 공용 컴퓨터를 사용하지 않으며, 웹사이트가 합법적이고 안전한지 확인해야 합니다. 이러한 예방조치를 따르면 보다 안전한 온라인쇼핑을 할 수 있습니다. 최근 어린이를 겨냥한 신분도용 사례가 늘어나고 있습니다. 실제로 18 세 미만의 어린이/청소년은 성인에 비해 신원을 도난당했을 가능성이 51 배가 더 높습니다. 어린이들은 신용기록이 깨끗하고 온라인에 공유하는 개인정보에 대한 경각심이 덜하기 때문에 범죄자들에게 타켓이 되기 싶습니다.

- 자녀의 신용상태 확인: https://www.creditcards.com/credit-card-news/instructions-how-to-check-child-credit-report.php

비디오 게임- 비디오 게임산업은 최근 많은 변화를 불러왔습니다. 많은 게임들은 어린이들이 다른 게임사용자들과 직접 연결을 할수있는 기능을 제공합니다. 다행히 대부분의 게임장치는 보호자가 안전 설정을 할수있는 기능을 가지고 있습니다. 보호자는 반드시 자녀가 비디오 게임을 하는 시간을 관리해야 합니다.

- 4-8 학년을 위한 안전한 게임 자료: http://mediasmarts.ca/digital-media-literacy/educational-games

자녀와 인터넷안전에 관하여 이야기하기:

SOURCE: http://www.family.ca/internet-safety-tips/

1. 개인정보를 보호하기. 보호자의 허락없이 이름, 전화번호, 학교 또는 집주소를 알려주지말기.
2. Facebook 과 Twitter 와 같은 소셜 네트워킹 사이트에서 게시물을 볼수 있는 사람을 선택하기. 보호자와 함께 개인정보 설정을 변경하기.
3. 소셜미디어에 공유하거나, 비공개설정을 포함한 인터넷에 올리는 모든 내용은 다른 사람이 볼수있음을 알기. '포스트' 또는 '보내기' 를 클릭하기 전 항상 다시 생각하기.
4. 온라인에서 부적절한 내용을 보았을 경우 보호자나 믿을 수 있는 어른 (선생님 등) 에게 조언을 구하기. 부적절한 내용을 우연히 보게 된 것은 잘못이 아니라고 말해주기.
5. 누군가 이메일이나 소셜미디어를 통해 무례한 것을 보낸다면, 절대 응답하지말고 보호자나 믿을 수 있는 어른에게 이야기하기.
6. 다른 사람이 포함된 사진이나 비디오를 공유하는 경우 항상 먼저 허락을 요청하기.
7. 보호자의 허락없이 온라인으로 물건을 사거나 다운로드 하지 말기.
8. 온라인으로만 알고 있는 사람과 직접 만나기 말기. 자신의 실제 신분 (나이, 성별 등) 을 속이고 있을수 있음!
9. 비빌번호를 다른 사람과 공유하지 않기.
10. 괴롭힘에 동참하지 않기– 다른 사람을 험담하거나 놀리지않기. 온라인 괴롭힘에 관한 정보 http://www.family.ca/standup/

사기 및 사이버 안전을 위한 수칙

사기성 전화:

큰 회사나 기관을 사칭하는 전화를 조심하세요.

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdInt-clls-en.aspx

사기성 전화를 받았을 경우:

회사나 기관을 사칭하는 사기성 전화를 받았을 경우 바로 끊습니다. 확실하지 않을 경우 전화를 끊은 후, 해당 회사의 고객 서비스센터에 다시 문의하십시오. 사기성 전화 신고: **http://www.antifraudcentre-centreantifraude.ca** 또는 전화 1-888-495-8501.

온라인 사기:

이메일, 이벤트, 프로모션이 실제인지 사기인지 알아내는 것은 쉬운 일이 아닙니다. 조건이 너무 좋아보일수도 있습니다. 사기일 경우 나타날 수 있는 특징을 알고있는 것이 도움이 될 수 있습니다. **https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx**

더 많은 정보가 필요하다면?

사기에 관한 온라인 정보. **The Financial Consumer Agency of Canada website** 를 방문하셔서 은행 및 기타 금융기관과의 거래 시 여러분의 권리에 대한 정보를 확인하세요. 전화번호 1 800 O-Canada (1-800-622-6232), TTY: 1-800-926-9105.

온라인 사기를 당했을때 해야할 일

캐나다에서 가장 흔한 사기 중 하나는 상대방이 사업체 또는 정부기관으로 신원을 사칭하는 피싱 또는 스미싱 사기입니다. 예를 들어 캐나다 국세청 (CRA)를 사칭하며 돈을 내지않으면 경찰이 와서 체포할 것이라고 한다거나, 환불을 받기위해 링크를 누르라고 알려줍니다. 일부는 사용자를 새로운 웹페이지로 안내한 후 개인정보 변경사항을 검토하고 양식을 작성하라는 메세지를 받습니다.

메세지가 합법적인지 확실하지 않으면 응답하지 마십시오. 기관의 웹사이트를 직접 방문하여 직접 전화를 하십시오. 캐나다 국세청 (CRA)를 사칭한 사기성 전화가 매우 많으므로 CRA 에서는 다음과 같은 조언을 제공합니다:

- CRA 는 이메일이나 문자를 통해 개인정보를 요구하지 않습니다.

- CRA 는 비트코인 또는 기프트카드로 결제를 요청하지 않습니다.

CRA 에 돈을 지불해야한다는 전화, 문자 메세지 또는 이메일을 받는다면 My Account or My Business Account 계정을 이용하여 확인하거나, CRA 에 직접 전화로 확인하십시오. 1-800-959-8281.

사기의 피해자가 되었을 경우 다음과 같은 조치를 취할 수 있습니다.:

1. 거주 지역 담당 경찰 비응급 전화로 신고: 버나비 거주자는 604-646-9999 또는 웹사이트: **http://burnaby.rcmp-grc.gc.ca**

2. 사회보장번호 (Social Insurance Number) 를 도난당한 경우 서비스 캐나다에 신고 1-800-206-7218

3. RCMP 의 캐나다 사기방지 센터(**Canadian Anti-Fraud Centre)** 에 신고.

은행 등의 Sign-in Partner 나 GCKey 를 사용하셔야합니다. 전화신고는 1-888-495-8501 로 하시면 됩니다.

은행이나 크레딧카드회사를 사칭하는 사기전화도 비슷한 수법을 사용합니다. 예를 들면, 거래하지 않는 은행임에도 사용내역서를 검토하도록 요규하는 이메일이나 전화문자를 받을 수 있습니다. 본인이 거래하지않는 은행일 경우, 사기성 메세지임을 쉽게 구분할 수 있으나, 실제 본인이 거래하는 은행을 사칭할 경우 진실 여부를 가리기위해 직접 은행에 문의하거나,온라인뱅킹을 통해 확인을 해야합니다. (물론 안전한 인터넷연결을 사용하여) 사기일 경우, 해당 은행에 신고하는 것도 잊지 말아야합니다.

더 많은 정보: **Canadian Centre for Cyber Security**.

안전한 사용안내: **TWITTER, FACEBOOK, INSTAGRAM.**

스마트 기기에서 개인 정보를 보호하는 5 가지 방법 (스마트폰/태블릿/스마트워치):

아래의 정보는 가정에서 사용하는 인터넷에 연결된 모든 장치에 적용됩니다. 스마트장치는 재미있고 우리의 삶을 편하게 해주지만, 해커들이 개인적 정보에 접근할 수 있는 기회를 제공하기도 합니다. 본인과 가족의 안전을 위해 아래의 정보를 확인하세요:

1. **와이파이 네트워크 보안:** 스마트 기기는 인터넷을 사용하여 정보를 보내고 수집합니다. 가정의 와이파이 연결이 안전하지 않으면, 정보도 안전하지 않습니다. 와이파이를 사용할때는, 최소 무선 암호화 및 비밀번호 설정을 해야합니다. 무선 설정에서 라우터에 WPA2 암호화가 활성화되어 있는지 확인하십시오. 그 다음 어려운 비밀번호로 무선 네트워크를 잠그십시오. 어려운 비밀번호는 대문자,소문자, 숫자 및 특수문자를 조합하여 만들 수 있습니다. 가능하다면, 와이파이 네트워크에 별도의 네트워크영역을 만들어 스마트 기기를 연결하십시오. 이를 ' 기기 격리 (device isolation)' 라고 하며 게스트 와이파이 (Guest Wi-Fi) 네트워크와 비슷한 원리입니다. 이동 중 스마트 기기를 사용할 경우, 신뢰할 수 있는 암호로 보호된 네트워크에만 연결하고, 와이파이 네트워크 자동검색/연결 기능을 끄십시오.

2. **사용하지 않을때 위치정보 설정 끄기:** 많은 스마트기기에는 지도 등 위치정보를 사용하여 서비스를 제공하는 앱이 있습니다. 앱에서 사용자위치를 볼수있다면, 해커 또한 마찬가지입니다. 위치정보를 사용하지 않을 때는 설정을 끄십시오.

3. **앱을 설치하기 이전에 앱의 개인정보보호정책 및 사용약관 이해:** 모든 앱에는 정보를 볼 수 있는 사람과 볼 수 있는 내용을 제한하는데 도움이 되는 개인 정보 설정이 있습니다. 이름이나 연락처 등의 개인정보의 접근을 제한하도록 개인정보 설정을 바꿔야합니다. 불필요하거나 과도한 정보를 요구하는 앱을 주의하고 모든 것에 대해 '허용'을 클릭하지 마십시오.

4. **사용하지않을때 마이크 및 카메라 끄기:** 대부분의 헤드셋, 스마트 티비, 스마트 워치, 스마트 스피커는 마이크와 카메라와 내장되어 있습니다. 안전하지않은 경우, 원하지 않는 정보가 스마트 기기를 통해 전송될 수 있습니다. 사용하지 않을때는 마이크와 카메라 기능을 끄십시오.

5. **개인정보를 포함하지않는 사용자 이름 만들기:** 과도한 정보제공은 위험합니다. 로그인 이름을 만들거나 할 경우, 아이디가 본인의 이름, 나이, 위치, 연락처 등의 개인정보를 포함하지 않도록 주의하세요.

6. **스마트폰 이해하기:** 스마트폰은 위치추척을 포함하여 연락처 등의 정보를 노출할 수 있습니다. 신뢰할 수 있는 앱을 사용하고, 암호 또는 지문인식기능으로 전화기를 보호하세요. 전화 분실시 다른 방법을 사용하여 데이터를 복구하거나 삭제할 수 있는 법을 알아두세요. **ConnectSafely.org/cellphone-safety-tips.**

7. **인터넷 라우터 보안:** 가정에서는 인터넷연결을 위해 라우터 또는 광대역 모뎀이라고 하는 작은 장치를 사용합니다. 라우터에는 비밀번호와 사용자이름을 설정하는데 때로는 기본으로 설정되어있는 비밀번호를 추측하기가 매우 쉽습니다. 도움이 필요하다면 전문가나 인터넷회사에 연락해 비밀번호를 변경하는 법에 대한 조언을 구하세요.

8. **장치를 보호하기:**
   비밀번호 설정으로 장치를 보호하고, 컴퓨터의 경우에는 보안 및 방화벽 소프트웨어가 제대로 설정이 되어있는지 확인을 하세요. 도움이 필요하다면 컴퓨터지식이 있는 친구나 가족, 또는 인터넷/핸드폰 사업자등에게 문의하세요. 신뢰할 수 있는 회사가 제공하는 무료 보안소프트웨어를 사용할 수 도 있습니다. **ConnectSafely.org/securityvendors**.

더 많은 정보를 위해서 아래 링크를 방문하세요:

FightSpam.gc.ca: 스팸 및 온라인 위협을 피하기 위한 정보
Youth Privacy: Office of the Privacy Commissioner 청소년의 개인정보 보호를 위한 정보

온라인 쇼핑 중 자신을 보호하는 방법:

강력하고 고유한 비밀번호: 이메일과 소셜미디어 계정에 강력한 비밀번호를 사용하세요. 계정관리를 믿고 맡길 수 있는 사람이 아니라면 비밀번호를 다른 사람과 절대 공유하지 마세요. 비밀번호는 8 자 이상이어야 하고, 숫자, 대문자, 소문자, 특수 기호를 포함하며 이름이나 흔한 단어를 사용하지 마세요. 더 많은 정보: **ConnectSafely.org/passwords**

링크를 열지마세요: 은행, 크레딧카드 회사, 정부기관 또는 그 외 다른 회사이름으로 오는 이메일이나 소셜미디어에 포함된 링크를 100% 합법적이라고 믿을 수 있는 경우 외에는 열지마세요. 링크를 누르면 합법적으로 보이는 웹사이트로 연결이 되지만 이는 개인정보를 도용하기 위해 만든 사기 사이트일 수 있습니다. 회사이름이 이메일 주소에 포함되어있다고 하더라도, 사기일 수 있습니다. 가장 안전한 방법은 평소와 같이 직접 웹사이트 주소를 입력해 해당 사이트를 방문하고, 의심스러운 경우 기관이 직접 전화하여 확인하는 것입니다.

비현실적으로 좋은 제안을 경계하세요: 참가하지않은 콘테스트에서 우승했다거나, 휴가 또는 상품에 대해 낮은 가격으로 제공받는다는 제안에 주의하세요. 특히 저렴한 의약품 또는 의료혜택에 대한 제안에 주의하세요.

믿을 수 있는 온라인 판매상 이용: 한번도 들어본적 없는 온라인 판매상은 주의하세요. 대부분은 합법적이지만 그 중 일부는 크레딧카드의 정보나 기타 정보를 훔치거나, 지불한 비용에 비해 제대로 되지 않은 물건을 제공할 수 있습니다. 의심스러울 경우, 온라인 쇼핑에 익숙한 사람에게 물어보거나, 판매자에 대한 리뷰를 잘 확인하세요.

쇼핑 및 온라인뱅킹: 쇼핑 및 온라인 뱅킹을 할때 주소창에 *https* 를 확인하세요. https 의 s 는, 보안의 "secure"를 의미합니다. 브라우저의 주소가 *http* 라면 보안된 사이트가 아닙니다. 모바일 앱을 사용하여 쇼핑하거나 온라인뱅킹을 할 경우, 해당 회사의 앱이 맞는지 확인하고, 확실하지 않을 경우 전문가의 도움을 받으세요.

크레딧가드 사용: 온라인쇼핑을 할때는 크레딧카드를 사용하거나 안전한 온라인 결제서비스인 Paypal 또는 데빗카드를 사용하세요. 절대 현금이나 머니오더를 보내지마세요. 개인수표를 보내는 것 또한 위험할 수 있습니다. 문제가 생길경우 크레딧 회사는 조사가 이루어지는 동안 결제를 중단해줄 수 있습니다. 데빗카드 또한 이러한 보호장치가 있지만, 돈을 돌려받기 위해서 시간이 걸릴 수 있습니다. Paypal, Android Pay, Apple Pay 등 도 이러한 보호가 가능하지만, 크레딧 카드를 사용하는 것이 제일 좋습니다.

클릭을 하기 전 다시 한번 확인하세요: 잘못된 주식을 사고 팔거나, 환불이 불가능한 항공편이나 호텔 객실 구매 등, 취소를 할 수 없는 경우가 있으므로, 결제 클릭을 하기 전 늘 확인을 하세요. 실수를 한 경우 회사에 즉시 연락해 취소가 가능한지 물어보세요. 많은 온라인

판매자는 구매를 취소할 수 있는 기능이 있지만, 즉시 취소를 해야합니다. 일단 상품이 배송준비가 되면 주문을 취소하기에는 너무 늦습니다. 구매 상품을 반품할 수 있지만, 반송 배송비를 지불해야 할수도 있습니다. 반품 정책이 어떠한지 확인하고, 배송, 취급수수료 및 세금을 포함한 모든 요금정보를 확인하세요.

크라우드 펀딩: Kickstarter, Indiegogo, GoFundMe 같은 크라우드펀딩은 새로운 제품을 구매하거나, 의미있는 일에 기부를 하는 등, 도움이 필요한 사람들과 기관에 도움을 줄 수 있는 좋은 방법이지만, 언제나 주의를 기울여야 합니다. 설명을 꼼꼼히 읽고, 기부를 요청하는 사람이나 기관에 대해 조금 더 알아보세요. 어떤 목적으로 기부를 요청하는지, 사실을 바탕으로 하는지 확인을 하세요. 의심이 든다면, 돈을 보내지 마세요.

신원 도용 방지: 합법적인 은행 계좌, 크레딧 카드, 대출 신청, 신용조회 등의 경우 외에는 절대 사회보장번호 (Social Insurance Number) 를 제공하지 마세요. 합법적인 사이트인 페이스북이나 은행 사이트에서도 생년월일을 요청하지만, 합법적인 사이트인지 확실하지 않다면, 생년월일, 출생지, 주소 등 개인정보를 입력하라는 메세지가 나올때 주의하세요. 합법적인 온라인 판매자에게만 크레딧카드 정보를 입력하고, 의심이 들때는 좀 더 조사를 해봐야합니다.

온라인 뱅킹 계좌 확인하기: 크레딧카드, 데빗카드, 은행계좌에 잘못된 청구내역이 없는지 항상 확인하세요. 의심이 가는 내역이 있다면, 즉시 은행과 카드회사에 연락해 신고하세요. 온라인뱅킹을 하지 않더라도, 사기의 피해자가 될 수 있습니다. 문제가 있을 경우 즉시 신고를 하세요. 대부분의 경우 사기를 당했을 경우 보호를 받을 수 있지만, 신고를 해야합니다.

기부 사기: 대부분의 비영리 자선단체는 웹사이트와 온라인 기부 옵션이 있습니다. 여러분이 알고있고, 지원을 하는 합법적인 단체라면 문제가 없지만, 자선 단체처럼 보이는 기관에서 온라인 기부를 요청하는 이메일을 받았다면 주의하세요. 익숙하지 않은 기관을 경우 CharityNagitator.org 에서 확인을 하고, 온라인으로 기부를 하려는 경우, 기관의 합법적인 사이트에서 하세요. 이메일에 첨부된 기부 링크를 클릭하지말고, 브라우저에 웹사이트주소를 직접 입력해서 기관의 홈페이지로 방문하세요.

온라인 쇼핑에 관련한 조언

(Source: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx)

신뢰할수 없는 쇼핑 사이트의 예

- 사이트가 엉성하게 만들어졌고 제대로 관리가 되지 않음
- 업체의 주소나 전화번호를 찾을 수 없음
- 판매, 반품 및 개인정보보호 정책이 찾기 어렵거나 없음
- 뒤로가기 버튼을 사용할 수 없음. 다시 말해 페이지에서 앞으로 돌아가는 기능이 없음
- 구매를 하지 않음에도 크레딧 카드 정보를 요구함

온라인쇼핑 시 자신을 보호하는 법

- 현금대신 크레딧카드로 지불하기
- 비현실적으로 싼 가격에 주의하기
- 온라인 결제시 공용 와이파이를 사용하지 말기
- 개인정보 보호 정책을 읽기 정보가 어떻게 사용되는지 이해하기
- 개인재정정보를 요구하는 이메일이나 팝업메세지에 응답하지말기 합법적 회사는 개인정보를 이렇게 요구하지 않음.
- 크레딧카드 명세서를 확인하고 청구내역 확인하기
- 보안 방화벽이 켜져있는 지 확인하기. 최신버젼의 윈도우에서 방화벽 기본설정을 확인하여 늘 켜놓기:
    - 시작 단추를 클릭한 다음 제어판을 선택하여 윈도우 보안방화벽 (firewall) 을 열기
    - 또는 찾기에서 "firewall" 검색
    - 왼쪽창에서 방화벽 켜기 또는 끄기 선택
- 비밀번호, 주소 등의 개인정보 자동입력기능을 사용하지말고, 크레딧카드 정보를 사이트에 저장하지말기

씨니어 안전: 사기의 피해자가 되는 것을 방지할 10 가지 수칙

(Source: https://www.freedomshowers.com/blog/senior-safety-10-tips-avoid-victim-fraud/)

어느 날, 집에서 차를 마시는 중 전화가 울립니다.
"할머니 안녕하세요, 저 할머니 손자에요. 지금 지갑하고 여권을 잃어버려서 돈이 필요한데 보내주실 수 있으세요?" 전화기 너머 명확하지않은 목소리에 어떤 손자인지 알수없었지만, 누구냐고 물어보면 손자의 기분이 상할까봐 물어보지 않았습니다. 빨리 손자를 도와주고 싶은 마음에 어떻게 돈을 보내주면 될지 물어봅니다. 안타깝게도 그것은 손자가 아니라, 할머니의 손자사랑을 이용해 돈을 훔치려는 사기꾼입니다.

이와 같은 전화는 다른 사람의 돈을 노려 빈번하게 발생하며, 이러한 사기전화의 발생수는 놀라운 속도로 늘어나고 있습니다. 많은 피해자들이 피해를 보고하지않기때문에 실제로는 더 많을 것이라 추측됩니다.

예방법

- 경찰, 판사 또는 정부기관은 송금기관을 이용해 돈을 내라는 요청을 절대 하지 않습니다.
- 상대에게 개인정보를 절대 알려주지마십시오.
- 송금을 고려하기전에, 가족이나 친구가 어디있는지 다른 사람에게 연락해 먼저 확인하세요.
- 모르는 사람에게 돈을 송금하지마세요. 도와주기 전에 상대의 신원을 확인하세요.

사기의 피해자가 되는 것을 막기 위한 10 가지 방법:

1. 비현실적으로 좋은 조건은 말그대로 비현실적입니다. 사기꾼은 사람들의 빠른 해결, 기적적인 효과와 쉽게 돈 버는 법을 원하는 심리를 이용합니다. 무료 제품과 서비스, 큰 선물을 제공하는 척 하면서 원하지 않는 것에 가입하도록 유도하고, 작은 배송비 또는 수수료를 지불하도록 합니다. 이들은 대부분 사기이며, 수수료를 받은 후 약속된 제품 또는 서비스를 제공하지 않습니다. **팁: 모든 조건 또는 상품들의 정보를 서면으로 받아 어떤 것에 서명하거나 동의하기 전 다시 확인을 할 수 있도록 하고, 믿을 수 있는 다른 사람의 의견을 물어보세요.**

2. "고맙지만 사양합니다", "지금은 괜찮습니다" 또는 "조금 생각해보겠습니다" 라고 응답하세요. 합법적인 회사와 기관이라면, 정보를 서면으로 요청하거나, 생각할 시간을 요구하는 것을 이해할 것입니다. **팁: 무언가에 즉시 서명하거나 돈을 지불하라는 압력을 받고있다면, 전화를 끊거나 대화를 멈추세요.**

3. 원하지않는 전화 또는 이메일로 은행, 크레딧카드 정보, 사회보장번호, 의료보험번호 등의 정보를 알려주지마세요. 다시 한번 강조하지만, 합법적인 회사는 여러분께서 하고자하는 확인절차에 협조를 할 것입니다. **팁. 중요한 개인 정보는 이미 잘 알고 있고 신뢰할수 있는 기관에만 제공하세요.**

4. 과도히 친절하거나 정상적으로 보이는 전화를 주의하세요: 사기꾼들은 친절해보이거나, 공식적으로 보이게 행동하여 쉽게 믿음을 산 후 돈거래나 개인정보제공을 유도합니다. 은행, 경찰, 정부 공무원들은 절대로 전화나 집에 찾아와 돈을 지불하도록 요구하지 않습니다. 만약 누군가가 여러분께서 지불해야할 돈이 있다고 말한다면, 직접 확인한 후 연락하겠다고 말하세요. **팁: 직접 해당 기관에 찾아가 지불을 하거나, 기관에 직접 연락하여 지불해야할 돈이 있는지 확인하세요.**

5. 집 수리 등 공식적 업무로 담당자가 집에 올 경우, 항상 사전에 통지를 할 것입니다. 낯선 사람이 찾아와 문을 열어달라고 한다면 항상 주의를 기울이세요. 찾아올 사람이 없다면 문을 열어줄 필요가 없습니다. 혼자있지 않은 시간에 다시 찾아오라고 해도 됩니다. 누군가 오기로 했다하더라도, 항상 신분증을 요구하십시오. 잠시 외부에서 기다리라고 한 다음, 회사에 연락해 직원을 파견했는지 확인을 하는 것도 좋습니다. 찾아온 사람이 경찰이라하더라도 마찬가지입니다. **팁: 모르는 사람을 집으로 들어오게 하지 마세요.**

6. 작게 쓰여진 설명을 꼼꼼히 읽으세요**.** 많은 사람들이 작게 쓰여진 이용약관을 읽지않아 문제가 발생하거나 원하지않는 상황에 빠지게 됩니다. 몇년 전 런던에서 행해진 실험으로, 공용 와이파이 접속을 하며 이용약관을 제대로 읽지않고 서명을 한 사람들의 예가 있습니다. 신문기사링크 **팁: 어떤 내용인지 제대로 이해하지 못했다면 절대로 서명하지마세요**.

7. 누군가 개인정보 또는 비용지불을 요구한다면, 어떤 내용에 서명을 하거나 지불을 하기전에 합법적인 회사/기관/사람인지 확인하세요**.** 정식으로 등록이 되어있는지, 자격증이 있는지 확인하세요. Better Business Bureau 에서 고객불만사항을 확인할 수 있습니다. 대부분의 합법적인 회사에 있는 웹사이트, 주소와 고객평점을 확인할 수 있지만, 이러한 정보 조차 위조될 수 있다는 점에 주의하세요. 의심이 들 경우, 주위에 물어보세요. 페이스북같은 소셜미디어를 사용하는 경우 친구와 가족에게 물어보세요. **팁: 돈이나 정보를 제공할 경우 신뢰할 수 있는 사람인지 확인하세요.**

8. 정보를 가진 후 구매하세요. 가격과 품질을 시간을 들여 비교하세요**.** 질문을 하고 영업사원이 알려주는 정보를 다시 확인하세요. **팁: 구매를 하기 전 스스로 정보를 찾아보세요. 본인이 필요하고 원하는 것을 구매하도록 하세요.**

9. 모르는 사람에게 송금하지 마세요. 계좌이체는 추적, 역추적 또는 반납이 거의 불가능합니다. 사기꾼이 추적을 피할 수 있는 가장 좋은 방법인 현금을 보내는 것 과 마찬가지입니다. 2014 년

사기를 당한 돈 중 30%는 은행의 계좌이체를 통해 송금되었습니다. 또 다른 30%의 피해는 선불기프트카드를 통한 사기였습니다**. 팁: 누군가 추적을 할수없고 환불을 받을수없는 방법으로 비용지불을 요구한다면, 주의하세요.**

10. 사기의 피해자가 되었다면 경찰에 신고하세요**.** 많은 사람들이 사기를 당했을 경우 속았다는 수치심에 경찰에 신고를 하지 않습니다. 그렇지만, 매우 능숙하고 지능적인 사기꾼들에 속은 것은 **여러분의 잘못이 아닙니다**. 피해신고를 할 경우, 손실된 자금을 되돌려받을 가능성이 작게나마있으며, 다른 사람의 피해를 막을 수 있게 될지 모릅니다. 또한 개인정보가 유출되었다고 생각되면 금융기관에 알려 취할수있는 보호조치를 확인하세요.

사기의 피해자가 되었을때 신고 방법

사기의 피해자가 된 것이 부끄럽다고 여겨지거나, 손해본 액수가 적은 경우에도 모든 사기 행각은 꼭 신고가 되어야합니다. 손해본 돈을 돌려받지 못할 수 도 있지만, 다른 사람이 같은 사기의 피해자가 되는 것을 막을 수 있습니다. 모든 사기는 아래의 기관에 신고할 수 있습니다:

1. 거주 지역 관할 경찰: 버나비 RCMP **Non-emergency (24-hour)** Tel: 604-646-9999 and website: **http://burnaby.rcmp-grc.gc.ca**
2. Canadian Anti-Fraud Centre **Toll Free within Canada: 1-888-495-8501 or visit website: https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/report-fraud.html**
3. **Financial Consumer Agency of Canada (FCAC):** 은행 및 금융기관 관련 권리 정보 제공. Tel: 1-866-461-3222 (TTY 613-947-7771, or 1-866-914-6097), Website: **fcac.gc.ca**
4. 더 많은 정보 **Canada.ca/Seniors** 또는 가까운 서비스 캐나다 사무실 방문

사기범죄를 신고하는 순서:

1: 사기에 관련된 모든 정보 수집. 관련 서류, 영수증, 이메일 또는 문자메세지 사본
2: 지역경찰에 신고. 이를 통해 어떠한 사기범죄가 해당 지역에서 일어나는지 경찰이 알수있음. 모든 통화 및 파일 번호를 기록.
3: **Canadian Anti-Fraud Centre** 에 신고. Tel: 1-888-495-8501 (영어) 월-금 9:00 am - 4:45 pm
4: 송금을 받은 금융기관에 사건 신고(예: Western Union or MoneyGram, 은행, 신용조합, 크레딧카드회사, 인터넷 지불서비스 제공업체 등).
5: 사기범죄가 페이스북, 이베이, 키지지 등 웹사이트에서 일어났다면 해당 웹사이트 관리자에 보고. "report abuse" 또는 "report an ad."
6: 신원 도용 사기의 피해자는 모든 계좌에 피해사실을 알리고 (은행, 크레딧카드 등) 신용기관에 신고 Equifax (**https://www.consumer.equifax.ca/personal/**), TransUnion (**https://www.transunion.ca/**)

씨니어를 위한 18 가지 인터넷 안전수칙

(Source: http://www.vistaspringsliving.com/blog/18-internet-safety-tips-for-seniors)

일반적 안전과 보호:

1. 비밀번호가 고유하고 안전한지 확인하세요. 개인정보가 포함되지않은 강력한 비밀번호를 사용하세요. 많은 웹사이트에서 대문자, 소문자,숫자 및 기호를 포함한 비밀번호설정을 추천합니다. 둘 이상의 계정에 동일한 비밀번호를 사용하지 마세요.

2. 맬웨어 방지 소프트웨어 및 기타 보호 소프트웨어를 사용하세요. 컴퓨터에 신뢰할 수 있는 보호 프로그램이 설치되어 있는지 확인하고, 최신 위험으로부터 보호되도록 자동 업데이트설정을 하세요. 무엇을 설치해야할지 잘 모르겠다면 전문가에게 문의하세요.

3. 알수없는 첨부파일이나 소프트웨어를 다운로드하지 마세요. 신뢰할 수 없는 출처의 첨부파일이나 이미지 또는 소프트웨어를 다운로드 하지마세요. 사기꾼들은 종종 바이러스 및 각종 맬웨어를 무료 소프트웨어나 흥미로운 내용으로 위장하여 다운받도록 유도합니다.

4. 신뢰할 수 있는 가족이나 친구가 응급상황에 귀하의 계정에 들어갈수있는 권한을 부여하는 것을 고려해보세요. 위급상황에 신뢰할 수 있는 가족이나 친구가 온라인 이메일, 은행 또는 파일 저장 계좌에 들어가야하지만 이가 어렵거나 불가능할수있습니다. 미리 계획하고 변호사와 **상의하여 신뢰할 수 있는 사람에게 귀하의 계정에 들어갈 수 있는 권한을 부여하십시오**.

이메일과 소셜 미디어:

5. '**스팸'필터 기능 이해** 스팸은 원치 않는 이메일을 말합니다. 대부분 이메일회사는 이러한 스팸메일을 편지함에서 제거하는 스팸필터가 있습니다.

6. **소셜미디어 개인정보 설정 사용** 소셜미디어에 게시하는 내용을 잘 관리하고, 개인정보 설정을 사용하여 신뢰하는 사람들에게만 게시물접근을 제한하세요.

7. **남용 사례 신고** 사이버폭력은 어린이와 청소년과 관련이 있을 수 있지만, 성인이라고 해서 안전하지는 않습니다. 사이버폭력이 일어났다면 응답하지말고, 도움을 줄 수있는 사람들에게 신고를 하세요. 사이버폭력의 피해자가 된것은 귀하의 잘못이 아님을 기억하세요.

8. **사기범죄의 특징** 조건이 너무 좋을 경우, 비현실적으로 낮은 가격의 상품, 의약품, 무료 여행 티켓 등의 제공은 일반적으로 사기일 경우가 많습니다. 또한 사기꾼들이 지인의 계정을

이용하여 돈을 요청할수도 있습니다. 이럴 경우, 다른 방법으로 상대방과 먼저 확인을 하기전에 답을 하지 마세요.

돈 과 구매:

9. 안전한 웹사이트. 결제정보를 웹사이트에 입력하라는 메세지가 표시되면, 먼저 웹사이트가 안전한지 확인하세요. 인터넷 브라우저 상단의 URL 표시줄에서 "https://" 를 확인하세요. ("S"는 보안을 나타냅니다)

10. 피싱 시도를 알고 피하세요. 구매 또는 결제정보입력을 요청하는 사이트로 연결되는 링크에 주의하세요. 온라인사기의 유형인 '피싱'은 가짜 사이트를 합법적인 사이트처럼 보이게 한 다음, 개인정보유출을 유도합니다. 문법 오류, 철자 오류, 익숙하지않은 URL 주소 등에 주의하세요. 의심이 될 경우, 링크를 사용하는 대신, 직접 정확한 웹사이트 주소를 URL 표시줄에 입력하세요.

11. 알지못하는 사이트에 개인정보나 결제정보를 입력하지마세요. 비슷하게, 개인정보나 결제정보를 입력하기 전, 합법적 웹사이트인지 확인하세요. 온라인 소매업체에 대한 이용후기를 확인하고, 은행이나 정부 사이트의 경우, 정보요청에 응답하지 마세요. 은행 및 정부기관은 비밀번호, 사회보장번호, 결제정보 등을 절대 요구하지 않습니다.

12. 은행계좌정보를 확인하세요. 모든 예방조치를 취하고 있다 하더라도, 결제정보가 유출되거나 신뢰할수있는 업체로부터 도난당할 수 있습니다. 은행계좌와 크레딧 카드의 결제정보를 확인하세요.

인터넷 상에서 사람만나기:

13. 불행히도 인터넷에서는 많은 사람들이 본인의 신원을 속이는 일이 일어납니다. 온라인 데이트 사이트나 취미동호회 등 새로운 사람을 만날 수 있는 기회가 많이 있지만, 많은 사람들이 거짓 신분을 사용할 수 있습니다. 온라인상에서 새로운 사람을 만날때 늘 주의를 하시고, 너무 많은 개인적인 정보를 나누지 마세요.

14. 인터넷 상에서 알게 된 사람에게 돈을 보내지 마세요. 개인적 정보와 마찬가지로, 돈을 목적으로 접근을 하여 친분을 쌓은 후, 돈을 부탁하고 돈을 받은 후 연락을 끊어버리는 사기범죄가 일어날 수 있습니다. 온라인으로 알게 된 사람이 슬픈 개인사나 곤경에 처한 상황을 빌미로 돈을 요구한다면 주의를 하세요.

15. 온라인에서 알게 될 사람을 실제로 만나려 한다면, 사람들이 많은 공공장소를 선택하고, 가족이나 친구에게 가는 장소와 만나는 사람에 대한 정보를 미리 알려주세요. 그 사람을 잘 알고 있다고 느낀다고 하더라도, 안전을 장담할 수 없습니다.

건강과 안전:

16. 사실과 가짜를 구분하세요. 건강에 대한 조언이나 정보 등을 소개하는 웹사이트는 방문자들이 광고를 클릭하게 하여 돈을 벌고, 자극적인 제목의 기사를 사용하여 웹사이트의 방문횟수를 늘립니다. 권위있는 자료처럼 보인다 할지라도 온라인에서 접하는 모든 정보가 사실이 아니라는 것에 주의하세요.

17. 온라인 정보에 의지하여 스스로의 건강상태를 판단하지마세요. 온라인 검색을 통해 증상을 찾아보고 질병 목록이나 진단에 관한 정보를 찾는 것은 매우 쉽습니다. 그렇지만 여러분의 건강상태를 이해하는 면허가 있는 의료전문가만이 진단을 내리고 치료를 처방해줄 수 있습니다. 인터넷정보를 따라 자가 진단 및 치료를 시도한다면 상태가 치료되지 않거나 악화될 수 있음을 기억하세요.

18. 전문가와 상담하세요. 물론 인터넷에서 접하는 모든 건강 정보가 생사와 관련한 심각한 것은 아닙니다. 온라인으로 영양에 관한 조언, 운동 및 건강한 삶에 도움이 되는 많은 정보를 접할 수 있지만, 인터넷 정보를 바탕으로 여러분의 식사습관이나 운동 계획 같이 여러분의 건강에 영향을 줄 수 있는 생활패턴에 변화를 주려고 한다면, 의사, 간호사, 영양사 등의 전문가와 상담을 하는 것을 추천합니다.

정보를 찾아 배움으로써 여러분의 안전을 유지할 수 있습니다. 더 많은 정보를 아래의 링크에서 찾아보세요.:

RCMP 노인관련 안전 정보- http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7

온라인쇼핑: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx
온라인 안전 기본 팁: https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice
온라인 쇼핑, 뱅킹, 기부하기- https://www.connectsafely.org/seniors/

이메일, 컴퓨터, 모바일 보호를 위한 10 가지 팁: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/