فهرست مطالب

تقدیر و سپاسگزاری

گروه کاری ارتباطات بین الفرهنگی

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

مترجمین:

عربی: Abeer Hattab
چینائی: Derek Chen
Tom Su
فارسی: Zarif Akbarian
Sossan Kayoumi
Nabila Akbari
کوریائی: Darae Lee
اسپانیائی: Mary Blanca Battenberg
Pilar Sain
تیگرینیا: Tigist Dubus Tesfamariam
Daniel Debesay Michael
Tedros Gebrengus
Enbakom Berhane
Asmait Tekle

نکات ایمنی درباره انترنت برای والدین

صحبت دربارهٔ ایمنی انترنت : خطرات زیادی در انترنت وجود دارد از نگرانی های حریم خصوصی تا سرقت هویت. کودکان و نوجوانان در هر سنی که باشند چه 5 یا 15 ساله, هنگام استفاده از انترنت باید نظارت شوند و بزرگسالان نیز باید مراقب باشند. توجه به مراقبت های ایمنی، مانند به اشتراک گذاشتن مکان، عکس و اطلاعات شخصی، برای محافظت عزیزان شما مسیرطولانی را طی خواهد نمود.

- چگونه تکالیف خانگی و مدت زمان انلاین را تنظیم نمایید: https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- 10 نکتهٔ ایمنی انترنتی و توصیه های استفاده از تکنالوژی برای والدین: https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- مشوره های ایمنی انترنت: توصیه های برتر برای والدین: https://www.webwise.ie/parents/advice-top-10-tips-for-parents/

استفادهٔ زودهنگام/استفاده از انترنت بدون نظارت - در یک نظرسنجی توسط Shared Hope International , یکی از هر هشت والدین به فرزندانشان اجازه می دهند که از سن دو سالگی از انترنت استفاده کنند و تنها یکی از هر ده والدین به فرزندانشان اجازه میدهند که از سن 10 سالگی از انترنت استفاده کنند (همانطور که توسط کارشناسان توصیه می شود). در نتیجه، بسیاری از کودکان در سنین پایین بدون نظارت، از انترنت استفاده می کنند. در اینجا بیان شده که چگونه از فرزندانتان وقتی که انلاین هستند محافظت نمایید:

- 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

از فعالیتهای آنلاین فرزندان خود نظارت نمائید - متأسفانه ، صرف نظر از مداخلهٔ والدین، بسیاری از نوجوانان تاریخچهٔ جستجوی انترنت خود را از والدین مخفی یا حذف می کنند .ضروری است که والدین کوشا و هشیار باشند. نوجوانان همچنین دارای ایمیل یا حساب رسانه های اجتماعی هستند که والدین آنها شاید از آنها بی اطلاع باشند .در بعضی موارد ، کودکان برای ایجاد این حساب ها, درمورد سن خود دروغ می گویند.

- https://protectkidsonline.ca/app/en/info_monitoring_online_activities
- برای حمایت والدین درمواردی که کودکان قربانی رفقای همسال خود شده اند، والدین میتوانند به منبع "هرم پشتیبانی" مراجعه نمایند از طریق: https://witsprogram.ca/pdfs/families/pyramid-of-support.pdf

تلفنهای همراه - تلفنهای همراه برای تماس ودر مواقع اضطراری عالی هستند. تقریبا 69 درصد از افراد 11 تا 14 ساله تلفن همراه شخصی دارند. کاربران یا استفاده کنندگان تلفن همراه باید متوجه باشند که GPS تلفن همراه, مکان فیزیکی دقیق کاربر را نشان میدهد. همچنین همیشه در مورد ارسال شماره تلفن های شخصی به صورت آنلاین محتاط باشید.

- زمانی که به فرزند خود یک تلفن همراه میدهید: https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- توصیه های ایمنی تلفن همراه: https://protectkidsonline.ca/app/en/info_phone_safety
- اولین تلفن همراه: قوانین و مسئولیت ها: https://www.ahaparenting.com/Ages-stages/tweens/Cell-Phone-Rules-Safe-Responsible-Kids
- برنامه مراقبتی مخصوص والدین برای ردیابی تلفن های همراه در سرتاسر کانادا و فراتر از مرزها: https://pumpic.com/parental-monitoring-app-canada.html

آزار و اذیت های انلاینی – چندین برنامه مکالمه بصورت مستعار یا ناشناس و سایت انترنتی وجود دارند که امکان ارسال معلومات سایرین بصورت ناشناس وجود میداشته میباشد. این برنامه های مستعار, که شامل Whisper, Yik

Yak, Ask.FM, میباشند خیلی خطرناک بوده, زیرا اینها بخاطر ترویج آزار و اذیت, شناخته شده میباشند. زورگویان با مخفی کردن هویت های ناشناس خود, به آسانی سایرین را طعمه کرده و باعث آزار و اذیت وپایین زدن دیگران میشوند. خیلی مهم است که همیشه مراقب بوده و هر گونه سوء استفاده, چه مشکوک و چه اثبات شده را گزارش دهیم.

- PREVNet: ارتقاء و ترویج روابط و رفع خشونت شبکه ای یا Violence Network از صلاحیت ها ی دولت کانادا بوده که توسط تحقیقات, و منابع جهت پیشگیری از آزار و اذیت تطبیق میگردد
- اگر فرزند شما مورد آزار و اذیت انترنتی قرار گرفته است چه باید کرد؟ https://needhelpnow.ca/app/en/resources_cyberbullying
- WISTProgram: پروگرام WIST مدارس, خانواده ها و جوامع را جهت ایجاد یک فضای پشتیبان یکجا نموده که بتوانند بچه هائی را که مورد آزار و اذیت انترنتی و یا قربانی همسالان خود قرار گرفته اند را کمک نمایند.
- مرکز پیشگیری از جرائم جوانان RCMP: این مرکز به کانادائی ها معلومات پیشگیری از جرائم, متناسب با سن و سال و همچنین وسایل جهت پیشگیری ازجرائم و قربانی شدن جوانان را فراهم میسازد
- شماره تماس کمک به بچه ها, یک مرجع خوب برای والدین و فرزندانشان میباشد. دسترسی به مشاوره را فراهم میسازد. آیا هم اکنون به کمک نیاز دارید؟ CONNECT را به شماره 686868 پیام دهید تا با یک داوطلب رسیدهگی به بحران 24/7 در تماس شوید. https://kidshelpphone.ca/search/?keys=Cyberbullying

عکس های برهنه – تحقیقات نشان داده اند که از هر هفت نوجوان یک نفر تصویر برهنه و یا نمیه برهنه از خودشان میگیرند, و بیشتر از نصف این تصاویر با یک شخص دیگر از طریق انترنت شریک شده است. این خیلی مهم است که بدانیم وقتی که معلومات در انترنت ارسال شد, دیگر هیچ راهی برای حذف کامل وجود ندارد.

- Cybertip.ca: خط راهنمائی کانادا برای گزارش دهی آزار و اذیت جنس آنلاین کودکان
  - 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

خریداری انلاین, سرقت هویت, جستجوی انترنت – خیلی مهم است که هنگام جستجوی انترنت مراقب باشید. تاریختچه فعالیت و جستجوی انترنت شما بصورت متداوم ردیابی میگردد. بازدید از سایت های انترنتی نا امن و نامناسب ممکن است که باعث لورفتن معلومات شخصی و مالی شما شده و یا به کامپیوتر شما صدمه برساند. داشتن امنیت مناسب و نصب نرم افزارهای ضد ویروسی در کامپیوتر خیلی مهم میباشد. جهت خریداری انترنتی باید همیشه ازیک ارتباط یا Connection مطمئن استفاده گردد, هیچ وقت از یک کامپیوتر عمومی جهت خریداری انلاین استفاده نکنید, و پیش ازاینکه وجه را پرداخت کنید, مطمئن شوید که سایت انترنتی مورد نظر قانونی و امن میباشد. پیگیری این احتیاطات به کاربران, تجربهٔ ایمن تری را ارائهٔ خواهد نمود. بچه ها اغلبا قربانی سرقت هویت میشوند. در حقیقت, به مقایسهٔ بزرگسالان, بچه ها ی زیرسن 18 سال, 51 مراتبه بیشتر احتمال دارد که هویت شان به سرقت برود. مجرمین بچه ها را هدف قرار میدهند چون بچه ها سوابق اعتبار پاک میداشته باشند, همانطور که قبلا گزارش داده شد, بچه ها غالباً بیشتر معلومات شخصی خود را از طریق انلاین ارسال میکنند.

- چگونه وضعیت اعتبار بچه ها را بدانیم, طرزالعمل مرحله به مرحله برای چک کردن گزارش اعتبار بچه ها: https://www.creditcards.com/credit-card-news/instructions-how-to-check-child-credit-report.php

بازیهای ویدوئی – بازیهای ویدوئی در سالاهای اخیر پیشرفت زیادی داشته اند. با موجودیت بازیهای متنوع زیاد, والدین باید از این موضوع که بسیاری از دستگاهای بازی, بچه ها را مستقیما به انترنت و سایر بازیکنان وصل میکنند, آگاه باشند. خوشبختانه بسیاری از دستگاهای بازی, امکان تنظیمات ایمنی و کنترول توسط والدین را میداشته باشند. والدین باید مدت زمان بازی های ویدوئی را برای فرزندان شان محدود نمایند.

- بازی های آموزشی آنلاین توصیه شده برای بچه ها ونوجوانان مقاطع چهارم تا هشتم مدارس در مورد اینکه چگونه بچه ها بتوانند در هنگام استفاده از انترنت ایمن باشند: http://mediasmarts.ca/digital-media-literacy/educational-games

در مورد ایمنی انترنت با فرزندان خود صحبت کنید

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

1. اطلاعات شخصی خود را خصوصی نگه دارید – نام, شماره تلفن، مدرسه یا آدرس خود را بدون اجازۀ والدین / سرپرست به کسی ندهید.

2. بیشتر سایت های شبکه های اجتماعی مانند فیس بوک و توییتر به شما این امکان را می دهند تا بتوانید کسانی را که مطالب شما را مشاهده کنند, انتخاب نمائید. از یک بزرگسال بخواهید تا در تغییر تنظیمات حریم خصوصی تان به شما کمک نماید.

3. بخاطر داشته باشید که هر چیزی که در رسانه های اجتماعی به اشتراک بگذارید - حتی به صورت خصوصی - توسط اشخاص دیگر قابل مشاهده است. همیشه قبل از کلیک بر روی "مطلب "یا" ارسال" دو بار فکر کنید!

4. در صورت مشاهدۀ هر مطلب یا چیز نامناسب به صورت آنلاین، از والدین یا یک شخص بزرگسال مورد اعتماد مشوره بگیرید. به یاد داشته باشید، تقصیر شما نیست که آن را دیده اید!

5. اگر کسی مطلب یا چیز زشتی را از طریق ایمیل یا رسانه های اجتماعی به شما ارسال میکند ، پاسخ ندهید - در عوض ، با یک یکی از مسئولین و یا یک بزرگسال مورد اعتماد صحبت کنید.

6. اگر میخواهید عکس یا فیلم هایی که اشخاص دیگری در آنها وجود دارند را به اشتراک بگذارید، همیشه ابتدا از آنها اجازه بخواهید.

7. هرگز بدون اجازه والدین / یا سرپرست چیزی را به صورت آنلاین خریداری و یا دانلود نکنید.

8. هیچ وقت با ملاقات حضوری با شخصی که شما او را فقط از طریق آنلاین می شناسید موافقت نکنید. به یاد داشته باشید که ممکن است اشخاص, آن کسی که میگویند نباشند!

9. رمزهای عبور یا پسوردهای خود را مخفی نگه دارید! حتی بهترین دوستان شما هم لازم نیست پسوردهای شما را بدانند!

10. در برابر آزار و اذیت بایستید - کسی را تحقیر نکنید و غیبت دیگران را نکنید! اگر اطلاعات بیشتر در مورد آزار و اذیت انترنتی یا آزار و اذیت در کل لازم دارید، به این سایت انترنتی مراجعه کنید:http://www.family.ca/standup/

صفحه راهنمایی برای بزرگسالان: کلاهبرداری، فریب و امنیت انترنتی

تماس هاس فریبکارانه:

از تماس گیرندگانی که به دروغ ادعا می کنند نماینده یک شرکت یا سازمان قابل اعتماد هستند، باخبر باشید. **https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdlnt-clls-en.aspx**

اگر شما چنین تماسی را گرفتید, چه باید بکنید؟
اگر چنین تماسی دریافت کردید، تماس را فورا قطع کنید. هرگز اجازه دسترسی از راه دور به کامپیوتر خود را به در خواست اشخاصی که غیر منتظره به شما تماس گرفته اند ندهید. اگر مطمئن نیستید، با مرکز خدمات مشتریان شرکت یا سازمان تماس بگیرید. کانادایی ها را قویاً تشویق مینمائیم تا چنین موارد فریت را به مرکز مبارزه با تقلب کانادا از طریق : http://www.antifraudcentre-centreantifraude.ca یا از طریق تماس به شماره تلفن 1-888-495-8501 گزارش دهند.

فریب و کلاهبرداری انلاین:

تعیین اینکه یک ایمیل، یک رقابت یا مسابقه, ویا یک امتیاز واقعی است یا یک کلاهبرداری و فریب انترنتی است، همیشه آسان نیست. ممکن است این پیشنهادها برای واقعی بودن خیلی خوب به نظر برسند – و ممکن است چنین باشند. نکته کلیدی برای ایمن ماندن, شناخت علائم هنرمندان کلاهبرداری است.
https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx

کجا میتوان معلومات بیشتر بدست اورد؟
منابع آنلاین بسیار خوب درباره اطلاعات مربوط به فریب و تقلب و کلاهبرداری وجود دارد. سایت انترنتی آژانس مشتریان مالی کانادا، اطلاعات در مورد حقوق شما در معاملات با بانک ها و سایر موسسات مالی را ارائه می دهد.
برای سفارش نسخه های اضافی از این نشریه، یا برای یافتن شماره تلفن در استان و منطقهٔ خود، با شماره 1 800 O-Canada (1-800-622-6232), TTY: 1-800-926-9105. تماس بگیرید.

اگر فکر میکنید مورد کلاهبرداری قرار گرفته اید, چی باید کرد؟

یکی از رایج ترین کلاهبرداری ها در کانادا ، کلاهبرداری phishing یا Smishing است که در آن کلاهبردار, خود را به عنوان یک سازمان تجاری یا دولتی مطرح می نماید. به عنوان مثال کلاهبرداری را که ادعا می کند از آژانس درآمد کانادا یا Canada Revenue Agency است، در نظربگیرید. بعضی اوقات به قربانی مورد نظر گفته می شود که مقدار زیادی بدهی دارد، و اگر پرداخت نکند، پلیس یا RCMP آنها را دستگیر خواهد کرد. گاهی اوقات به قربانی مورد نظر گفته می شود که "برای قبول بازپرداخت بر روی یک لینک کلیک کند ." برای بعضی به سادگی گفته میشود که برای مرور تغییرات در اطلاعات شان یک لینک را دنبال کنند, یا یک فرم اطلاعات شخصی خود را پر نمایند.
اگر فکر میکنید مورد کلاهبرداری قرار گرفته اید, چی باید کرد؟

اگر مطمئن نیستید که پیام قانونی و مطمئن است، پاسخ ندهید! به سایت انترنتی سازمان مراجعه کنید و مستقیما به آنها تماس بگیرید تا از موثق بودن اطلاعات که دریافت نموده اید مطمئن شوید. از آنجا که بسیاری از ما پیام تقلبی سازمان درآمد کانادا یا CRA را که خواستار پرداخت مالیات شده اند، دریافت نموده ایم, CRA توصیه های زیر را ارائه می دهد:

- CRAهرگزاطلاعات شخصی را از طریق ایمیل یا پیام نمی خواهد
- CRAهمچنین هیچوقت پرداخت توسط بیت کوین یا کارتهای هدیه را درخواست نمیکند.

در صورت دریافت تماس، پیام نوشتاری, و یا ایمیل که اذعان دارد که شما به CRA بدهکار هستید یا قرار است که به شما بازپرداخت صورت گیرد و یا قرار است مزایائی را دریافت نمائید، برای مشخص نمودن وضعیت مالیات خود, وارد حساب شخصی خود (My Account) یا حساب تجاری خود (My Business Account) شده و یا اگر حساب به این حسابات ثبت نکرده اید, ثبت نام نمائید و یاهم به شماره تماس CRA برای پرسشهای مربوط به مالیات عواید فردی از طریق شمارۀ 1-800-959-8281 تماس بگیرید.

اگر قربانی کلاهبرداری شده اید، چندین مرحله وجود دارد که باید انجام دهید:

1. کلاهبرداری را به پلیس محلی خود گزارش دهید: Burnaby RCMP's Non-emergency (24-hour) Tel: 604-646-9999 و سایت انترنتی:http://Burnaby.rcmp-grc.gc.ca
2. اگر شماره بیمه اجتماعی یا شماره SIN شما به سرقت رفته است، به خدمات کانادا یا Service Canada مرا جعه یا از طریق شمارۀ 1-800-206-7218 تماس بگیرید.
3. کلاهبرداری را به مرکز مبارزه با کلاهبرداری کانادا گزارش دهید. از شما خواسته می شود که ازیک شریک برای ورود (بطور مثال بانک شما) و یا GCKey (همانطوری که شما برای دسترسی به حساب CRA خود انجام میدهید) استفاده کنید. این بخاطر تضمین امنیت شما هنگام گزارش کلاهبرداری میباشد. همچنین می توانید با شماره 1-888-495-8501با مرکز مبارزه با کلاهبرداری تماس بگیرید.

کلاهبرداران برای تظاهر از نمایندگی بانک های یا شرکت های کارت های اعتباری، از روشها و تاکتیک های مشابه استفاده می کنند. به عنوان مثال ، شما ممکن صورت حساب مالی خود را از بانکی که با آن سر و کار ندارید دریافت کنید تا آن را مرور نمائید. وقتی پیام از طرف بانک شما نباشد, تشخیص Physhing ویا Smishing خیلی ساده است. اما اگر نگران هستید که پیام ممکن ازبانک شما باشد ، به این پیام پاسخ ندهید - مستقیماً از طریق تلفن یا حضوری به بانک بروید یا به سایت بانکی آنلاین خود وارد شده و از برنامه های بانکی استفاده کنید (حتما از یک ارتباط امن انترنت استفاده نمائید) تا تشخیص کنید که پیام واقعی و درست است. و فرا موش نکنید که پیام Physhing و Smishing را به بانک خود گزارش دهید.

برای کسب اطلاعات بیشتر در مورد سایر حوادث انترنتی و گزارش دادن ، به مرکز امنیت انترنتی کانادا مراجعه کنید.

.ایمن بود در فضای انترنتی را در توییتر ، فیس بوک و اینستاگرام دنبال کنید
توصیه برای محافظت اطلاعات شخصی در دستگاههای هوشمند 5
:(تلفون ها، تبلیت ها و ساعت های هوشمند)

این نکات مربوط به هر دستگاهی است که به انترنت وصل میشود که ممکن است در خانه داشته باشید. در حالیکه دستگاههای قابل اتصال به انترنت (همچنین به عنوان "دستگاه های هوشمند" نیز شناخته می شوند) سرگرم کننده هستند و زندگی ما را آسان تر می سازند، اما همچنین برای هکرها فرصتی را مهیا میسازند تا به اطلاعات شخصی ما دسترسی پیدا کنند. با پیروی از این نکات برای محافظت از خود و خانواده خود اقدام کنید:

1- **ایمن ساختن شبکهٔ انترنت (Wi-Fi) خانه:**
دستگاه های هوشمند از انترنت برای ارسال و جمع آوری داده ها استفاده می کنند. اگر اتصال Wi-Fi منزل شما ایمن نیست ، داده های شما نیز ایمن نیست !هنگام استفاده از Wi-Fi، حداقل امنیتی که باید داشته باشید رمزگذاری بی سیم و حافظت توسط پسورد یا رمز عبور میباشد. تحت تنظیمات بی سیم خود ، اطمینان حاصل کنید که در روتر شما, رمزگذاری WPA2 فعال باشد. سپس شبکه بی سیم خود را با یک پسورد بی نظیر قفل کنید. یک پسورد قوی شامل حروف بزرگ ، حروف کوچک ، اعداد و علامات است. اگر یک کاربر پیشرفته هستید، برای اتصال دستگاه های هوشمند خود یک منطقه شبکه جداگانه در شبکه Wi-Fiخود ایجاد کنید. این جداسازی دستگاه "Device Isolation" نامیده می شود و به طور مشابه با شبکه های "مهمان "Wi-Fiعمل می کند. هنگام استفاده از دستگاه هوشمند خود در بیرون (On the Go) فقط به شبکه های قابل اعتماد و با پسورد وصل شوید و تنظیماتی را که به طور خودکار, شبکه های Wi-Fi را جستجو می کنند، غیر فعال کنید.

2- **موقعیت یابی جغرافیائی (Geolocation) را هنگامی که استفاده نمیکنید غیر فعال سازید:**
بسیاری از دستگاه های هوشمند برنامه هایی دارند که از مکان جغرافیایی برای ارائه خدمات، مانند پیگیری تناسب اندام یا نقشه ها استفاده می کنند. اگر برنامه ای بتواند موقعیت مکانی شما را ببیند، هکر هم می تواند این کار را بکند. در تنظیمات دستگاه ، مکان جغرافیایی (geolocation) را غیر فعال نمائید.

3- **قبل از نصب برنامه ها، پالیسی خصوصی و شرایط استفاده از نرم افزار را بفهمید:** همه برنامه ها دارای تنظیمات حریم خصوصی هستند که به کنترل افرادی که می توانند اطلاعات شما را ببینند و آنچه می بینند کمک می کنند. این تنظیمات حریم خصوصی را انتخاب کنید تا اطلاعات شخصی مانند نام کامل و اطلاعات تماس پنهان شوند. همچنین مراقب برنامه هایی باشید که اطلاعات غیر ضروری یا اطلاعات بیش از حد را درخواست می کنند. نگاهی به مجوزها بیندازید و فقط روی "اجازه "برای همه چیز کلیک نکنید.

4- **میکروفون و دوربین هارا زمانی که استفاده نمیکنید غیر فعال نمائید:**
بیشتر هدفون های بازی ، تلویزیون های هوشمند ، ساعت هوشمند و بلندگوهای هوشمند دارای میکروفون و /یا دوربین هستند. اگر ایمن نباشد ، دستگاه شما می تواند اطلاعاتی را که قصد آن را ندارید ، ارسال کند. هنگامی که از آن استفاده نمی کنید ، دوربین خود را خاموش کرده و میکروفون خود را بیصدا نمائید.

5- رمزهای کاربری (usernames) را ایجاد کنید که اطلاعات هویتی و مشخص کننده نداشته باشند:

اشتراک گذاری زیاد می تواند حریم خصوصی شما را در معرض خطر قرار دهد. هنگام تنظیم ورود به سیستم برای دستگاه خود(یا برای یک بازی یا برنامه) ، اطمینان حاصل کنید که نام کاربری شما حاوی اطلاعات شناسایی مانند نام ، سن ، مکان شما یا اطلاعات تماس نباشد.

6- دانای تلفن هوشمند یا Smartphone Savvy باشید:

تلفن های هوشمند می توانند مکان شما را ردیابی کرده و اطلاعات مربوط به شما ، و مخاطبین شما را فاش کنند. مراقب باشید که فقط برنامه های معتبر و قابل اطمینان را نصب و استفاده کنید و اطمینان حاصل کنید که توسط پسورد (یا اثر انگشت) از تلفن خود محافظت کنید. بدانید که چگونه از ابزارها برای یافتن و حذف کردن اطلاعات شخصی تلفنهای گم شدهٔ خود استفاده کنید. اطلاعات بیشتری را در **ConnectSafely.org/cellphone-safety-tips** پیدا خواهید کرد.

7- روتر انترنت خود را ایمن کنید:

احتمالاً یک وسیله کوچک در خانه شما وجود دارد ، به نام روتر یا مودم که شما را به انترنت متصل می کند. این دستگاه دارای پسورد و نام کاربری است و بعضی اوقات رمزهای پیش فرض خیلی ساده بوده که میتوان به آسانی حدس زد. راه اندازی مجدد یا Configure کردن روترها بسیار دشوار است ، بنابراین اگر در انجام آن شک دارید، برای مشاوره در مورد تغییر پسورد با یک متخصص یا ارائه دهنده خدمات انترنت خود تماس بگیرید.

دستگاه های خود را محافظت کنید:

مطمئن شوید که دستگاه ها توسط پسورد محافظت می شوند و در مورد کمپیوتر ها، اطمینان حاصل کنید که امنیت خوب میداشته باشند و نرم افزاری دفاعی (Firewall) در آنها نصب میباشند. اگر به کمک نیاز دارید، از دوستان یا اعضاء خانواده که در این زمینه اطلاعات میداشته باشند کمک بخواهید و یا با ارائه دهنده خدمات انترنت یا تلفن همراه خود در تماس شوید. ارائه دهندهٔ خدمات انترنتی SHAW و برخی دیگر از ارائه کننده گان خدمات انترنتی ممکن است نرم افزارهای ضد ویروسی رایگان ارائه کنند, و هم می توانید نرم افزارهای امنیتی را از یک شرکت معتبر مانند شرکت های ذکر شده در **ConnectSafely.org/securityvendors** خریداری و یا بصورت رایگان بدست آورید.

منابع توصیه شدهٔ دیگر , برای توصیه های بیشتر بازدید نمائید:

FightSpam.gc.ca: کمک برای کانادائی ها و شرکت های تجاری جهت جلوگیری از Spam و سایر تهدیدهای الکترونیکی

حریم خصوصی جوانان (Youth Privacy): اطلاعات و ابزار توسط دفتر کمیشنر حریم خصوصی برای کمک به جوانان تا از حریم خصوصی خود محافظت نمایند.

خریداری انلاین- چگونه خود را هنگام خریداری انلاین محافظت نمائید

پسورد قوی و بینظیربکار ببرید: یک باردیگر، پسورد های قوی بسیار حائز اهمیت میباشند, همانطوری که درایمیل و حساب های رسانه‌های اجتماعی اهمیت دارند. هرگز پسورد خود را با کسی شریک نکنید، مگر اینکه شخصی را که مورد اعتماد شما است, برای مدیریت حسابهای خود تعیین کرده باشید. اطمینان حاصل کنید که پسوردهای شما حداقل هشت حرف داشته باشند. از اعداد ، حروف بزرگ و کوچک و علایم را در ساختن پسورد استفاده کنید واز اسم ها یا کلمات دیکشنری یا فرهنگ لغت استفاده نکنید. در ConnectSafely.org/passwords، توصیه ها و اطلاعات درباره نحوه استفاده از multi-factor authentication و شناخت نشان انگشت یا Finger Print Recognition جهت امنیت پیشرفته پیدا خواهید کرد.

به لینک ها یا پیوندها (Links) کلیك نکنید: لینک ها ممکن در ایمیل, یا در رسانه های اجتماعی از طریق بانکها ، شرکتهای کارت های اعتباری، سازمانهای دولتی یا سایر سازمانها باشند, مگر اینکه صد درصد مطمئن هستید که آنها قانونی هستند. یک نوع کلاهبرداری یا Scam متداول وجود دارد که به نام فیشینگ یاد میشود که شخصی برای شما یک لینک را میفرستد که مانند یک سایت انترنتی قانونی بنظر میرسد، اما در واقع یک سایت جعلی برای کلاهبرداری بوده که توسط جنایتکاران ایجاد شده است تا پسورد شما یا سایر اطلاعات شخصی شما را سرقت کنند. حتی اگر نام شرکت جزئی از آدرس وب باشد، باز هم این می تواند کلاهبرداری باشد. امن ترین شرط برای شما این است که آدرس انترنتی را مانند آنچه معمولاً انجام می دهید تایپ کنید و در صورت شک ، با سازمان مورد نظر تماس بگیرید.

از پیشنهاداتی که بیش از اندازه خوب برای واقعی بودن به نظر میرسند آگاه باشید: مثلا به شما گفته می شود که در مسابقه ای که هرگز شرکت نکرده اید برنده شده اید. یا به شما پیشنهاد تعطیلات یا محصولات به قیمت بسیار ارزانتر از آنچه که توقع میرود پرداخت نمایئد میگردد. بویژه در مورد پیشنهادات تداوی ها ویا خدمات بیمه های پزشکی کم هزینه مراقب باشید.

فقط از شرکت های بازرگانی معتبرآنلاین خرید کنید: در مورد بازرگانان یا شرکت های تجاری آنلاین که هرگز در مورد آنها نشنیده اید، مراقب باشید. بسیاری از شرکتهای انلاین قانونی هستند اما برخی هم برای سرقت شمارهٔ کارت اعتباری یا سایر اطلاعات مالی شما فعالیت میکنند، و یا به ساده گی از تحویل آنچه که شما برای آن پرداخت نموده اید ناتوان هستند. اگر مشکوک هستید، از کسی که با خریداری آنلاین آشنا است بپرسید یا در مورد آن بصورت انلاین تحقیق کنید و ببینید که در مورد شرکت و یا بازرگان انلاین نظر و مرور مشتریان وجود دارد یا خیر.

هنگام خریداری آنلاین و انجام کارهای بانکی از سایت های انترنتی امن استفاده کنید: با یک https در نوار آدرس جستجوگر انترنت. "S" مخفف secure "امن" است. اگر فقط http باشد، آن یک سایت امن نیست. اگر با استفاده از یک برنامه یا نرم افزار تلفن همراه اقدام به خرید یا انجام کارهای بانکی می کنید، اطمینان حاصل کنید که آن برنامه یا نرم افزار توسط همان شرکت معرفی شده است. اگر مطمئن نیستید، مرورو یا نظر سایر استفاده کننده گان را جستجو کنید و یا از یک متخصص بپرسید.

در صورت امکان ازکریدت کارتها استفاده کنید: در غیر اینصورت از کارت‌های دبت یا خدمات پرداخت آنلاین امن مانند پی پال (Paypal) استفاده کنید. هرگز وجه نقد، چک های نقدی, و یا حواله های پستی ارسال نکنید. حتی ارسال چک شخصی نیز می تواند خطرناک باشد. بهترین راه برای خریداری آنلاین, استفاده از کارت های اعتباری یا Credit Cards میباشد, زیرا در صورت دعوا، موسسهٔ کارت اعتباری , پرداخت وجه را متوقف و یا هم پول شما را به شما برمیگرداند و در عین زمان ادعای شما را مورد بررسی قرار میدهد. کارتهای دبیت نیز دارای امنیت یا حمایت میباشند اما بعضی اوقات برای پس گرفتن پول خود باید انتظار بکشید. سرویس هایی مانند

Paypal، Android Pay و Apple Pay نیز دارای امنیت و حمایت میباشند اما کارت های اعتباری هنوز بهترین برای خریداری آنلاین هستند.
قبل از کلیک کردن، مراقب باشید: موارد خاصی وجود دارند که ممکن است نتوانید آنها را لغو کنید، مانند خرید یا فروش یک سهام اشتباه یا خرید یک پرواز یا اتاق هتل بدون بازپرداخت. قبل از تأیید آنها، همه معاملات را با دقت بررسی کنید. اگر اشتباه کردید ، سریعاً با شرکت تماس بگیرید تا ببینید که آیا امکان لغو آن وجود دارد یا خیر.
بسیاری از شرکت ها یا تجارت های آنلاین ویژگی لغو را دارند که به شما امکان می دهد که خرید خود را لغو نمائید، اما باید سریعا این کار را انجام دهید. وقتی که اجناس خریداری شده برای ارسال آماده شدند، برای لغو سفارش آن جنس, دیگر ممکن خیلی دیر باشد. شما اغلب می توانید خریدهای خود را مسترد کنید، اما احتمالاً مجبور خواهید بود تا مصرف پست جنس برگشتی را پرداخت کنید.
اطمینان حاصل کنید که شما پالیسی های مسترد کردن اجناس شرکت بازرگانی آنلانی را میدانید و از تمام هزینه ها بشمول ارسال, تهیه و مالیات با خبر هستید.
قبل از اهدا کردن به خیریه های انلاین کمی تحقیق نمائید: سایت های تمویل شدهٔ مردمی مانند Kickstarter ، Indiegogoو GoFundMe مکان های خوبی برای اولین حامیان یا خریداران محصولات جدید، اهدا به موضوعات با ارزش و موسسات بوده، و حتی کمک مالی برای افرادی که دلایل قانع کننده دارند را نیز برآورده میسازند, اما باید با احتیاط عمل کنید. تمام مطالب را با دقت مطالعه نمائید و در مورد شخص یا سازمانی که در عقب آن میباشد کمی تحقیق نمائید. اگر آنها به دنبال جمع آوری پول هستند ، سعی کنید دریابید که واقعیت داشته باشد، و اگر محصول جدید خیلی عالی را عرضه می کنند، مطمئن شوید که واقع بینانه است ولی اگر مشکوک هستید, از آن صرف نظر کنید.
محافظت از سرقت هویت: هرگز شماره بیمه های اجتماعی خود (SIN) را به صورت آنلاین وارد نکنید مگر اینکه بدانید در یک سایت قانونی قرار دارید که نیاز واقعی به آن اطلاعات وجود داشته باشد ، مانند درخواست برای یک حساب بانکی ، درخواست کارت اعتباری یا وام (از یک موسسه مالی قانونی)، ویا گرفتن گزارش اعتباری. مگر اینکه کاملا مطمئن هستید که سایت قانونی میباشد, در غیر آن, از ارسال تاریخ کامل تولد و محل تولد خود پرهیز کنید و در هنگام درخواست ارسال سایر اطلاعات شخصی مانند آدرس خانه نیز محتاط باشید. سایتهای قانونی مانند فیس بوک و موسسات مالی ممکن است ملزم به درخواست تاریخ تولد شما باشند. شمارهٔ کریدت کارت خود را فقط به اختیار شرکت های بازرگانی و تجاری قانونی انلاین قرار دهید. وقتی مشکوک هستید, کمی تحقیق کنید و ببینید سایر مردم دربارهٔ آنها چه می گویند.

حساب های مالی آنلاین خود را نظارت کنید: همیشه فعالیت های اخیر خود را مرور کنید تا مطمئن شوید که هیچ گونه هزینهٔ اضافی و یا غیر واقعی که از طرف شما انجام نشده است در حساب های بانکی, اعتباری، ویا دبت شما وجود نداشته باشد. حساب های سرمایه گذاری آنلاین خود را بررسی کنید تا مطمئن شوید که هیچ فعالیت غیرمجاز وجود نداشته باشد. اگر چیزی مشکوک پیدا کردید ، آن را فوراً به دیپارتمنت فریب و کلاهبرداری موسسه مالی و یا به شماره تلفن رایگان کارت های اعتباری یا دبت گزارش دهید. حتی اگر شما فعالیت بانکی آنلاین ندارید، باز هم ممکن قربانی فریبکاری و یا کلاهبرداری شوید. اگر موضوعی را متوجه شدید, فوراً به موسسه مالی اطلاع دهید. در بیشتر موارد شما در برابر فریبکاری و کلاهبرداری محافظت می شوید اما باید آن را گزارش دهید.
کلاهبرداری خیریه ها: بیشتر موسسات خیریه دارای سایت انترنتی هستند و گزینه برای اهدا آنلاین میداشته باشند. تا زمانی که در سایت مورد نظر قرار دارید و این همان موسسهٔ خیریه قانونی است که شما آن را پشتیبانی میکنید, مشکلی وجود ندارد. در صورت گرفتن ایمیلی که ظاهراً یک موسسه خیریه است که از شما درخواست اهداء کمک مالی از طریق آنلاین را دارد، بسیار مراقب باشید. اگر با سازمان مورد نظر آشنایی ندارید ، آن را در CharityNavigator.org بررسی کنید و اگر قصد اهداء آنلاین دارید ، مطمئن باشید که در سایت قانونی موسسهٔ خیریه بروید. برای ایمن بودن ، به جای کلیک روی لینک ، آدرس سایت انترنتی موسسهٔ خیریه مورد نظر را در جستجوگر انترنت تایپ کنید.

توصیه های ضروری برای خریداری انلاین

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

مواردی که سایت خرید و فروش انلاین قابل اعتماد نیست

- سایتهایی که خیلی ضعیت طراحی شده، غیر حرفه ای بوده, و دارای لینک های انترنتی شکسته باشند.
- یک آدرس یا شماره تلفن مشخص برای انجام معاملات وجود ندارد.
- پالیسی های فروش، مسترد کردن و حفظ حریم خصوصی بسیار به دشواری قابل پیدا بوده و یا واضح نمیباشند.
- دکمه برگشت به صفحهٔ قبلی غیرفعال است. به عبارت دیگر ، شما در یک صفحه گیر مانده و نمیتوانید به صفحهٔ قبلی برگردید.
- اطلاعات کارت اعتباری شما را در زمان غیر از زمان انجام خرید , از شما درخواست می شود.

چگونه می توانید هنگام خریداری آنلاین, از خود محافظت کنید

- در صورت امکان با کارت اعتباری پرداخت کنید. پول نقد ارسال نکنید.
- مراقب قیمت ها باشید تا واقعی بوده و دور از واقعیت نباشند. در اینصورت آنها احتمالاً برای فریب و کلاهبرداری هستند.
- برای خرید آنلاین از Wi-Fi عمومی استفاده نکنید.
- پالیسی محرمیت را بخوانید و از نحوهٔ استفاده از اطلاعات شما , آگاهی حاصل کنید.
- به ایمیل یا پیامی که در صفحهٔ کامپیوتر و یا تلفن هوشمند شما ظاهر شده و اطلاعات مالی را شما را درخواست می کند پاسخ ندهید. شرکت های مشروع این چنین اطلاعات را از این طریق جمع آوری نمیکنند.
- صورت حساب کارت اعتباری خود را مطالعه کنید و هزینه هایی که از طرف شما نبوده است را بررسی کنید.
- اطمینان حاصل کنید که سیستم دفاعی یا Firewall شما روشن است. به عنوان مثال ، Windows Firewall به طور پیش فرض درنسخه های جدید ویندوز روشن است، اما برای اینکه مطمئن شوید که خاموش نیست:
  - با کلیک بر روی دکمه Start و سپس Control Panel ، Windows Firewall را باز کنید
  - در جعبه جستجو" Firewall "را تایپ کنید و سپس روی Windows Firewall کلیک کنید
  - در قسمت سمت چپ ، روی گزینهٔ روشن و خاموش کردن Windows Firewall کلیک کنید

- اجازه ندهید که پسورد و اطلاعات شخصی مانند آدرس شما بصورت خود کار پرشود و هرگز به یک سایت اجازه ندهید که اطلاعات کارت اعتباری شما را ذخیره کند.

امنیت انترنتی سالمندان: 10 نکته جهت پیشگیری از فریب خوردن

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

یک روز درحالیکه در خانه از نوشیدن پیاله چای خود لذت می برید, تلفن زنگ می زند.
"سلام مادر بزرگ ، من نوۀ شما هستم که بشما تلفن میکنم. من در حال سفر بودم که کیف پول و پاسپورت خود را گم کردم. آیا می توانید کمی پول برای من بفرستید؟" صدا کمی گنگ است, نمیتوانید بفهمید که کدام نوه تماس گرفته است, و تردید دارید که در صورت پرسش مبادا ناراحت شود. هر مادربزرگ دلسوز دوست دارد نوۀ خود را برای نجات از مشکل کمک کند، بناءً از نوۀ خود می خواهید که پول را به کجا ارسال کنید. متأسفانه ، تماس گیرنده نوه شما نیست بلکه یک کلاهبردار فریبکار است که سالمندان را هدف قرار داده تا پول شان راسرقت کند. آنها از طبیعت دلسوز شما سوء استفاده میکنند.

این چنین تماسها همیشه برای سرقت پولی که مردم به سختی عاید کرده اند صورت میگیرد. تعداد تبادلات مالی کلاهبرداری به یک میزان اخطار دهنده در حال افزایش است. تعداد واقعی احتمالاً بسیار بیشتربوده, زیرا بسیاری از کسانی که فریب خورده اند, ان را گزارش نمی دهند.

نکات پیشگیرانه:

- پلیس ، قضات یا اشخاص حقوقی و دولتی هرگز از شما نمیخواهند که پول از طریق خدمات پولی تجاری ارسال نمائید
- هرگز اطلاعات شخصی خود را از طریق تلفن به شخص تماس گیرنده ندهید
- قبل از تصمیم گیری برای ارسال پول، محل زندگی عضو خانواده یا دوست مورد نظررا که قصد ارسال پول دارید با سایر بستگان تأیید کنید
- هرگز از طریق خدمات پولی wire به افرادی که شخصاً آنها را نمی شناسید پول ارسال نکنید. قبل از هرگونه اقدام خیرخواهانه و یا کمک به اشخاص, هویت شخص را تأیید کنید. هنگامی که شماره حوالۀ پولی به کسی داده شود, پول را میتوان از هر کجای دنیا بدست آورد.

10 نکته برای پیشگیری از فریب خوردن

1. مادرم همیشه میگفت: **اگر چیزی خیلی بیش از اندازه برای واقعی بودن خوب بنظر میرسد, احتمالا چنین است.** تصور کنید که آیا فریبکاران برای علایق ما همچو رفع سریع مشکلات, علاج معجزه آسای بماریها و بدست آوردن پول آسان, تپ و تلاش کنند. آنها با ارائه محصولات و خدمات رایگان ، قیمت های بسیار پائین که بمشکل متوان در برابر آنها مقاومت کرد و یا جوایز بزرگ ، مردم را برای ثبت نام برای چیزی که لازم ندارند, ترغیب به پرداخت هزینه حمل و نقل و یا هزینه تبادله پولی می کنند. اینها اغلب کلاهبردار هستند، جایی که "هزینه و یا فیس" از شما می گیرند ولی محصول ، خدمات یا جایزه ای را که قول داده اند را ارائه نمی کنند. **نکته: بخواهید که کلیه پیشنهادات یا جزئیات جایزه را به صورت کتبی برای شما ارسال کنند, که بتوانید قبل از انجام هرگونه تعهد ، امضا یا توافق برای هر کاری ، آن را بخوانید. یک نظر دومی را از شخص مورد اعتماد بخواهید.**
2. اشکالی ندارد که بگویید "نه ، متشکرم" "الان نه" یا "بگذارید در مورد آن فکر کنم." شرکت ها و سازمان های قانونی در صورتی که درخواست کتبی اطلاعات و یا خواهان زمان برای تحقیق را میفهمند. **نکته: اگر برای پرداخت چیزی ویا برای ثبت نام خدمتی, خود را تحت فشار احسساس میکنید, تلفن را گذاشته و از آن معامله بیرون شوید.**
3. اطلاعات کارت های اعتباری و یا بانکی خود, شماره تامین اجتماعی , بیمه یا شمارهای بهداشتی خود را به هیچ وجه از طریق تلفن و یا انترنت با یک تماس گیرندۀ غیر منتظره شریک نکنید. مجدداً, شرکت ها قانونی, تلاش شما را جهت واقعیت یابی درک میکنند. **نکته: اطلاعات شخصی و مالی را فقط با شرکتهای آشنایی که با آنها تماس گرفته اید و تحقیق کرده اید به اشتراک بگذارید.**

4. از تماس گیرنده گان حیله گر و ترفند بندی که رسمی بنظر میرسند آگاه باشید. کلاهبرداران خیلی زیرک هستند و میدانند که بسیاری از افراد متقاعد به ارسال پول و یا اطلاعات خواهند شد در صورتی که آنها رسمی و خیلی زیبا بنظر برسند. بانکها, افسران پلیس, و یا مقامات دولتی هیچ وقت از شما نمیخواهند که از طریق تلفن و یا دم در برایشان پول بپردازید. گر شخصی به شما گفت که بدهکار هستید ، به آنها بگویید که سوابق خود را بررسی کرده و مستقیماً با دفاتر یا موسسات آنها تماس خواهید گرفت. **نکته: برای پرداخت هزینه ها, حضوری به ساختمان های رسمی بروید یا برای تأیید پول بدهی خود با این سازمان تماس بگیرید.**

5. نمایندگان و یا تعمیر کننده گان همیشه قبل ازفرستادن شخص به خانهٔ شما با شما تماس گرفته اطلاع میدهند. در صورتیکه یک فرد ناشناس دم خانهٔ شما در زد, جانب احتیاط را مد نظر بگیرید. اگر شما کسی را منتظر نیستید, مجبور نیستید در را باز کنید. بخواهید که کمی دیرتر بیایند, و مطمئن شوید وقتی آنها میایند تنها نیستید. اگر کسی را منتظر هستید, باز هم از آنها بخواهید که مدرک شناسائی خود را نشان دهند. مشکلی نیست که از آنها بخواهید بیرون منتظر بمانند, تا موقعی که شما با شرکت که آنها را فرستاده است تماس بگیرید و تائید کنید که واقعا شرکت آنها را فرستاده است. این موضوع حتی در مورد پلیس نیزصدق میکند. **نکتیه: هیچ وقت افراد ناشناس و یا غیر منتظره را به خانه خود اجازه ندهید.**
6. **برای خواندن مطالب وقت بگذارید:** بسیاری از مردم شرایط و مواد درج شده را مطالعه نمیکنند و این ممکن شما را به یک مشکل جدی مواجه و یا شما را متعهد به چیزی که نمیخوهید نماید. چند سال قبل یک تحقیق آزمایشی در لندن انجام شد که مردم برای گرفتن Wi-Fi رایگان بدون مطالعه, با شرایط وضوابط موافقت کرند, حتی متوجه آنچه را که در حقیقت امضاء کرده بودند, نشده بودند. مقاله را میتوانید بخوانید. نکته: هیچ وقت چیزی را که کاملا نفهمده اید امضاء نکنید.
7. قانونی بودن و درستی هر موسسه, شرکت , یا رقابت و یا هر کسی که از شما اطلاعات یا پول درخواست میکند, یا قبل از ثبت نام و یا پرداخت هر هزینه , حتما بررسی کنید. اطمینان حاصل کنید که آنها ثبت و یا جواز فعالیت از مراجع منطقه ای میداشته باشند. شما میتوانید از طریق سازمان تجارت بهتر یا Better Business Bureau شکایات قبلی را بررسی نمائید. اکثر شرکت های قانونی سایت انترنتی, آدرس, و مطمئناً چند مروریا نظر مشتریان میداشته باشند, با آنهم متوجه باشید که حتی این معلومات هم ممکن غیر واقعی باشند. وقتی مشکوک هستید, از این طرف و آن طرف پرس و جوکنید. اگر شما در شبکه های اجتماعی مانند فیس بوک هستید, از دوستان و خانواده خود بپرسید که ایا شرکت مورد نظر را میشناسند . **نکته: مطئن شوید که اطلا عات و پول خود را به کسی که میشناسید میدهید و اینکه آنها قابل اعتماد باشند.**

8. **یک مصرف کننده مطلع و با خبر باشید:** برای مقاسیهٔ قیمت و کیفیت کمی وقت بگذارید و از این طرف و آن طرف معلومات بگیرید. سوالات زیادی بپرسید و معلوماتی را که فروشنده برای شما میگوید دوباره بررسی کنید. **نکته: پیش از خریداری تحقیق نمائید. مطئن شوید که چیزی را که لازم دارید و میخواهید میخرید.**
9. **هیچ وقت پول را از طریق Wire Transfer به کسی که نمیشناسید ارسال نکنید:** ردیابی, پیگیری و استرداد انتقال پول که از طریق Wire Transfer صورت گرفته باشد, تقریبا غیر ممکن است. این نوع انتقال پول مانند انتقال پول نقد بوده که یکی از بهترین راه ها برای فریبکاران جهت انجام فعالیت های کلاهبرداری شان میباشد. سی درصد از همهٔ پولی که در سال 2014 کلاهبرداری شده بود, از طریق Wire Transfer انتقال شده بود. سی درصد دیگر از طریق کارت های هدیه پیش پرداخت کلاهبرداری شده بودند. **نکته: اگر کسی از شما درخواست پرداخت از طریقی که قابل ردیابی و قابل استرداد نیست دارد, مشکوک شده و پرداخت نکنید.**
10. **اگر متوجه شدید که قربانی کلاهبرداری شده اید, به پلیس گزارش دهید:** اغلب موارد کلاهبرداری گزارش داده نمیشود بخاطریکه مردم از این که به دام افتاده اند خجالت میکشند و یا فکر میکنند که باید بهتر میدانستند. واقعیت این است که کلاهبرداران در انجام آنچه که انجام میدهند خیلی خوب هستند و اگر شما قربانی تکنیک های بشدت قانع کنندهٔ انها شده اید, شما کدام اشتباه مرتکب نشده اید. اگر گزارش دهید, چانس کمی وجود دارد که پول گم شدهٔ شما دوباره بدست آید و احتمالا شما اشخاص دیگر را از جنایت های مشابه حفظ مینمائید. همچنان اگر باور دارید که کسی به اطلاعات محرم و حساس شما دسترسی پیدا کرده است, موسسهٔ مالی خود را در جریان قرار دهید تا ببینید برای محافظت شما چه میتواند انجام شود.

اگر فکر می کنید که از شما کلاهبرداری شده است و یا قربانی فریب و تقلب شده اید چه باید بکنید؟

تمام کلاهبرداریها و فریب ها باید گزارش شوند, حتی اگر شما احساس خجالت میکنید و یا فکر میکنید که مقدار پول از دست رفته بسیار ناچیزبوده و نگران آن نیستید. هرچند ممکن شما قادر نباشید که پول خود را پس بگیرید, ولی شما میتوانید به توقف کلاهبرداری کمک کنید. تمام موارد فریب و کلاهبرادری را به مراجع زیر گزراش دهید:

1. پلیس محلی در جامعه شما: Burnaby RCMP's **Non-emergency (24-hour)** Tel: 604-646-9999 و سایت انترنتی: http://burnaby.rcmp-grc.gc.ca
2. مرکز ضد فریبکاری کانادائی **1-888-495-8501 بدون هزینه داخل کانادا** و یا به سایت انترنتی مراجعه کنید: https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/report-fraud.html
3. موسسهٔ مصرف کنندگان مالی کانادا (FCAC): اطلاعات راجع به حقوق شما در معاملات همراه بانکها و سایر موسسات مالی ارائه میکند. Tel: 1-866-461-3222 (TTY 613-947-7771, or 1-866-914-6097), Website: fcac.gc.ca
4. برای معلومات بیشتر به Canada.ca/Seniors و یا به نمایندگی خدمات کانادا Service Canada مراجعه نمائید.

مراحل گزارش دادن فریب و کلاهبرداری

مرحلهٔ اول: تمام معلومات مربوط فریب را جمع آوری کنید. این شامل اسناد, رسید های, کپی تمام ایمیل ها و پیامهای تلفنی میباشد.
مرحلهٔ دوم: واقعه را به پلیس محلی گزارش دهید. این باعث میشود که پلیس دریابد که کدام نوع کلاهبرداری, ساکنین و تجارت های منطقه را هدف قرار داده است. تمام تماسها, تمام پرونده ها یا شماره های وقوع را ثبت کنید.
مرحلهٔ سوم: مرکز مبارزه با فریب کانادا را تماس بگیرید, با تلفن به شماره Tel: 1-888-495-8501
ساعات کاری: دوشنبه تا جمعه ساعت 9:00 صبح تا 4:45 بعد ازظهر (به وقت شرقی)
مرحلهٔ چهارم: واقعه را به موسسهٔ مالی که پول به آن ارسال شده است گزارش دهید (بطور مثال خدمات پولی Western Union یا MoneyGram, بانک یا اتحادیه مالی اعتباری, موسسهٔ کارت اعتباری, یا فراهم کنندهٔ خدمات پرداخت انترنتی)
مرحلهٔ پنجم: اگر فریب آنلاین صورت گرفته است مانند فیس بوک, eBay, سایت های طبقه بندی شده مانند Kijiji یا یک سایت انترنتی دوست یابی, حتما واقعه را مستقیما به سایت انترنتی گزراش دهید. این جزئیات تحت "report abuse" یا "report an ad." یافت میشود.
مرحلهٔ ششم: قربانیان فریب و کلاهبرداری هویتی, باید که در تمام حسابهای خود اخطاریه گذاشته و باید به هر دو موسسهٔ اعتباری Equifax (https://www.consumer.equifax.ca/personal/) و TransUnion (https://www.transunion.ca/) گزارش داده شود.

نکته دربارهٔ امنیت انترنتی برای سالمندان 18

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

امنیت و محافظت عمومی:

1. مطئمن شوید که رمز عبور یا پسورد شما ایمن و بی نظیر است. رمز عبور یا پسورد قوی که هیچگونه اطلاعات شخصی را نداشته باشد استفاده کنید, و کوشش کنید که کلمات فرهنگ لغت و یا عبارات را استفاده نکنید. بسیاری از سایت های انترنتی ترکیبی از حروف بزرگ و کوچک , شماره ها, و علایم را توصیه میکنند. بعلاه یک پسورد را برای بیشتر از یک حساب استفاده نکنید.
2. از نرم افزارهای خنثی کنندهٔ نرم افزارهای مخرب یا malware و سایر ابزارهای محافظت کننده استفاده کنید. اطمینان حاصل کنید که در کامپیوتر شما نرم افزارهای معتبر نصب شده است, و آنها را طوری تنظیم کنید که بصورت خودکار بروز رسانی شوند که بتوانند شما را در مقابل آخرین خطرات حفاظت کنند. اگر مطمئن نیستید که چه نرم افزاری را نصب کنید، از یک فرد متخصص یا متخصص فناوری اطلاعات سؤال کنید.
3. **ضمیمه ها و نرم افزارهای ناشناخته را دانلود و نصب نکنید.** هرگز اسناد, عکس و یا نرم افزاری را که نمیشناسید و به منبع آنها اعتماد ندارید, دانلود نکنید. کلاهبرداران و هکرها, اغلباً ویروسها و سایر نرم افزارهای مخرب را به نرم افزار های "رایگان" و سایر محتویات جالب برای دانلود تبدیل میکنند.
4. **یک دوست و یا عضو خانوادهٔ خود را که مورد اعتماد شما هست اجازه دهید که به احسابهای شما دسترسی داشته باشد.** در مواقع اضطراری, برای دوستان و خانوادهٔ شما بسیار مشکل یا غیر ممکن خواهد بود تا به ایمیل انلان شما, حساب بانکی, و حسابهای فایل های ذخیره تان دسترسی پیدا کنند. قبلا برنامه ریزی کنید تا با یک وکیل کارنموده و کسی را که مورد اعتماد شما هست, صلاحیت دسترسی به حسابهای خود بدهید.

ایمیل و رسانه های اجتماعی:

5. **فیلترهای "اسپم " را بشناسید:**اسپم به ایمیل های نا خواسته و نامنتظره گفته میشود. اکثر ارائه دهندگان ایمیل فیلتراسپم دارند که این ایمیل ها را از صندوق ورودی یا inbox اصلی شما حذف میکنند.
6. **استفاده از تنظیمات حریم خصوصی در رسانه های اجتماعی.** از آنچه که در هر رسانهٔ اجتماعی به اشترک میگذارید یا پست میکنید باخبر باشید واز تنظیمات حریم خصوصی استفاده کنید و دسترسی به پست ها یا مطالب ارسالی تان را محدود به افرادی بسازید که به آنها برای دسترسی به معلومات شخصی اعتماد دارید.
7. **هرگونه مورد سوء استفاده را گزارش دهید.** هرچند آزار و اذیت انترنتی ممکن بیشتر ارتباط به اطفال و نوجوانان داشته باشد, ولی این بدان معنی نیست که بزرگسالان از طریق آنلاین مورد سوء استفاده قرار نمیگیرند. در این گونه مواقع هرگز پاسخ ندهید. در عوض سوء استفاده را گزارش دهید, به هر دو طریق: هم در گروهی که هستید و هم به کسانی که میتوانند به شما کمک کنند, و بخاطر داشته باشید که سوء استفاده تقصیر شما نیست.
8. **علایم کلاهبرداری را بشناسید.** اگر چیزی خیلی بیش از حد برای واقعی بودن درست بنظر میرسد, معلمولا این چنین نیست. پیشنهادات خیلی پائین قیمت, بلیط های رایگان چیز های بزرگ مانند تعطیلات, دستگاهای الکترونیکی, و دواها معمولا ترفند های کلاهبرداری میباشند. از سوی دیگر, بعضی وقتها کلاهبرداران برای شما ایمیل درخواست پول از حسابهای شخصی دوستان شما میفرستند. هیچوقت جواب ندهید و همچنان هیچ موقع بدون تصدیق درخواست با شخص از یک طریق دیگر, پول ارسال نکنید.

پول و خریداری:

9. **دنبال سایت های خریداری امن باشید.** هرموقع که از شما خواسته شد که اطلاعات پرداخت پول را در سایت انترنتی داخل کنید, اول معلومات بگیرید که سایت انترنتی امن باشد. در نوار URL در بالای جستجو گر انترنت خود دنبال "https://"برای سایت امن باشید, (s مخفف secure یا امن است).

10. **درک و پیشگیری از تلاشهای فیشینگ (Phishing)**. از لینک ها یا پیوستهایی که ارتباط به سایتهایی دارند که از شما میخواهند تا خریداری کنید و یا معلومات پرداخت پول را داخل کنید بر حذر باشید. یکی از کلاهبرداری های رایج انترنتی فیشینگ (Phishing) است که سایت ساختگی که مانند یک سایت قابل اعتماد به نظر میرسد، ولی اطلاعات شما را به کلاهبردار می دهد. به دنبال خطاهای دستوری ، اشتباهات املایی و URL هایی باشید که متفاوت از آنچه قبلاً استفاده می کردید, به نظر میرسند. اگر شک دارید ، آدرس سایت مورد نظر را که شما میدانید درست است مستقیماً در نوار URL تایپ کنید.
11. **هیچگاه معلومات شخصی و یا معلومات پرداخت پول را در سایتی که نمیشناسید داخل نکنید**. همچنین درصورتیکه می خواهید اطلاعات شخصی یا پرداخت پول را وارد کنید ، موثق بودن وب سایت مورد نظر را اول تأیید کنید. به دنبال نظرات و یا مرور های خریداران آنلان باشید. در مورد سایت های بانکی یا دولتی, هیچگاه به درخواست اطلاعات پاسخ ندهید. بانکها و موسسات دولتی هیچگاه پسورد یا کلمات عبور, شماره های تامین اجتماعی, و یا اطلاعات پرداخت پول را درخواست نمیکنند.
12. **حسابهای مالی خود را نظارت کنید.** حتی اگر شما تمام احتیاطات لازم را مد نظر بگیرید, این احتمال وجود دارد که ممکن است اطلاعات پرداخت پول شما از یک فروشنده معتبر لو رفته یا سرقت شود. حسابهای بانکی و کارتهای اعتباری خود را برای خریدهایی که شما انجام نداده اید بررسی کنید.

<u>ملاقات با افراد جدید:</u>

13. **همیشه محتاط باشید**. متاسفانه همهٔ افراد در انترنت, کسانی نیستند که میگویند هستند. فرصتهای بسیار زیادی برای ملاقات افراد جدید آنلاین وجود دارد, از سایتهای دوستیابی گرفته تا گروه های سرگرمی و انجمن ها, ولی همه افراد قابل اعتماد نیستند. هنگام ملاقات و محاوره با افراد جدید خیلی محتاط باشید و اطلاعات شخصی خود را خیلی زیاد شریک ننماید که بتوانند شما را پیدا کنند.
14. **برای آشنایان جدید پول ارسال نکنید**. همانند اطلاعات شخصی, بعضی از مردم, خویشاوندان خود در انترنت مورد سوء استفاده قرار میدهند(خود را معرفی نمیکنند), بعداً درخواست پول میکنند و دیگر هیچوقت شنیده نمیشوند. هیچوقت فریب داستانهای مصیبت بار یا درخواست پول برای بازدید را نخورید, مگراینکه در مورد نیت خوب افراد مثبت هستید.
15. **هنگام ملاقات حضوری, ایمن باشید**. اگر تصمیم دارید با کسی که از سایتهای دوست یابی, و یا یک دوستی را که آنلاین آشنا شده اید, ملاقات کنید, یک مکان عمومی را انتخاب کنید و به یک دوست یا یکی از اعضای خانواده خود بگویید که به کجا می روید و با چه کسی ملاقات می کنید. هیچ وقت شما خیلی امن نخواهید بود حتی اگرشما احساس میکنید که شخص را خیلی خوب میشناسید.

<u>تندرستی و سلامتی:</u>

16. **واقعیت را از تخیل درک کنید**. سایت های انترنتی مانند ناشران اخبار و وبلاگ های مشاوره بهداشت اغلب با جذب بازدید کنندگان برای مشاهده و کلیک روی تبلیغات در صفحات خود ، درآمد کسب می کنند. و برای بدست آوردن بازدیدهای بیشتر, سرفصل های میهج نشر میکنند. هرآنچه در یک سایت انترنتی نشرشود درست نیست, مهم نسیت چقدر رسمی بنظر میرسد.
17. **از تشخیص های خودسر و توصیه های بهداشتی خودسرانه خودداری کنید**. یافتن لست بیماریها از طریق داخل کردن علایم بیماری در جستجوگرهای انلاین و یا در از طریق انجمن هائی که تشخیص ها را بحث میکنند , بینهایت آسان میباشد. ولی فقط متخصص بهداشتی که جواز کار دارد و و سوابق بهداشتی شما را میداند, میتواند بیماری را تشخیص و تداوی تجویز کند. تلاش برای استفاده از انترنت جهت انجام این چنین کارها به معنی این است که وضعیت بدون تداوی مانده و و ممکن وخیم گردد.
18. **همراه یک متخصص پیگیری کنید**. هرچند هریک از توصیه های بهداشتی در انترنت زندگی و مرگ نیست. خیلی منابع مفید آنلاین برای توصیه های تغذیه, تندرستی, و تناسب اندام وجود دارند, ولی همیشه خوب است که با یک متخصص (دکتور, نرس یا پرستار بهداشت, کارشناس تغذیه) قبل ازانجام هر کاری مانند رژیم غذائی یا برنامه تمرینی که ممکن سلامت شما را متاثر سازد مشورت نمائید.

با آموزش خود میتوانید در امان باشید. در اینجا منابع دیگربرای بررسی وجود دارد:

کتابچهٔ راهنمای ایمنی و محافظت سالمندان RCMP - http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7

چگونه خود را هنگام خریداری آنلاین محافظت کنید - https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx

نکات و مشوره های اساسی آنلاین - https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice

خریداری آنلانی, بانک داری, خیریه و سفر- https://www.connectsafely.org/seniors/ -

10 نکته برتر برای محافظت از صندوق ورودی یا Inbox ، کامپیوتر و تلفن همراه تان - https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/ _