BritishRedCross

Home Office

پروژه توانمندسازی دیجیتال و برقراری ارتباط زنان پناهنده

راهنمای همراهی با کارگاه 3

این راهنما به عنوان یک ابزار حمایتی برای زنانی ایجاد شده است که در کارگاه‌های پروژه توانمندسازی دیجیتال و برقراری ارتباط زنان پناهنده شرکت می‌کنند. هدف این راهنما زنانی هستند که از پناهندگی، حمایت بشردوستانه یا ویزای گرد هم آیی مجدد خانواده پناهندگان برخوردار هستند و در انگلستان زندگی می‌کنند. بودجه این پروژه توسط دفتر حمایت از پناهندگان وزارت کشور و بودجه یکپارچه تامین می‌شود.

ما می‌خواهیم از اعضا و سفیران شبکه VOICE که به ایجاد این اسناد کمک کرده‌اند، تشکر و قدردانی کنیم. این مطالب به زبان انگلیسی، امهری، عربی، فارسی، کردی (سورانی)، سومالی، تیگرینیا و اردو در دسترس هستند. امید می‌رود که زنان پناهنده که قادر به شرکت در این کارگاه‌ها نیستند بتوانند از این اطلاعات در مسیر خود استفاده کنند.

محتوا

پیش گفتار

این ابزار قادر به کاوش و تشریح تمامی تهدیدها و معیارهای حفاظتی که در دسترس کاربران اینترنت است نمی‌باشد و تنها به عنوان یک مقدمه پایه در نظر گرفته می‌شود که امیدوار است توجه شما را به برخی از نکات مهم و جاهایی که می‌توانید اطلاعات بیشتر در این خصوص کسب کنید، جلب کند.

ما می‌دانیم که در گفتگو در مورد امنیت دیجیتال ما به مسادلی پیرامون خشونت مبتنی بر جنسیت، سو استفاده و جرایم کیفری که می‌توانند حساس و اغلب تابو باشند، می‌پردازیم. مأموریت بشردوستانه ما و اصل «عدم آسیب رسانی» ما به این معنی است که ما برای انجام آنچه در توان ماست برای مقابله با خشونت مبتنی بر جنسیت، از جمله ارائه اطلاعات برای حمایت از مردم برای انتخاب گزینه‌هایی که به آنها قدرت می‌بخشند و تصمیماتی که از آنها محافظت می‌کند، دعوت به عمل می‌شویم.

در سراسر این راهنما، لینک‌هایی وجود دارند که می‌توانید با کلیک بر روی آنها به وب سایت‌های مربوطه بروید. به عنوان مقال، اگر اینجا کلیک کنید، شما به وب سایت صلیب سرخ بریتانیا هدایت خواهید شد. در جایی که امکان داشت، ما سعی کرده‌ایم که لینک‌های مربوط به منابع ترجمه شده را قرار دهید، اما بسیاری از لینک‌های داخل این راهنما مربوط به اطلاعات انگلیسی هستند. هرچند که ما معایب و محدودیت‌های ترجمه خودکار را می‌دانیم، اما در خصوص نحوه استفاده از این قابلیت در راهنمای دو صحبت کرده‌ایم:

مشاوره جامع در خصوص امنیت دیجیتال شامل نحوه محافظت از وسایل و مراحل حفاظت از خود و دیگران از تهدیدهای آنلاین را می‌توانید در وب سایت www.getsafeonline.org.uk و مرکز ملی امنیت سایبری www.ncsc.gov.uk مشاهده کنید. اطلاعات و حمایت‌های بیشتر برای قربانیان سو استفاده آنلاین در وب سایت Stop Online Abuse (سو استفاده آنلاین را متوقف کنید) موجود است - www.stoponlineabuse.org.uk برای کسب اطلاعات و حمایت‌های بیشتر برای مقابله و گزارش هر گونه خشونت مبتنی بر جنسیت، سو استفاده یا آزار خانگی، با مرکز پناهندگان یا خط مشاوره سو استفاده خانگی ملی تمس بگیرید / www.refuge.org.uk 08082000247 www.nationaldvhelpline.org.uk

اگر مشکل فوری دارید یا می‌خواهید جرمی را گزارش کنید، با پلیس - 999 (موارد اورژانسی) - 101 (موارد غیر اورژانسی) تماس بگیرید.

کلمات کلیدی

امنیت دیجیتال - اعمال و عاداتی برای ایمن نگهداشتن خود، دیگران و اطلاعات شخصی خود در هنگام استفاده از اینترنت

میان فردی - مرتبط با تعاملات بین افراد

تهدید آنلاین - خطر یا مشکلی که باعث یک حادثه یا عمل نامطلوب از طریق اینترنت می‌شود.

رمز عبور - یک مجموعه از کاراکترهای مخفی که اجازه دسترسی شما به یک سیستم کامپیوتری یا سرویس را فراهم می‌آورد.

امن - ایمن ماندن و بدور از تهدید بودن، قرار نگرافتن در معرض خطر و آسیب.

امنیت دیجیتال چیست؟

امنیت دیجیتال به معنی آگاهی و دانستن نحوه حفاظت از خود (و داده‌های خود) از خطرات در اینترنت است. امنیت دیجیتال اغلب تنها به معنی چند عادت درست است که باعث می‌شود کمتر نسبت به جرایم سایبری، کلاهبرداری و یا تهدید آسیب پذیر باشید. این کار شامل دانستن ترفندهایی است که مجرمین ممکن است برای بدست آوردن اطلاعات یا پول افراد و یا به خطر انداختن زندگی خصوصی افراد از آنها استفاده کنند.

رایج‌ترین نوع تهدید از این قرارند

- ویروس‌ها و بدافزارهایی که سعی می‌کنند اطلاعات شخصی یا اطلاعات حساب‌های شما را سرقت کنند («هک کنند»)، یا نرم افزارهایی روی دستگاه شما نصب کنند که می‌توانند جاسوسی شما را کنند.
- تقلب آنلاین که مجرمین در آن تلاش می‌کنند شما را متقاعد کنند که اطلاعات خود را به آنها بدهید
- زورگویان، کمین کنندگان و سو استفاده گرها کسانی هستند که از ناشناس بودن در اینترنت برای آزار رساندن، سو استفاده کردن و یا کنترل کردن شما استفاده می‌کنند.

تهدیدهای آنلاین به صورت بالقوه توانایی تاثیرگذاری در تندرسی فردی، مالی و عاطفی را دارند. با توجه به این موضوعات، آگاهی نسبت به امنیت دیجیتال به افراد کمک می‌کند که اعتماد بنفس خود در محیط آنلاین را افزایش دهند.

توصیه‌های ضروری در خصوص امنیت دیجیتال

داشتن رمز عبور قوی

ایمیل و تمامی حساب‌های آنلاین دیگر توسط یک رمز عبور یا کلید، قفل می‌شوند تا از دسترسی دیگران به حساب شما جلوگیری کنند. پیچیده کردن رمز عبور یا «قوی کردن» آن بهترین روش بری جلوگیری از دسترسی دیگران به اطلاعات خصوصی شما است.

داشتن یک رمز عبور قوی برای ایمیل ضروری است. اگر یک هکر به ایمیل شما دسترسی داشته باشد، می‌تواند رمز عبور تمامی حساب‌های دیگر شما را با استفاده از گزینه «فراموشی رمز عبور» ریست کند و به اطلاعات حساس شما در حساب‌هایتان دسترسی پیدا کند.

هکرها می‌دانند که بسیاری از ما از رمز عبورهایی مانند 123456، یک روز مهم در زندگی یا اسم کودک خود استفاده می‌کنیم - از مواردی که حدس زدن آنها آسان است استفاده نکنید. رمز عبورهای ساده را می‌توان به سرعت شکست، اما یک رمز عبور خوب اجازه دسترسی مجرمین را قطع می‌کند. ارزشش را دارد که وقت بگذارید و یک رمز عبور خوب ایجاد کنید.

برای ساختن یک رمز عبور قوی این مراحل را انجام دهید:

1. سه کلمه تصادفی را با هم تلفیق کنید: مانند، fork (چنگال)، fire (آتش)، rug (فرش) را با هم تلفیق کنید و کلمه‌ای مثل rugfirefork بسازید.
2. از حروف بزرگ استفاده کنید، مانند RugFireFork
3. عدد اضافه کنید، مانند 19RugFireForK90 و
4. برای پیچیده تر کردن رمز عبور از علامت هم استفاده کنید: !19RugFireForK90

هکرها لیستی از میلیون‌ها رمز عبور احتمالی را به اشتراک می‌گذارند، و سه کلمه تصادفی ساده‌ترین روش برای ایجاد یک رمز عبور جدید منحصر بفرد است و کمتر می‌شود آن حدس زد. به شدت توصیه می‌شود که رمزهای عبور خود را به صورت دوره‌ای تغییر دهید و از رمزهای عبور مشابه برای تمامی حساب‌های خود استفاده نکنید. اگر در ایجاد یک رمز عبور جدید مشکل دارید رمز عبور ساز ابزار خوبی است.

از برنامه مدیریت رمز عبور استفاده کنید

اگر نگران فراموش کردن رمزهای عبور «قوی» خود هستید، می‌توانید از برنامه مدیریت رمز عبور استفاده کنید. برنامه‌های مدیریت رمز عبور می‌توانند رمز عبور شما را در مرورگر اینترنت (از جمله Google Chrome یا Microsoft Edge) ذخیره کنند، بنابراین مرورگر رمز عبور شما را به خاطر دارد. این کار امن‌تر از استفاده از رمزهای عبور بد یا ضعیف است، اما در صورت از دست دادن دستگاه خود از آنها حفاظت کنید. برخی شرکت‌های متخصص در زمینه آنتی ویروس و امنیت آنلاین اگر از آنتی ویروس‌های آنها استفاده کنید، به طور استاندارد یک برنامه مدیریت رمز عبور ارائه می‌دهند؛ شرکت‌های دیگر به تنهایی اقدام به ارائه برنامه مدیریت رمز عبور می‌کنند.

تنظیم تایید دو مرحله‌ای

تایید دو مرحله‌ای با درخواست اطلاعاتی علاوه بر رمز عبور از شما، لایه‌ای دیگر از حفاظت را برای حساب شما ایجاد می‌کند. این کار کمک می‌کند که دیگران نتوانند به حساب‌های شما دسترسی داشته باشند، حتی اگر رمز عبور شما را داشته

باشند. دستورالعمل‌های مربوط به نحوه فعالسازی تایید دو مرحله‌ای برای ایمیل‌ها و رسانه‌های اجتماعی محبوب را می‌توانید در وب سایت **مرکز ملی امنیت سایبری** در اینجا مشاهده کنید.

حفاظت از دستگاه‌های خود در مقابل ویروس‌ها

ویروس‌ها برنامه‌های مخفی‌ای هستند که از طریق وب سایت‌ها، لینک‌های داخل ایمیل، ضمیمه‌ها یا رسانه‌های قابل حذف (مانند حافظه‌های USB) قابل انتقال هستند. آنها می‌توانند اختلالات زیادی ایجاد کنند و می‌توانند دسترسی شما به کامپیوتر و حساب‌هایتان را قطع کنند، اطلاعات شخصی شما را برای فروش یا استفاده سرقت کنند، پول شما را بدزدند، یا حتی شما را در منزل تحت نظر بگیرند. موضوع نگران کننده این که همه نمی‌دانند چطور از دستگاه‌های خود در مقابل این تهدیدها محافظت کنند. ONS گزارش داد که در سال 2020، 17% از افراد بزرگسالی که گوشی هوشمند داشتند، امنیت دستگاه خود را تامین نکرده بودند و 32% از آنها نمی‌دانستند که برنامه‌های امنیتی دارند یا خیر.

درست مانند یک سپر امنیتی، **آنتی ویروس** ابزاری است که بر روی لپ تاپ، تبلت یا تلفن نصب می‌شود و مشکلاتی که باعث آلوده شدن دستگاه‌های شما می‌شوند را متوقف می‌کند. حفاظت آنتی ویروس از یک کامپیوتر، لپ تاپ یا گوشی هوشمند برای جلوگیری از تهدیدهای رایج از جمله موارد زیر مهم است:

- **تروجان‌ها** که وانمود می‌کنند برنامه‌ای هستند که می‌خواهید آن را دانلود کنید (مثل یک برنامه آنتی ویروس، نرم افزار عکس یا یک فیلم رایگان) اما نرم افزارهای مخربی هستند (بد افزار) که بعد از نصب روی کامپیوتر یا گوشی فعال می‌شوند.
- **جاسوس افزار** که به ردیابی اطلاعات می‌پردازد و به منظور اعمال مجرمانه آنچه بر روی کامپیوتر خود انجام می‌دهید را نظارت می‌کند.
- **نرم افزار تبلیغاتی** که اقدام به باز کردن پاپ آپ های تبلیغاتی می‌کند و سعی می‌کند چیزهایی را به شما بفروشد.
- **باج افزار** که دسترسی شما به دستگاه‌تان را قطع می‌کند و از شما تقاضای پول می‌کند.
- **اسپم** که اقدام به تولید برنامه‌هایی به نام کرم می‌کند که از طریق اتصال به اینترنت وارد سیستم شما می‌شود، و برای ارسال ایمیل‌های «اسپم» به مخاطبین شما خود را تکثیر می‌کند. به ایمیل‌های ناخواسته **اسپم** یا **آشغال** گفته می‌شود. ایمیل اسپم را می‌توان تنها به عنوان مزاحمت در نظر گرفت، اما از آن همچنین می‌توان برای گول زدن افراد و گسترش اطلاعات نادرست استفاده کرد.

در اکثر سیستم‌ها **آنتی ویروس** یا نرم افزار محافظت در مقابل **جاسوس افزار** از قبل نصب شده است، به عنوان مثال در لپ تاپ‌های دارای Microsoft Windows10 نرم افزار Windows Defender نصب شده است.

می‌توانید محافظت آنتی ویروس مضاعفی دریافت کنید: گاهی اوقات این حفاظت رایگان است، اما شرکت‌هایی هم هستند که به ارائه برنامه‌های پولی می‌پردازند.

نرم افزارهای قدیمی‌تر ممکن است دارای حفره‌هایی باشند که ویروس می‌تواند از طریق آنها نفوذ کند. **به روز رسانی** این حفره‌ها را می‌بندد. می‌توانید تنظیم کنید که برنامه‌ها و نرم افزارها به طور خودکار به روز شوند تا هرگونه حفره موجود در امنیت بسته شود. این به این معنی است که نیازی نیست که این کار را به خاطر بسپارید. گاهی اوقات ممکن است مجبور شوید به طور دستی دستگاه خود را به روز کنید و معمولا انجام این کار به شما یادآوری می‌شود. این به روز رسانی‌ها را نادیده نگیرید!

تهیه نسخه پشتیبان از داده‌ها

ویروس‌ها می‌توانند داده‌ها و اطلاعات شما را حذف و یا سرقت کنند. برای حفاظت از عکس‌ها، فایل‌ها و اطلاعات شخصی خود، باید قبل از به روز رسانی دستگاه از این اطلاعات نسخه پشتیبان تهیه کنید. نسخه پشتیبان به معنی ایجاد یک نسخه است که می‌تواند فیزیکی و با استفاده از یک هارد درایو قابل حمل، یا ایجاد نسخه در یک دستگاه دیگر، و یا در حافظه «ابری» (آنلاین) باشد. دلیل این امر این است که گاهی اوقات به روز رسانی‌ها می‌توانند باعث تغییر در فایل‌ها شوند، اما اگر نسخه پشتیبان از داده‌های خود داشته باشید می‌توانید به سرعت آنها را بازیابی کنید و امکان اخاذی از شما توسط باج افزارها وجود ندارد. می‌توانید تهیه نسخه پشتیبان خودکار را فعال کنید، این کار به این معناست که نیازی نیست تهیه نسخه پشتیبان را به خاطر داشته باشید.

برای کسب اطلاعات بیشتر در خصوص تهیه نسخه پشتیبان می‌توانید به این وب سایت مراجعه کنید
www.getsafeonline.org/protecting-your-computer/Backups

به طور خلاصه

- برای ایمیل خود از یک رمز عبور مجزا استفاده کنید
- بررسی کنید که آیا رمزهای عبور ایمیل یا حساب‌های دیگر شما قوی هستند یا خیر
- بررسی کنید که آیا می‌دانید چطور رمز عبور خود را تغییر دهید و این کار را مرتب انجام دهید
- از یک رمز عبور مشابه برای چندین حساب استفاده نکنید و اگر نگران فراموش کردن رمزهای عبور خود هستید، ز برنامه مدیریت رمز عبور استفاده کنید.
- از تایید دو مرحله‌ای استفاده کنید
- بررسی کنید که آیا آنتی ویروس دارید و اینکه آنتی ویروس شما فعال هست یا خیر (و اگر مطمئن نیستید از کسی کمک بگیرید)
- از آنتی ویروس خود استفاده کنید و آن را به روز کنید - به طور منظم دستگاه خود را اسکن کنید و آنتی ویروس خود را به روز نگهدارید تا در مقابل ویرس‌ها و باگ‌های جدید در امان باشید
- مراقب باشید که چه چیزی دانلود میکنید - برنامه‌های جاسوسی و تبلیغاتی با چسباندن خود به چیزهایی که دانلود میکند به کامپیوتر شما نفوذ میکنند، پس بدانید که از کجا باید فایل‌های خود را دانلود کنید.

اگر مشکلی پیش بیاید چه کار کنیم

اگر لینکی را روی لپ تاپ خود باز کرده‌اید یا دستورالعمل‌های نصب آن را رعایت کرده‌اید اما شک دارید، نرم افزار آنتی ویروس را باز کنید و کامپیوتر خود را اسکن کنید. به آنتی ویروس اجازه دهید ویروس‌ها را حذف کند و با استفاده از توصیه‌های آن دستگاه خود را بازیابی کنید. اگر مشکل حل نشد می‌توانید از یک متخصص کمک بگیرید.

دوست نزدیک شما با شما تماس می‌گیرد و خیلی ناراحت به نظر می‌رسد. او فایل ضمیمه شده به یک ایمیل که فکر می‌کرده یک تصویر است، را باز کرده. اما در واقع آن یک تروجان حاوی باج افزار بوده است و اکنون امکان دسترسی به کامپیوتر خود را ندارد. چه کار خواهید کرد، و به او می‌گویید که چکار کند؟

اگر به باج افزار آلوده شده‌اید، بدانید که در صورت پرداخت وجه به آنها شما پول اعمال مجرمانه را پرداخت می‌کنید، و هیچ تضمینی وجود ندارد که بتوانید به دستگاه خود دسترسی داشته باشید؛ این کار می تواند این تصور را ایجاد کند که شما در آینده نیز دوباره هزینه خواهید کرد و به استقبال حملات آینده می‌روید.

انواع رایج تهدیدهای آنلاین

تقلب و کلاهبرداری

کلاهبرداری روشی برای سرقت پول از یک فرد یا ارائه اطلاعات شخصی آنها است، پس یک مجرم می‌تواند حساب‌های آنها و یا هویت آنها را سرقت کند. این می‌تواند شامل استفاده از ویروس‌هایی باشد که داده‌های کامپیوتر یا حساب آنلاین آنها را می‌دزدد و یا با گمراه کردن یا گول زدن فرد را مجبور می‌کند که با اراده خود به آنها پول پرداخت کند.

کلاهبرداری اغلب از طریق استفاده از ایمیل‌های تقلبی (**فیشینگ**)، پیام متنی (**اسمیشینگ**) یا تماس تلفنی (**ویشینگ**) انجام می‌شود. ایمیل‌ها و یا پیام‌های کوتاه ممکن است حاوی لینک‌هایی باشند که شما را به وب سایت‌های تقلبی هدایت می‌کنند و این وب سایت‌ها شما را وسوسه میکنند که اطلاعات شخصی خود را وارد کنید یا به عنوان گذرگاهی برای ورود ویروس به کامپیوتر شما عمل می‌کنند. یا ایمیلی که می‌تواند دارای یک فایل ضمیمه باشد که این فایل حاوی ویروسی است که اطلاعات بانکی، اطلاعات شخصی یا عکس‌های شما را می‌دزدد.

کلاهبرداری‌ها باعث می‌شوند فکر کنید که یک سازمانی که آن را می‌شناسید و یا گاهی اوقات فردی که نیاز به کمک دارد، با شما تماس گرفته است. این کلاهبرداری‌ها به گونه‌ای طراحی شده‌اند که شما را برای انجام یک «عمل» تحت فشار قرار می‌دهند - باز کردن یک لینک، رائه اطلاعات، کلیک بر روی یک فایل ضمیمه. آن را باور نکنید!

ما در اینجا زمان کافی برای لیست کردن انواع کلاهبرداری‌ها و تقلب‌ها را داریم. برای کسب اطلاعات بیشتر در خصوص موارد استفاده از کلاهبرداری‌های مجرمانه، و همچنین توصیه در مورد نحوه گزارش دادن تقلب و جرایم سایبری از این وب سایت بازدید کنید: www.actionfraud.police.uk

فیشینگ

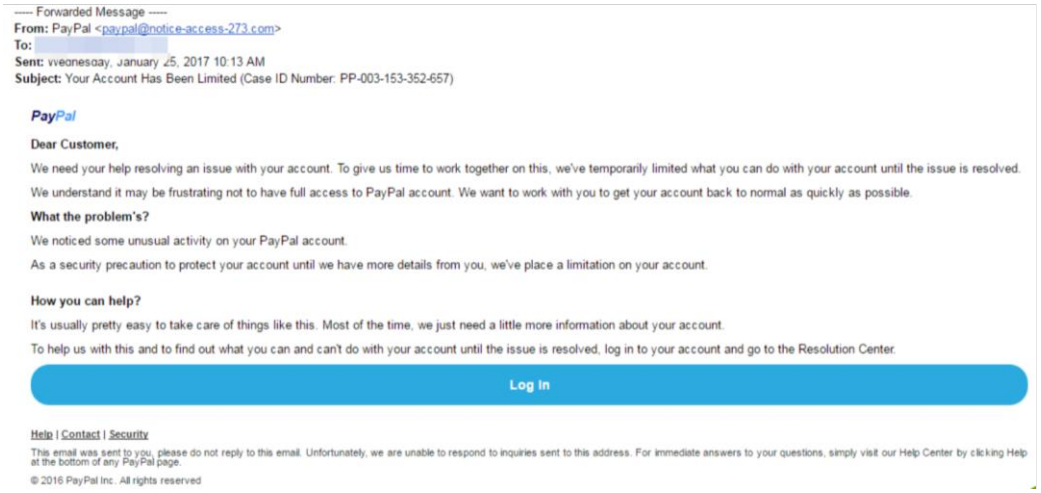
فیشینگ نوعی کلاهبرداری است که مجرم سایبری از یک «قلاب» برای فریب افراد در ارائه اطلاعات شخصی، حساب بانکی یا اطلاعات کارت بانکی، یا اطلاعات تماس و رمزهای عبور استفاده می‌کند. آنها سپس از این اطلاعات برای دسترسی به حساب‌های شما و سرقت پول یا حساب‌های ایمیل و یا سرقت هویت استفاده می‌کنند. مجرمین ممکن است یک ایمیل فیشینگ را به هزاران فرد بفرستند، با این امید که بتوانند تنها چند نفر را گول بزنند و از آنها پول یا اطلاعات سرقت کنند.

هکرها و کلاهبردارها در وانمود کردن به اینکه از طرف یک فرد یا یک سازمان مورد اعتماد شما تماس می‌گیرند بسیار عالی عمل می‌کنند و حتی ممکن است از نام و اطلاعات فردی دیگر شما نیز برای متقاعد کردنتان استفاده کنند. آنها سعی خواهند کرد با استفاده از یک پیشنهاد و یا تهدید شما را فریب دهند. به عنوان مثال، ممکن است وانمود کنند که از طرف دولت هستند مثلاً مامور مالیات و می‌خواهند وجه پرداختی را به حساب شما برگردانند، و برای این کار باید اطلاعات حساب شما را داشته باشند. آنها می‌توانند وانمود کنند که از طرف شورای محلی شما تماس می‌گیند، و بگویند که باید جریمه‌ای را بپردازید یا در غیر اینصورت به دادگاه احضار می‌شوید، یا وانمود کنند که از طرف بانک یا یک شرکت واسط بانکی مثل PayPal تماس می‌گیرند و بگویند که دسترسی شما به حسابتان مسدود شده است.

این ویدئوی پلیس Metropolitan در خصوص فیشینگ را مشاهده کنید.

روش سریع برای بررسی اینکه این ایمیل واقعاً از طرف چه کسی ارسال شده است و اینکه فیشینگ است یا خیر، این است که به آدرس فرستند ایمیل دقت کنید نه به آدرس که در فیلد From (از طرف) نوشته شده است. یک پیام واقعی اغلب از طرف یک آدرس سازمانی قابل شناسایی ارسال می‌شود (مانند noreply@yourbank.com)، اما کلاهبرداران و مجرمین نمی‌توانند از دامین‌های اصلی بانک یا سازمان شما استفاده کنند، پس اغلب آدرس ایمیل با یک چند کلمه و عدد تصادفی پر می‌شود (مانند noreply@1234bank12.com) اگر ایمیل از طرف یک آدرس خصوص باشد (مانند person@gmail.com) احتمال ندارد که واقعاً از طرف یک سازمان رسمی ارسال شده باشد - حتی Google از دامین GoogleMail (@gmail) برای ارسال ایمیل‌های سازمانی استفاده نمی‌کند.

با نگاه انداختن به این مثال، می‌توانید ببینید که هرچند به نظر می‌رسد که این ایمیل واقعاً از طرف PayPal ارسال شده باشد، اما از یک **دامین متفاوت** در آن استفاده شده است: Paypal@**notice-accessxxx.com**


----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

بهتر است در مورد ایمیل‌هایی که برای اینکه واقعی باشند زیادی خوب هستند، یا ایمیل‌هایی که شما را وادار می‌کنند سریع تصمیم گیری کنید، محتاط باشید، حتی اگر از لوگوی درست استفاده کنند و قانونی به نظر برسند. آرامش خود را حفظ کنید و پیامی که دریافت کرده‌اید را به چالش بکشید. پاسخ ندهید و بر روی لینکی کلیک نکنید. به محض اینکه بر روی لینک کلیک

کنید ممکن است ویروس روی کامپیوتر شما نصب شود و اطلاعات شما را بدزدد، یا ممکن است به یک وب سایت مخرب یا تقلبی هدایت شوید و از شما خواهسته شود اطلاعات بانکی خود را وارد کنید و این اطلاعات را سرقت کنند.

شناسایی ایمیل‌های فیشینگ و کلاهبرداری

- آیا فرستنده را می‌شناسید؟ آیا به یک شکل کلی شما را خطاب قرار می‌دهند؟
- آیا در آن اشتباهات املایی وجود دارد و نگارش آن ضعیف است؟
- آیا از شما می‌خواهد کاری را انجام دهید یا در آن ضرورت وجود دارد یا شما را تهدید می‌کند؟
- آدرس ایمیلی که این پیام از طرف آن آمده است را باز کنید. آیا آدرس دامین درست است؟
- آیا این پیام غیر منتظره است و یا از سمت شرکتی ارسال شده است که آن را می‌شناسید؟
- اگر این ایمیل شما را به یک وب سایت هدایت می‌کند، آیا علامت قفل و https:// در ابتدای آدرس وب سایت وجود دارد؟

برای اطلاع از نکات بیشتر در خصوص شناسایی ایمیل‌های فیشینگ می‌توانید به این وب سایت مراجعه کنید:
www.ncsc.gov.uk

Zahra ایمیلی دریافت می‌کند که فکر میکند از سمت بانکش ارسال شده است - او ایمیل را باز می‌کند و می‌بیند که آنها به طور موقت حساب او را مسدود کرده‌اند. Zahra با ترس متوجه می‌شود که بانک فعالیت غیر طبیعی در حساب بانکی او مشاهده کرده است و تصمیم گرفته برای حمایت از او حساب را مسدود کند. ایمیل می‌گوید که او نمی‌تواند تا زمانی که وارد حساب خود نشده و حساب را دوباره فعال نکند از حساب بانکی خود استفاده کند، و از او می‌خواهد که روی یک لینک کلیک کند. Zahra می‌داند که باید فردا اجاره بهای خود را پرداخت کند و باید به سرعت به حساب خود دسترسی داشته باشد، اما مشکوک می‌شود.

Zahra برای مشورت با شما تماس می‌گیرد: به او چه می‌گویید و چطور او را مشاوره می‌دهید؟

لینک ممکن است خطرناک باشد. ممکن است به این معنا باشد که هکرها می‌خواهند برای مقاصد کلاهبرداری از قبیل سرقت اطلاعات یا هک ایمیل، بانک یا حساب‌های رسانه‌های اجتماعی، چیزی را روی کامپیوتر او نصب کنند. یا اینکه لینک ممکن است او را به وب سایتی هدایت کند (یک نسخه تقلبی از بانک) و از او بخواهد نام کاربری و رمز عبور و یا اطلاعات بانکی دیگر را وارد کند. وقتی او این اطلاعات را به وب سایت بدهد، حساب بانکی و پول خود را به کلاهبرداران تقدیم خواهد کرد.

بانک شما برای درخواست اطلاعات شخصی از طریق ایمیل، تلفن یا پیامک با شما تماس نخواهد گرفت. اگر مطمئن نیستید که تماس واقعاً از سمت بانک است یا یک کلاهبرداری ویشینگ است، تماس را قطع کنید و در اینترنت به دنبال شماره تلفن مرکز خدمات مشتری بگردید. قبل از تماس مجدد 5 دقیقه صبر کنید و از یک خط تلفن دیگر استفاده کنید، شاید کلاهبرداران بتوانند خطوط تلفن را بدزدند.

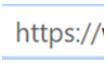
بعد از صحبت با شما:

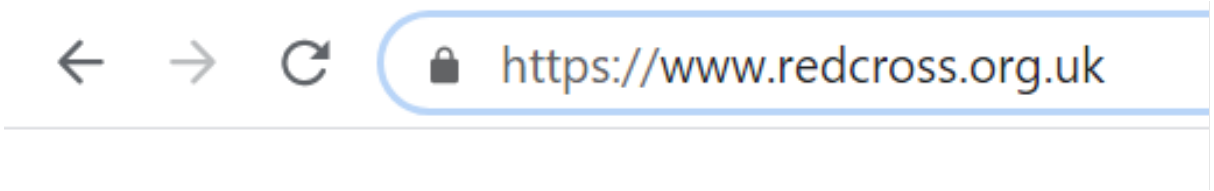
Zahra در اینترنت شماره تلفن مرکز خدمات مشتری را جستجو میکند. بانک تایید می‌کند که این ایمیل تقلبی است و حساب او مثل سابق کار می‌کند. آنها به او می‌گویند که لینک داخل ایمیل او را به وب سایتی هدایت می‌کند که شبیه به وب سایت بانک است. گاهی اوقات اگر بانک بتواند ثابت کند که افراد مراقب حساب خود نبوده‌اند، پس گرفتن پول برای قربانیان این نوع کلاهبرداری دشوار است.

برای کسب اطلاعات بیشتر در خصوص فیشینگ می‌توانید به وب سایت مرکز ملی امنیت سایبری مراجعه کنید.
www.ncsc.gov.uk/guidance/phishing

وب سایت‌های امن و غیر امن

مهم است بتوانید بررسی کنید که آیا یک وب سایت امن است یا خیر. هر وب سایتی که بازدید میکنید ممکن است نا امن باشد و هکرهایی که ایمیل‌های تقلبی برای شما ارسال می‌کنند ممکن است شما را به وب سایت‌های تقلبی‌ای هدایت کنند که احتمالاً خیلی واقعی به نظر می‌رسند.

به این علامت قفل  یا این علامت‌ها  در نوار مرورگر نگاه کنید، اینها به معنی امن بودن وب سایت هستند.



گاهی اوقات شما هم علامت **قفل** و هم **https** را خواهید دید، یا فقط علامت قفل را، این موضوع به کامپیوتر و یا مرورگر شما برمی‌گردد. یک وب سایت که تنها دارای **http** است، ممکن است امن نباشد چون که **'s'** نشان دهنده ایمن بودن وب سایت است.

اگر از شما خواسته شد که وارد یکی از حساب‌های خود شوید، اطلاعات پرداخت و یا اطلاعات دیگر خود را وارد کنید، مطمئن شوید که وب سایتی که در ابتدای نام وب سایتی که در آن حضور دارید 'https' وجود دارد. تنها اطلاعات ورود خود را زمانی وارد کنید که مطمئن هستید که آدرس وب سایت درست است ووب سایت ایمن است.

همیشه برای ورود به وب سایت بانک آدرس کامل را وارد کنید، بخصوص اگر وارد حساب بانکداری اینترنتی خود می‌شود. هیچگاه از موتور جستجو برای ورود به وب سایت بانک استفاده نکنید، زیرا ممکن است این مراحل توسط هکرها برای سرقت اطلاعات شما چیش بینی شده باشد.

اقدام علیه فیشینگ و وب سایت‌های کلاهبردار

برای حفاظت از خود نکات زیر را به خاطر بسپارید:

- نرم افزار مرورگر، آنتی ویروس و ضد جاسوس خود را به روز نگه دارید
- از وب سایت‌های پر خطر که امن نیستند و علامت قفل ندارند اجتناب کنید
- هیچ وقت بر روی لینک داخل ایمیلی که منبع آن ناشناخته یا مشکوک است، کلیک نکنید
- هیچ وقت اطلاعات شخصی، رمز عبور یا کدهای امنیتی خود را در اختیار دیگران قرار ندهید

اگر هدف یک کلاهبرداری قرار گرفتید چکار باید بکنید

ایمیل، تماس، پیام یا وب سایت را گزارش کنید.

اگر ایمیلی دریافت کردید و از آن مطمئن نبودید، می‌توانید آن را از طریق report@phishing.gov.uk به مرکز خدمات **گزارش ایمیل‌های مشکوک (SERS)** ارسال کنید. آنها به شما خواهند گفت که این ایمیل فیشینگ است یا خیر.

اگر پیامک مشکوکی دریافت کردید، می‌توانید آن را به صورت رایگان به شماره 7726 ارسال کنید. این کار به ارائه دهنده تلفن شما امکان می‌دهد که پیام را بررسی کرده و در صورت کلاهبرداری اقدامات لازم را انجام دهد.

اطلاعات خود را به اشتراک نگذارید، در عوض آنها را بررسی کنید. هیچگاه با شماره تلفن داخل ایمیل تماس نگیرید یا روی لینک‌های موجود در آن کلیک نکنید، چون ممکن است شما را به یک حساب جعلی دیگر هدایت کنند. در عوض در اینترنت شماره‌های تبلیغاتی مختلف را پیدا کنید و با آنها تماس بگیرید.

بدون اینکه بدانید لینک‌ها شما را به کجا هدایت می‌کنند، روی آنها کلیک نکنید. برای بررسی اینکه آیا یک وب سایت اصل است، مرورگر خود را باز کنید و مستقیم با تایپ نام در نوار URL به سایت مراجعه کنید.

هیچ وقت رمز عبور یا شماره PIN خود را به اشتراک نگذارید. مهم نیست که کسی که این اطلاعات را از شما می‌خواهد مادرتان است یا بهترین دوستتان - رمز عبور خود را در اختیار کسی قرار ندهید.

اگر شما را برای ارائه اطلاعات بانکی خود گول زدند، سریعاً با بانک خود تماس بگیرید.

اگر پول خود را از دست داده‌اید، به بانک خود اطلاع دهید و آن را به عنوان یک جرم به مرکز **Action Fraud** (در انگلستان، ولز و ایرلند شمالی) یا **پلیس اسکاتلند** (برای اسکاتلند) گزارش کنید. انجام این کار باعث می‌شود که به دیگران کمک کنید در این دام نیافتند.

Action Fraud www.actionfraud.police.uk

روابط آنلاین

در این بخش در مورد تاثیر اینترنت بر روابط شخصی صحبت می‌کنیم. آنچه در محیط آنلاین انجام می‌دهیم می‌تواند مستقیما بر زندگی خصوصی ما تاثیر بگذارد. بنابراین، مهم است که در مورد اطلاعاتی که در اینترنت با دیگران به اشتراک میگذارید، مراقب باشید.

همه ما می‌خواهیم با دیگران ارتباط برقرار کنیم، و این یکی از بهترین خصوصیات اینترنت است که ما می‌توانیم با دوستان، خانواده و افرادی که دارای علایق یکسانی با آنها هستیم در سراسر دنیا به راحتی ارتباط داشته باشیم. در همین حین مهم است بدانیم که این ارتباطات باید به دقت مدیریت شوند، درست مانند ملاقات با یک فرد در خیابان، و اینکه دیگران ممکن است بخواهند با نیت بدی که منجر به سو استفاده می‌شود با ما ارتباط برقرار کنند.

سو استفاده آنلاین می‌تواند توسط افراد کاملا غریبه یا افرادی که آنها را از قبل می‌شناسیم اتفاق بیافتد، و ما در زیر به برخی نمونه‌های آنلاین سو استفاده میان فردی می‌پردازیم.

کلاهبرداری عشقی

کلاهبرداری عشقی زمانی اتفاق می‌افتد که یک نفر با استفاده از یک وب سایت یا اپلیکیشن دوستیابی یک رابطه را شکل می‌دهد تا اعتماد طرف مقابل را جلب کنید وسپس از او پول یا اطلاعات شخصی‌اش را درخواست می‌کند. احتمالاً آنها از یک پروفایل قلابی برای ایجاد رابطه استفاده می‌کنند و خود را مهربان و دلسوز نشان می‌دهند. اغلب اوقات این فراد سوال‌های شخصی زیادی می‌پرسند اما در مورد خودشان چیز زیادی نمی‌گویند. آنها تا زمانیکه فکر کنند اعتماد طرف مقابل را جلب کرده‌اند منتظر می‌مانند و از دلبستگی عاطفی برای درخواست کمک، معمولاً پول و گاهی اوقات دریافت یک بسته یا ارائه یک آدرس، استفاده می‌کنند. ممکن است تصاویری جعلی از خود ارسال کنند که اغلب آنها را از اینترنت گرفته‌اند.

صرف نظر از اینکه چقدر به آنها اعتماد دارید یا تا چه حد داستان آنها را باور کرده‌اید، **هیچ وقت** پول با کسی که در اینترنت با او آشنا شده‌اید پول رد و بدل نکنید و اطلاعات بانکی خود را به آنها ارائه ندهید.

اینکه کسی که فکر می‌کردید با شما دوستی خاصی را در اینترنت شکل داده است، شما را گول بزند، واقعاً بسیار ناراحت کننده است، اما می‌توانید موضوع را به Action Fraud گزارش کنید یا با شماره 03001232040 تماس بگیرید.

برای بررسی منبع یک تصویر می‌توانید از *جستجوی معکوس تصویر* استفاده کنید، این کار براساس نام تصاویر موجود در اینترنت را جستجو می‌کند تا دیگر افراد مشابه را بیابد. در اینجا می‌توانید جستجوی معکوس تصویر انجام دهید.

آزار و اذیت سایبری

آزار و اذیت سایبری یک اصطلاح عمومی برای آزار و اذیتی است که از طریق اینترنت یا با استفاده از تکنولوژی انجام می‌شود. این شامل هرگونه سو استفاده آنلاین می‌شود که هدف آن آسیب رساندن، ناراحت کردن و یا ضرر رساندن به دیگران است. اغلب آزار دهندگان از شبکه‌های اجتماعی مانند Facebook یا Twitter، پیامک یا انجمن‌های آنلاین استفاده می‌کنند. آزار و اذیت سایبری می‌تواند به نوبه خود آزار دهنده باشد زیرا می‌تواند از طریق اینترنت و تلفن موبایل در هر زمانی به سراغ افراد بیاید و محدود به یک موقعیت خاص مانند مدرسه یا محیط کار نیست.

اگر فردی مطالب غلط یا مخربی در مورد شما در اینترنت یا رسانه‌های اجتماعی منتشر کند، این کار به معناس آزار رساندن است و جرم محسوب می‌شود. همینطور اگر تماس تهدید آمیز یا ارعاب آوری دریافت کنید، فردی که این تماس را گرفته است مرتکب جرم کیفری شده است.

آزار رساندن می‌تواند متوجه هر کسی بشود، از جمله هم کودکان و هم بزرگسالان، اما اگر سرپرست یک کودک هستید باید بیشتر مراقب باشید. اگر شما یا فرزند شما یا فردی که او را می‌شناسید مورد آزار و اذیت از جمله آزار و اذیت آنلاین شده‌اید، می‌توانید برای مشاوره از طریق شماره 03003230169 با خط مشاوره ملی تماس بگیرید.

اغفال

اغفال وقتی اتفاق می‌افتد که فردی برای بهره برداری و کنترل فردی دیگر با او رابطه برقرار می‌کند. اغفال آنلاین کودکان و افراد جوان یک نگرانی خاص است، که در آن ممکن است کودک خردسال به منظور سو استفاده جنسی (به صورت آنلاین یا حضوری)، قاچاق مواد مخدر یا بهره برداری گمراه شود.

اغفال می‌تواند به صورت کوتاه مدت و یا بلند مدت رخ دهد و گمراه کنندگان ممکن است با خانواده کودک نیز رابطه برقرار کنند تا قابل اعتماد، معتبر و مفید به نظر برسند. هر کسی صرف نظر از نژاد، جنسیت، سن یا رابطه با کودک می‌تواند یک گمراه کننده باشد.

اغفال می‌تواند به صورت آنلاین رخ دهد که در این صورت گمراه کننده خود را همسن کودک معرفی می‌کند و برای اثبات آن به ارسال عکس و ویدئوی دیگران می‌پردازد. ممکن است برای محکم کردن موقعیت خود به عنوان یک دوست قابل اعتماد نزد فرد جوان با او بازی کنند، به او مشاوره دهند و برای او هدیه بخرند، یا سعی کنند که کودک را از خانواده و دوستان خود جدا کنند، برای مجبور کردن کودک به انجام یا عدم انجام کاری از او باج خواهی کنند، یا برای کنترل کودک از ایده «راز» استفاده کنند.

اطلاعات بیشتر در خصوص اغفال و منابع دیگر در مورد نحوه گفتگو با کودکان در مورد سو استفاده و تهدیدهای آنلاین را می‌توان در وب سایت NSPCC مشاهده کرد. www.nspcc.org.uk

اگر گمان می‌کنید کودکی در معرض خطر است موضوع را با پلیس در میان بگذارید. همچنین می‌توانید برای مشاوره و حمایت در خصوص گزارش انلاین سو استفاده با NSPCC تماس بگیرید.

پیام‌های سکسی و پورن انتقامی

پیام‌های سکسی به معنی ارسال پیام، عکس و ویدئوی سکسی به فردی دیگر می‌باشد. فرد ممکن است اقدام به ارسال تصویر خود یا تصویر دیگران کند. پیام سکسی می‌تواند به یک دوست، شریک یا فردی دیگر در اینترنت ارسال شود، و ممکن است حاوی لخت شدن جزئی یا کامل، ژست سکسی یا صحبت در مورد سکس باشد.

هرچند که ارسال پیام سکسی ممکن است با رضایت دو طرف انجام شود، اما تصاویر می‌توانند به سرعت بدون رضایت در اینترنت پخش شوند. اگر فردی تصویر یا ویدئویی که از شما در اینترنت به اشتراک گذاشته شده است را داشته باشد، می‌تواند آن را به افراد دیگر نیز ارسال کند.

پورن انتقامی زمانی رخ می‌دهد که فردی یک عکس یا فیلم **سکسی خصوصی** از یک فرد را بدون رضایت طرف و با نیت **مضطرب کردن او** به فرد یا افراد دیگر نشان دهد.

تهدید یک نفر به انتشار اطلاعات و عکس‌های خصوصی نیز باج خواهی است و جرم محسوب می‌شود. در اینجا می‌توانید اطلاعات بیشتری در خصوص پورن انتقامی بدست آورید

خط مشاوره پورن انتقامی - 08456000459

www.revengepornhelpline.org.uk/

به هیچ وجه درست نیست که فردی فرد دیگر را برای ارسال تصاویر لخت او تحت فشار قرار دهد.

مهم است به خاطر داشته باشید که تصاویر ارسال شده حتی با استفاده از سرویس‌هایی مثل Snapchat، را می‌توان اسکرین شات گرفت و ذخیره کرد. اگر تصویر لختی خود را ارسال کرده‌اید و نگران اتفاقات متعاقب آن هستید، می‌توانید به این نکات عمل کنید:

- بخواهید که تصویر را پاک کنند.
- به تهدیدها پاسخ ندهید.
- با یک نفر صحبت کنید و از او کمک بگیرید. می‌توانید با خط مشاوره پورن انتقامی تماس بگیرید.
- **آنچه اتفاق افتاده است را گزارش کنید.** می‌توانید محتوای توهین آمیز را در وب سایتی که این تصاویر در آن منتشر شده‌اند گزارش کنید. اکثر پلتفرم‌های رسانه‌های اجتماعی دارای ابزاری برای گزارش محتوا هستند. شما همچنین باید این نوع آزار و اذیت را به پلیس گزارش دهید. اگر ای موضوع اورژانسی نیست با 101 تماس بگیرید.

مهم است بدانید که به اشتراک گذاری تصاویر لختی یک فرد **زیر 18 سال** سو استفاده از کودک محسوب می‌شود و براساس قانون جرایم جنسی مصوب 2003، یک جرم کیفری است. اقداماتی مانند ارسال «پیام سکسی» به یک فرد زیر 18 سال می‌تواند منجر به تحقیقات پلیسی شود.

اگر نگران این هستید که تصاویر کودکانتان به اشتراک گذاشته شوند یا نگرانی دیگری در خصوص حفاظت از کودک خود در اینترنت دارید، می‌توانید این موضوع را به مرکز بهره برداری از کودک و ایمنی محافظت آنلاین گزارش کنید.
www.ceop.police.uk

کمین سایبری و نظارت

کمین یک الگوی رفتاری از جانب فردی دیگر است که شما را از اعمال خشونت علیه خود می‌ترساند و یا باعث می‌شود که شما هوشیار و مضطرب باشید و تاثیری جدی بر فعالیت‌های روزانه شما دارد. وقتی این اتفاق در محیط آنلاین رخ دهد، به آن کمین سایبری گفته می‌شود. این اقدام می‌تواند شامل جمع آوری اطلاعات در مورد شما، جعل هویت شما، ارسال پیام‌های ناخواسته یا تهدید آمیز، نظرت بر شما یا دسترسی به حساب‌های آنلاین و پخش اطلاعات غلط در مورد شما باشد. یک فرد کمین کننده می‌تواند یک فرد غریبه باشد. کمین سایبری می‌تواند تاثیری جدی بر قربانی خود داشته باشد و یک جرم کیفری محسوب می‌شود.

خط مشاوره ملی کمین - 08088020300
www.stalkinghelpline.org/faq/about-the-law/

اگر نگران هستید که توسط یک سو استفاده گر مورد کمین یا نظارت قرار گرفته باشید:

- از مواجه با فرد کمین کننده که اغلب سعی می‌کند با شما صحبت کند و وارد رابطه شود، خودداری کنید. هیچ وقت با ملاقات او موافقت نکنید و با او روبرو نشوید.
- این موضوع را جدی بگیرید و به پلیس اطلاع دهید. می‌توانید برای صحبت مستقیم با پلیس با شماره 101 تماس بگیرید، اما اگر فکر می‌کنید که این یک تهدید سریع است با 999 تماس بگیرید.
- تنظیمات حریم خصوصی خود را بررسی کنید و مطمئن شوید که تنها حداقل اطلاعات شما در اینترنت در دسترس هستند و برچسب موقعیت جغرافیایی را غیر فعال کنید.
- به افراد پیرامون خود هشدار دهید. آنها باید آنچه در مورد شما به اشتراک میگذارند را بررسی کنند و شاید نیاز باشد آنها نیز تنظیمات حریم خصوصی شان را چک کنند.
- آنچه اتفاق می‌افتد را ثبت کنید - شاید بخواهید از تماس‌ها، پیام‌ها یا پست‌های شبکه‌های اجتماعی خود اسکرین شات تهیه کنید، این به معنی داشتن یک نسخه از مدارک و شواهد در صورتیکه فرد مرتکب جرم پیام‌ها و پست‌های خود را بعداً حذف کند.

سو استفاده خانگی، آزار و اذیت و نظارت

یک سو استفاده گر به طور بالقوه می‌تواند از قابلیت‌های یک دستگاه متصل به اینترنت برای تماشا، چک کردن و کنترل یک قربانی سو استفاده کند. این امر می‌تواند شامل نظارت ارتباطات شما با دیگران، ردیابی موقعیت شما از طریق دستگاه، یا بررسی مخارج مالی شما باشد. وقتی این رفتار توسط یک شریک ، همسر قبلی، عضو خانواده یا سرپرست انجام شود، همه اینها تحت قانون انگلستان به معنای انواع سو استفاده خانگی تلقی می‌شوند.

اگر نگران هستید که فردی ممکن است تلفن همراه یا دستگاه دیگر شما را تحت نظارت داشته باشد، خط مشاورهسو استفاده خانگی ملی دارای یک **ابزار راهنمایی مرحله به مرحله** است که به شما در تغییر تنظیمات دستگاه برای ایمن‌تر کردن آن کمک می‌کند.

خط مشاورهسو استفاده خانگی ملی (24 ساعت شبانه روز) 08082200247

www.nationaldomesticviolencehelpline.org.uk

آیا با جملات زیر موافق هستید؟

تهدیدهای انلاین مهم نیستند چون در دنیای «واقعی» اتفاق نمی‌افتند

خیر. سو استفاده آنلاین تاثیری جدی بر زندگی افراد می‌گذارد و مقامات باید همیشه با آن به طور جدی برخورد کنند. کمین، نظارت و آزار و اذیت همگی رفتارهای پر خطری هستند که مقصر آنها شما نیستید. شما حق این را دارید که آنها را گزارش کنید، در این خصوص مشاوره بگیرید و برای رفع آنها کمک بگیرید.

جرم آزار و اذیت به معنی تهدید به خشونت در دنیای واقعی است.

قوانین میگویند که آزار و اذیت وقتی اتفاق می‌افتد که نیت رفتار یک فرد ایجاد اضطراب و هوشیاری باشد و این رفتار بیش از یک بار رخ دهد. ممکن است این رفتارها در مناسبات مختلف متفاوت باشند. به عنوان مثال، یک پیام که هدف ان مضطرب کردن شما باشد، آزار و اذیت محسوب نمی‌شود. دو پیام می‌تواند آزار و اذیت باشد، یا یک تماس به همراه یک ایمیل تهدید آمیز می‌تواند آزار و اذیت باشد. فعالیت‌های دیگری که ممکن است به عنوان آزار و اذیت قلمداد شوند شامل این موارد می‌باشد: تعقیب شدن، تحت نظارت بودن در محیط کار و منزل، ایجاد خسارت به اموال، یا اینکه بدون انجام کار اشتباهی شما را به پلیس گزارش کنند.

Zahra دختر عمویی دارد که بسیار به او نزدیک است. دختر عموی او اخیراً تغییر کرده است و ناراحت، حساس به نظر می‌رسد و همیشه هنگامی که آنها با هم هستند به طور عصبی گوشی خود را چک میکند. در نهایت، دختر عموی Zahra به او می‌گوید که چند وقتی است که نمی‌تواند راحت بخوابد و به خاطر تهدیدهای شوهر سابقش که از هم جدا شده‌اند، بسیار مضطرب است. او به طور مرتب ایمیل می‌فرستد و می‌گوید که او یک همسر و مادر افتضاح است، و باعث شرمساری هر دو خانواده است، و اینکه باید برگردد و با او زندگی کند. دختر عموی Zahra به خاطر این موضوع بسیار مضطرب است.

او توضیح می‌دهد که شوهر سابقش یک عکس لختی از او دارد که مربوط به زمانی است که رابطه آنها سالمتر بود. او تهدید میکند که اگر به او برنگردد، عکس لختش را برای خانواده‌اش ارسال می‌کند.

آیا دختر عموی Zahra قربانی یک جرم است؟

بله. دختر عموی Zahra قربانی **آزار و اذیت و کنترل اجباری** است. این تهدیدها برای اعمال کنترل بر او علیه دختر عموی Zahra انجام می‌شود. قانون میگوید که این جرم وقتی اتفاق می‌افتد که یک فرد طوری رفتار کند که نیت مضطرب کردن و هوشیار کردن طرف مقابل باشد. این رفتار باید بیش از یک بار از فرد سر بزند.

از آنجا که این رفتار از جانب همسر سابق او انجام می‌شود، این آزار و اذیت نوعی **کنترل اجباری** (نوعی از **سو استفاده خانگی**) محسوب می‌شود. این یک جرم کیفری است. او می‌تواند موضوع را به پلیس گزارش کند.

این اقدام همچنین مصداق تهدید پورن انتقامی است، یعنی به اشتراک گذاری تصاویر سکسی بدون رضایت، و با نیت ایجاد اضطراب یا تحقیر. این تهدید به خودی خود جرم محسوب نمی‌شود، با این حال، اگر شوهر سابق دختر عموی Zahra تصویر را از طریق ایمیل، رسانه‌های اجتماعی، از جمله Whatsapp یا پیامرسان‌های دیگر، در اینترنت پخش کند، این کار جرم است.

همسر Zahra نیز در مورد شرافت خانواده و اینکه جدایی آنها باعث «شرمساری» خانواده می‌شود صحبت می‌کند. این به اصطلاح خشونت «شرافت» نوعی از سو استفاده است و Zahra ممکن است بخواهد از سازمانی که متخصص کار بر روی

قربانیان سو استفاده مبتنی بر شرافت هستند، کمک دریافت کند. **Karma Nirvana** در روزهای دوشنبه تا جمعه یک خط مشاوره تلفنی دارد 08005999247 www.karmanirvana.org.uk

خلاصه

- قبل از ارسال پست فکر کنید. بدون در نظر گرفتن اینکه اگر مطالبی که منتشر می‌کنید به دست نا اهلان بیافتد چه می‌شود، محتوایی بارگذاری یا به اشتراک نگذارید. به محض اینکه چیزی را منتشر می‌کنید کنترل آن از دست شما خارج می‌شود، به خصوص اگر کسی از آن اسکرین شات بگیرد.
- از هویت خود محافظت کنید و هر چیزی را در شبکه‌های اجتماعی منتشر نکنید. رسانه‌های اجتماعی ابزاری عالی برای ارتباط گرفتن با دوستان و خانواده است اما به این فکر کنید که ممکن است بیش از آن چیزی که نیت آن را دارید از زندگی خود به دنیا اطلاعات بدهید.
- به دقت در نظر داشته باشید که چه کسی می‌تواند آنچه به اشتراک می‌گذارید را ببیند، بررسی کنید که آیا تنظیمات حریم خصوصی شما به درستی تنظیم شده‌اند و فکر کنید که دارید با چه کسی صحبت میکنید.
- در مورد نشانه‌های کلاهبرداری و نحوه نگاه کردن به ایمیل‌ها و وب سایت‌های کلاهبرداری آگاه باشید.
- هیچ وقت اطلاعات خیلی شخصی خود نظیر آدرس، شماره تلفن، نام کامل و تاریخ تولد خود را در اینترنت منتشر نکنید.
- هیچ وقت اطلاعات ورود به حساب و رمز عبور خود را منتشر نکنید.
- هیچ وقت ایمیل‌ها، فایل‌ها یا فایل‌های ضمیمه ناشناس را باز نکنید و نسبت به فیشینگ و کلاهبرداری‌ها هوشیار باشید.