

## پروژه توانمندسازی دیجیتالی و ارتباطی زنان پناهنده

3 رهنمود برای همراهی و رکشاپ



مصونیت دیجیتالی

این کتاب راهنما به حیث یک ابزار حمایتی برای زنانی که در ورکشاپ های پروژه توانمند سازی دیجیتالی و ارتباطی زنان مهاجر سهم می گیرند، تهیه گردیده است.

هدف این کتاب زنانی است که حالت مهاجرتی، حفاظت بشر دوستانه و پیوستگی فامیلی مهاجرتی دارند و در بریتانیا زندگی می کنند.

پروژه توسط دفتر حمایت از اسکان مجدد پناهگاهی و ریاست ادغام تمویل می شود.

جا دارد تشکری کنیم از از اعضای شبکه صدا (VOICES network) و سفیران شبکه صدا که در ایجاد این اسناد کمک کردند

این کتاب به زبان های انگلیسی، امهری، عربی، کردی (سورجانی)، سومالی، تیگرینیایی و اردو در دسترس است.

انتظار می رود که زنان مهاجر که قادر به اشتراک در این ورکشاپ نشدند، بتوانند به شکل سودمندی از این کتاب استفاده نموده تا از این طریق به شیوه خود شان معلومات را دریابند.

## محتویات

|                                                                  |                              |
|------------------------------------------------------------------|------------------------------|
| مقدمه                                                            | Error! Bookmark not defined. |
| اصطلاحات کلیدی                                                   | Error! Bookmark not defined. |
| مصونیت دیجیتالی چیست؟                                            | 4                            |
| توصیه های ضروری مصونیت دیجیتالی                                  | 5                            |
| قوی (Passwords) داشتن رمز عبور                                   | 5                            |
| استفاده از مدیر رمز عبور Password manager                        | 6                            |
| ترتیب نمودن تصدیق دو فاکتور                                      | 6                            |
| حفاظت دستگاه تان از ویروس ها                                     | 7                            |
| معلومات تان را پشتیبانی کنید (Backup your data)                  | 7                            |
| خلاصه                                                            | 8                            |
| اگر کار به درستی پیش نرود چی اقدامی باید صورت گیرد؟              | 8                            |
| انواع رایج تهدید های آنلاین                                      | 8                            |
| کلاهبرداری و فریبکاری                                            | 9                            |
| ایمیل های جعلی                                                   | 9                            |
| وبسایت های محفوظ و غیر محفوظ                                     | 11                           |
| چی باید کرد اگر شما توسط یک عمل فریبکاری مورد هدف قرار می گیرید؟ | 12                           |
| ارتباطات آنلاین                                                  | 13                           |
| فریبکاری عاشقانه                                                 | 13                           |
| قلدری سایبی                                                      | 13                           |
| بهره برداری                                                      | 14                           |
| سیکستینگ و سکس انتقام جویانه                                     | 14                           |
| کمین های سایبری و نظارت                                          | 15                           |
| سو استفاده خانگی، اذیت و نظارت                                   | 17                           |

## مقدمه

این وسیله به تنهایی برای جستجو نمودن، وضاحت دادن و سنجش تمام تهدیدهای محافظتی موجوده ناتوان است اما انتظار می‌رود که توجه شما را به چند نکات کلیدی که می‌توانید معلومات بیشتری را بدست بیاورید را جلب کند. ما اذعان می‌داریم که در بحث مصونیت دیجیتالی ما روی موضوعات مربوط به خشونت، سو استفاده و حملات جنایی جنسیتی، که می‌تواند حساس و اغلباً تابو باشند، صحبت می‌کنیم. اکثراً ماموریت بشردوستانه و اصل عدم ضرر رساندن ما به مفهوم انجام اقدامی که در حد توان ما می‌باشد تا برای مقابله با خشونت جنسی، به شمول تهیه معلومات جهت حمایت مردم در قسمت انتخاب و تصامیم شان به منظور تقویه و حفاظت آنها، انجام دهیم. در تمام این راهنمایی شما لینک های جاسازی شده را در میان متن ها خواهید یافت که اگر به روی آنها کلیک کنید شما را به سایت انترنتی مورد نظر سوق خواهند داد. به طور مثال اگر شما [اینجا](#) کلیک بکنید به سایت صلیب سرخ بریتانیا سوق داده می‌شود. تا جای ممکن تلاش کرده ایم تا لینک های منابع ترجمه شده را شامل کنیم اما اکثریت لینک های این راهنمایی بخاطر معلومات به لسان انگلیسی است. ضمن این که اعتراف بر محدودیت ترجمه ها به شکل خودکار داریم، ما معلومات در باره چگونگی استفاده از این کارکرد را در راهنمایی دوم داده ایم. مشوره جامع در مورد مصونیت دیجیتالی به شمول چگونگی محافظت دستگاه تان و اقدامات جهت محافظت خود تان و دیگران از تهدیدهای آنلاین در وب سایت [www.getsafeonline.org.uk](http://www.getsafeonline.org.uk)، و مرکز ملی امنیت سایبری [www.ncsc.gov.uk](http://www.ncsc.gov.uk) قابل دسترس است. معلومات بیشتر و حمایت از قربانیان آنلاین در [www.stoponlineabuse.org.uk](http://www.stoponlineabuse.org.uk) قابل دسترس می‌باشد. برای معلومات بیشتر و حمایت جهت مقابله و گزارش هر نوع خشونت جنسیتی، سو استفاده خانگی یا اذیت، به سازمان [www.refuge.org.uk](http://www.refuge.org.uk) پناهندگان و یا خط تلفونی ملی مبارزه با سو استفاده خانگی [www.nationaldvhelpline.org.uk](http://www.nationaldvhelpline.org.uk) 0808 2000 247 به تماس شوید.

اگر نگرانی جدی دارید و یا می‌خواهید یک جنایت را گزارش دهید، با پولیس به تماس شوید. 999 (عاجل) — 101 (عادی)

## اصطلاحات کلیدی

**مصونیت دیجیتالی** — شیوه ها و عادات که خود تان، دیگران و معلومات خصوصی تان را در حین استفاده از انترنت محفوظ نگهداری می‌کند.  
**ارتباطات میان فردی** — ارتباط داشتن با اثرات متقابل میان مردم  
**تهدید آنلاین** — یک خطر و یا مشکلی که باعث بروز یک واقعه یا عمل نامطلوب از طریق انترنت می‌گردد.  
**رمز عبور (Password)** — یک رشته از ارقام که اجازه دسترسی به سیستم و خدمات یک کمپیوتر را می‌دهد.  
**محفوظ بودن** — محفوظ و ایمن ماندن، در معرض خطر یا آسیب قرار نگرفتن

## مصونیت دیجیتالی چیست؟

مصونیت دیجیتالی به معنی آگاهی و شناخت از چگونگی حفاظت خود و معلومات تان از خطرات آنلاین می‌باشد. اغلباً مصونیت دیجیتالی تنها به مفهوم داشتن یک سری عادات خوب است که شما را در برابر جرایم سایبری، تقلب و تهدیدها کمتر مورد آسیب پذیری قرار می‌دهد.

این امر شامل شناختن بعضی از نیرنگ های می باشد که مجرمین می توانند جهت وادار کردن مردم در تسلیم نمودن معلومات و پول شان و یا در حمله نمودن به زندگی خصوصی شما از آن استفاده کنند.

رایج ترین انواع تهدید های آنلاین عبارت اند از:

- ویروس ها و نرم های افزار های مخرب که در تلاش سرقت (هک کردن) معلومات شخصی، جزییات حساب شما و یا نصب پروگرام های اند که بتوانند از شما تجسس کند.
- فریبکاری آنلاین که در آن مجرمین در تلاش قانع ساختن شما برای تسلیم دادن معلومات تان می باشد.

- قلدان و معتادین که از گمنامی آنلاین برای اذیت، سو استفاده و کنترل شما سود می برند.

تهدید های آنلاین اثر بالقوه به رفاه مالی، احساسی و شخصی شما دارد. با این تعادل فکری، آگاهی از مصونیت دیجیتالی مردم را در افزایش اعتماد شان به اینترنت کمک می کند.

## توصیه های ضروری مصونیت دیجیتالی

### داشتن رمز عبود (پسورد) قوی

ایمیل ها و تمام حساب های آنلاین دیگر با یک رمز عبور قفل می شوند. این یک راه حل کلیدی برای جلوگیری دیگران از دسترسی به حساب تان می باشد.

مغلق ساختن و قوی ساختن رمز عبور تان بهترین روش برای جلوگیری کسی است که می خواهد معلومات شخصی تان بدست بیاورد.

داشتن پسورد قوی ایمیل ضروری است. اگر یک هکر به ایمیل تان وارد شود، می تواند پسورد تمام حساب های دیگر را با استفاده از گزینه **Forgot password** دوباره تنظیم نموده و به تمام معلومات حساس خصوصی تان در تمام حساب های تان دسترسی پیدا کند.

هکرها می دانند که اکثریت ما پسورد های مانند 123456، یک تاریخ مهم در زندگی ما و یا نام یک کودک را استفاده می کنیم- چیزی را استفاده نکنید که به آسانی حدس زده می شود.

پسورد آسان به آسانی می تواند از بین برود اما یک پسورد خوب مانع دسترسی مجرمین می شود. ساختن یک پسورد قوی ارزش ضیاع وقت را دارد.

مراحل ذیل را برای ساختن یک پسورد قوی در نظر بگیرید:

1. سه کلمه تصادفی را برای ساختن عبارت (rugfirefork) متصل کنید: به طور مثال rug, fire, fork= rugfirefork

2. حروف بزرگ را علاوه کنید: به طور مثال RugFireForK

3. اعداد را علاوه کنید: به طور مثال 19RugFireForK90

4. سمبول ها را برای مغلق تر ساختن پسورد علاوه کنید: به طور مثال !19RugFireForK90!

هکر ها فهرست میلیون های رمز عبور سازشی (آسان) را شریک می سازند و 3 کلمه تصادفی یک روش آسانتر برای ساختن یک پسورد جدید است که برای شما بیشتر منحصر به فرد بوده و کمتر قابل حدس می باشد.

به شما شدیداً توصیه می گردد که به شکل دوره ای پسورد تان را تغییر دهید و از پسورد یکسان برای تمام حساب های تان استفاده نکنید. اگر شما در تلاش ساختن یک پسورد جدید هستید، یک مولد رمز عبور ([Password generator](#)) نیز یک انتخاب خوب است.

## ز بخش مدیر رمز عبور (Password manager) استفاده کنید

اگر شما نگران فراموش کردن یک رمز عبور قوی هستید، شما می توانید از مدیر رمز عبور استفاده کنید. بخش مدیر رمز عبور می تواند رمز عبور شما را در مرورگر اینترنت (مانند گوگل کروم و یا مایکروسافت ایج) ذخیره نماید که همین مرورگر رمز عبور تان را به یاد تان می آورد. آنها نسبت به استفاده رمز های عبور بد و یا ضعیف محفوظ تر هستند اما به یاد داشته باشید که در صورت مفقودی دستگاه تان از آنها حفاظت کنید. بعضی از شرکت های که در بخش نرم افزار های ضد ویروس و مصونیت آنلاین تخصص دارند، یک مدیر رمز عبور معیاری را تهیه خواهند کرد و اگر شما ابزار های نرم افزار ضد ویروس آنها را خریداری کنید؛ شرکت های دیگر خودشان مدیر رمز عبور را پیشکش می کنند.

## ترتیب نمودن تصدیق دو فاکتور

تصدیق دو فاکتور یک لایه محافظتی دیگر را به حساب تان اضافه می کند که این عمل با درخواست یک سری معلومات دیگر بر علاوه رمز عبور تان صورت می گیرد. این عمل مانع ورود دیگران به حساب تان میشود، حتی اگر آنها رمز عبور تان را داشته باشند. هدایات در مورد اینکه چگونه تصدیق دو فاکتور (Two Factor authentication) را برای ایمیل های مشهور و رسانه های اجتماعی تهیه کنیم را می توانید در وبسایت مرکزی مصونیت سایبری در [اینجا](#) بیابید.

## حفاظت دستگاه های تان در برابر ویروس ها

ویروس ها پروگرام های مخفی هستند که به وسیله وبسایت ها، لینک های ایمیل، ضمایم و یا واسطه های جدا شدنی (مانند USB) انتقال داده می شوند. آنها می توانند باعث اختلالات زیادی شوند و همچنان می توانند کمپیوتر و یا حساب های تان را مختل کنند، معلومات یا داتای تان را جهت استفاده یا فروش سرقت کنند، پول تان را اخذ کند و یا حتی شما را در خانه تان نظارت کنند. این نگران کننده است که همه افراد نمی دانند که چطور دستگاه های شان را از این تهدید ها حفاظت نمایند و کدام اقدامات را برای حفاظت دستگاه های شان انجام دهند. (ONS) در سال 2020 گزارش داد که از میان جوانان که تلفن های هوشمند دارند، تلفن 17% آنها امنیت ندارد و 32% شان نمی دانستند که آیا تلفن های شان امنیت دارند یا خیر.

نرم افزار ضد ویروس (anti-virus) همانند یک محافظ امنیتی، وسیله است که در لپ تاپ، تبلت و یا موبایل نصب شده و مشکلات که توسط پروگرام آلوده بوجود می آیند را متوقف می سازد. برنامه محافظتی ضد ویروس (anti-virus) برای یک کمپیوتر، لپ تاپ و یا تلفن هوشمند جهت جلوگیری از تهدیدهای ذیل مهم است:

- **تراجان ها (Trojans)** که خود را مانند یک برنامه که شما می خواهید دانلود کنید (مانند برنامه ضد ویروس، یک تصویر و یا یک فیلم رایگان) وانمود می کنند اما در حقیقت نرم افزار های مخرب بوده و زمانیکه شما آن را در تلفن یا کمپیوتر خود نصب می کنید فعال می شوند.
- **نرم افزار های جاسوسی (Spyware)** که معلومات را ردیابی می کنند و بخاطر مقاصد جرمی شما را نظارت می کنند که چی کاری را در کمپیوتر انجام می دهید.
- **ابزار های تبلیغاتی مزاحم (Adware)** که پنجره های غیر منتظره را باز می کنند تا سعی در فروختن معلومات تان کند.
- **رنزوم ویر (Ransomware)** که تلفن تان قفل نموده و از شما پول می خواهد.
- **هرزنامه (spam)** برنامه های را بنام کرم (worm) به وجود می آورد که به وسیله ارتباطات باز ویب وارد سیستم تان می شود و همچنان طوری عمل می کنند که ایمیل های نامطلوب هرزنامه را به مخاطبین تان ارسال می کنند. ارتباط ناخواسته از طریق ایمیل عبارت از هرزنامه و یا جنک ایمیل می باشد.
- ایمیل هرزنامه می تواند به شکل یک آزار و اذیت ساده باشد اما می تواند جهت فریب دادن مردم و پخش نمودن اطلاعات غلط استفاده شود.

اکثر سیستم ها از قبل دارای برنامه ضد ویروس (antivirus) و سیستم محافظت از نرم افزار های جاسوسی می باشند، به طور مثال لپ تاپ های دارای ویندوز 10 از قبل پدافندگر ویندوز (windows defender) را در می آورند.

شما می توانید نرم افزار های ضد ویروس (antivirus) اضافی را بدست بیاورید: این برنامه ها بعضی اوقات [رایگان](#) هستند اما هستند شرکت های که برنامه های دارای هزینه را تهیه می کنند.

نرم افزار های قدیمی شاید منفذ های داشته باشند که ویروس ها می توانند از طریق آن تحرکاتی داشته باشند. بروزرسانی ها (updates) به این منفذ ها کمک می کنند تا خود را ترمیم کنند. شما می توانید برنامه ها و نرم افزار های تان را طوری تنظیم کنید که به شکل خودکار هر منفذ داخل سیستم امنیتی تان را بروزرسانی نموده و آنرا ترمیم کند. این امر به منظور این است که

شما مجبور نخواهید بود تا آن را به یاد بیاورید. بعضی اوقات شما شاید مجبور شوید تا عملاً دستگاه را بروز رسانی کنید و اگر این چنین باشد، شما با یک تذکر (reminder) مواجه خواهید شد. از آنها چشم پوشی نکنید.

### معلومات تان را پشتیبانی کنید

ویروس ها می توانند داتا و معلومات را حذف و یا سرقت کنند. جهت حفاظت تصاویر، فایل ها و معلومات تان شما باید معلومات را قبل از بروز رسانی دستگاه تان پشتیبانی کنید. پشتیبانی به مفهوم ساختن یک کاپی از داتا می باشد که با استفاده از یک سخت افزار قابل حمل می توانید آن را از جایی به جای دیگر انتقال دهید اما روال معمول تر این است که در دستگاه دیگر داتا را در بخش حافظه آنلاین (cloud) ذخیره کنید. این عمل به این منظور است که بعضی اوقات بروز رسانی ها فایل ها را تغییر می دهد، اما اگر شما از معلومات پشتیبانی داشته باشید که بتوانید آن را به آسانی دوباره بدست بیاورید، در این صورت شما توسط حملات تهدیدآمیز تهدید نمی شوید. شما می توانید پشتیبانی خودکار را فعال بسازید که این عمل باعث می شود تا مجبور به پشتیبانی مداوم معلومات تان باشید.

هدایات بیشتر در زمینه پشتیبانی معلومات تان را می توانید در اینجا دریابید

[www.getsafeonline.org/protecting-your-computer/Backups](http://www.getsafeonline.org/protecting-your-computer/Backups)

### خلاصه

- یک رمز عبوری جداگانه را فقط برای ایمیل تان داشته باشید
- رمز عبور ایمیل و سایر حساب های تان را بررسی کنید که آیا مستحکم هستند
- ببینید که آیا طریقه تغییر دادن رمز عبور را می دانید و این کار را باید به طور منظم انجام دهید
- از رمز عبور یکسان برای چندین حساب استفاده نکنید و اگر نگران فراموش کردن رمز های عبور هستید، استفاده مدیر رمز عبور را در نظر بگیرید
- از تصدیق دو فاکتور استفاده کنید (Two Factor authentication)
- ببینید که آیا برنامه ضد ویروس فعال دارید (اگر مطمئن نیستید باید آن را تهیه کنید)
- از برنامه ضد ویروس استفاده نموده و آن را بروز رسانی کنید- به طور منظم سیستم تان را اسکن کنید و برنامه ضد ویروس را به منظور مقابله با ویروس های پیشرفته و اشکالات جدید بروز رسانی کنید.
- در مورد چیز های که دانلود می کنید محتاط باشید - اعلانات و نرم افزار های جاسوسی با پیوستن به چیز های که شما دانلود می کنید وارد کامپیوتر تان می شوند بنا جایی را که می خواهید فایل های تان را بدست بیاورید را بررسی کنید.

### اگر کار به درستی پیش نرود چی اقدامی باید کرد

اگر شما در لپ تان یک لینک را باز کرده اید و یا برای نصب چیزی هدایات را تعقیب کرده اید اما شک دارید، در این صورت نرم افزار ضد ویروس را باز کنید و اسکن کامل بکنید. به نرم افزار ضد ویروس اجازه دهید مشکل را ترمیم کرده و دستگاه تان را به وسیله هدایات که خودش می دهد به حالت اول آن برگرداند. اگر مشکل مرفوع نمی گردد شما باید کمک تخصصی بگیرید.

دوست نزدیک تان به شما تماس می گیرید و غمگین به نظر می رسد. او فایلی را که که گمان می کرد یک تصویر بود، را در یک ایمیل باز کرد. او در واقع یک اسب راجان (Trojan horse) بود که نرم افزار تهدید کننده (ransomware) را مخفی نموده و فعلاً آنها به کامپیوتر شان وارد شده نمی توانند. در این حالت شما چی می کردید، و به آنها چی توصیه می کردید تا انجام دهند؟

اگر شما با یک پیام تهدیدی آمیز مواجه شدید، آگاه باشید که اگر شما به آنها پول بدهید، این امر می تواند یک فعالیت جنایی را تمویل کند و هیچ ضمانتی هم وجود ندارد که شما به دستگاه تان دسترسی پیدا کنید؛ این عمل سودی به شما نداشته و این احساس را شما می دهد که در آینده هم شما به آنها پول می دهید و منتظر حملات بعدی هستید.

### انواع رایج تهدید آنلاین

فریبکاری و کلاهبرداری

کلاهبرداری عبارت از روش است که برای برای فریب دادن یک شخص جهت اخذ پول و یا وادار نمودن اشخاص برای تهیه جزییات معلومات شخصی شان می باشد، که بدینوسیله یک جنایتکار می تواند آن معلومات و هویت حساب شان را سرقت کند این می تواند شامل استفاده از ویروس ها جهت سرقت معلومات از کمپیوتر و یا حساب آنلاین اشخاص باشد و یا آنها را با فریب و نیرنگ وادار کند تا به خواست خود پول را تسلیم کند.

کلاهبرداری معمولا از طریق ایمیل های ساختگی (phishing)، پیام های نوشتاری (smishing)، و یا تماس صوتی (vishing) انجام می شود. ایمیل ها و متن ها احتمالا یک رابطه با ویسایت ها جعلی دارند که شما را وسوسه می کنند تا معلومات شخصی تان را وارد کنید و یا مانند یک دهلیز عمل کرده و به ویروس ها اجازه می دهند تا وارد کمپیوتر تان شوند. و یا آن ایمیل یک الصاق دارند که دارای یک ویروس است که جزییات بانکی، معلومات شخصی یا تصاویر را سرقت می کنند.

کلاهبرداری شما را وادار می کند تا فکر کنید که از یک سازمان که می شناسید برای تان تماس گرفته اند و یا بعضی اوقات کسی که به کمک ضرورت دارد. آنها طوری طراحی شده اند که شما در آن احساس می کنید تحت فشار قرار دارید تا به سرعت کاری انجام دهید، یک لینک را باز کنید، جزییات بدهید و یا روی یک الصاق کلیک کنید. به چنین چیزی باور نکنید.

ما در اینجا وقت کافی برای لیست نمودن تمام انواع کلاهبرداری و فریبکاری را نداریم. معلومات بیشتر در مورد انواع کلاهبرداری های که جنایت کاران استفاده می کنند و همچنان توصیه های در مورد اینکه چگونه فریبکاری و جرایم سایبری را گزارش دهیم را می توانید در اینجا دریابید: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

### ایمیل های جعلی (phishing)

ایمیل های جعلی یک نوع فریبکاری می باشند که در آن یک جنایتکار سایبری از یک دام برای اغوا کردن افراد جهت تهیه معلومات شخصی، بانکداری یا جزییات کارت بانکی، جزییات حساب و رمز عبور شان استفاده می کنند. بعدا آنها از این معلومات جهت دسترسی به حساب های تان، سرقت پول تان، ایمیل نمودن به مخاطبین شما از طرف شما و یا دزدیدن هویت تان استفاده می کنند. جنایتکاران شاید یک ایمیل جعلی را به هزاران شخص بفرستند به امید اینکه تعداد کمی از افراد فریب خورده پول یا معلومات شان را به جنایتکاران می دهند.

هکر ها و کلاهبرداران یک نقش بسیار خوبی را بازی خواهند کرد تا طوری وانمود کنند که شخص یا سازمان مورد اعتماد شما می باشند، و شاید آنها حتی نام و سایر معلومات شخصی تان را استفاده کنند تا شما متقاعد بسازند. آنها کوشش خواهند کرد تا شما را با یک پیشنهاد وسوسه کنند و یا با یک تهدید شما را طعمه خود بسازند. به طور مثال، شاید وانمود کنند که از دفتر مالیات حکومت با شما به تماس شده و پیشنهاد بازپرداخت پول به شما میکنند، اما آنها شما را ملزم به تهیه نمودن جزییات بانکی تان می کند تا برای تان پول بپردازند. آنها با گفتن اینکه شما باید پول بپردازید در غیر صورت به محکمه فراخوانده می شوید، می توانند وانمود کنند که شورای محلی شما میباشد، و یا می توانند وانمود کنند که بانک و یا واسطه بانکی شما هستند مانند پی پال (PayPal) و اینکه شما از استفاده حساب بانکی خود محروم هستید.

[این ویدیوی پولیس شهری را که در مورد ایمیل جعلی \(phishing\) میباشد، تماشا کنید.](#)

نگاه کردن به ایمیل آدرس فرستنده، نه تنها چیزی که در بخش ('From') میباشد، یک راه سریع است برای چک نمودن اینکه واقعا کی ایمیل را فرستاده و آیا این امر یک فریبکاری ایمیل جعلی محسوب می شود یا خیر.

یک پیام واقعی معمولا از آدرس قابل تشخیص یک سازمان دریافت می گردد (به طور مثال [noreply@yourbank.com](mailto:noreply@yourbank.com)) اما کلاهبرداران و جنایتکاران نمی توانند از نام اصلی بانک و یا سازمان شما استفاده کنند، بنا اکثر ایمیل آدرس با حروف تصادفی و اعداد تکمیل میشود (به طور مثال [noreply@1234bank12.com](mailto:noreply@1234bank12.com)) اگر ایمیل از یک آدرس شخصی است (به طور مثال [person@gmail.com](mailto:person@gmail.com)) بعید است که از سازمان رسمی باشد - حتی گوگل از نشانه (@gmail) برای ارسال ایمیل های سازمانی استفاده نمی کند.

با نگاه کردن به این مثال شما می توانید مشاهده کنید که اگرچه ایمیل ذیل از پی پال (PayPal) به نظر میرسد، اما در واقع از یک نشانی دیگر می باشد: [Paypal@notice-accessxxx.com](mailto:Paypal@notice-accessxxx.com)

— Forwarded Message —  
From: PayPal <paypal@notice-access-273.com>  
To: [REDACTED]  
Sent: vivesday, 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.

محتاط بودن در مورد ایمیل های که بسیار خوب به نظر می رسند، و یا درنگ کردن بخاطر گرفتن یک تصمیم سریع حتی وقتی که ایمیل ها از نشانی درست استفاده نموده و قانونی به نظر میرسند، خالی از ارزش نیست. آرامش خود را حفظ کنید و از چیزی که دریافت کرده اید تحقیق کنید. جواب ندهید و هیچ لینک را کلیک نکنید. اگر یکبار لینک را باز کردید، ویروس ها شاید در کمپیوتر تان نصب شده و معلومات را سرقت کنند، و یا شما به یک وب سایت جعلی و مخرب تغییر مسیر داده می شوید و از شما خواسته شود تا جزییات بانکی و حساب تان را وارد کنید که ممکن است در آینده سرقت شود.

## شناسایی ایمیل های جعلی و تقلبی

- آیا شما فرستنده را می شناسید؟ آیا آنها شما را با یک رویه معمولی مورد خطاب قرار می دهند؟
- آیا اشتباهات املائی در ایمیل وجود دارد و یا متن آن دارای محتوای ضعیف می باشد؟
- آیا فرستنده ایمیل می خواهد شما چیزی انجام دهید؟ آیا کدام احساس فوریت وجود دارد؟ آیا شما را تهدید می کند؟
- ایمیل آدرس که پیام از آن برای تان فرستاده شده را باز کنید. آیا ایمیل آدرس مذکور نام اصلی درست دارد؟
- آیا این غیرمنتظره است که شما ایمیل را از از شرکتی دریافت می کنید که کاری با آن ندارید؟
- اگر ایمیل شما را به یک وبسایت رهنمایی می کند، آیا کدام علامه قفل و <https://> در آغاز آدرس وب سایت نیست؟

راهنمایی های بیشتر در مورد شناسایی ایمیل های جعلی را می توانید در اینجا پیدا کنید: [www.ncsc.gov.uk](http://www.ncsc.gov.uk)

زهر را یک ایمیل را که فکر می کند از از بانک است دریافت می کند - هنگامیکه ایمیل را باز می کند میبیند که آنها می گویند که موقتاً حساب وی توسط آنها معلق گردیده است. زهر را با ترس و وحشت متوجه می شود که بانک فعالیت غیرعادی را در حساب بانکی وی پیدا کرده و تصمیم می گیرد تا برای محافظت خود آن فعالیت را متوقف سازد. ایمیل می گوید که زهر را تا وقتی که به سیستم وارد شده و دوباره آنرا فعال نکند، نمی تواند از حساب بانکی خود استفاده کند و همچنان از او می خواهد تا روی یک لینک کلیک کند. زهر را می داند که فردا باید کرایه خانه با بپردازد، و باید فوراً به حساب خود دسترسی پیدا کند، اما او مشکوک است.

## زهر را برای مشوره به شما زنگ میزند: شما به او چی میگویید و چگونه او را مشوره می دهید؟

لینک می تواند خطرناک باشد. این کار میتواند به این منظور باشد که هکر ها تلاش خواهند کرد تا چیزی را در کمپیوتر زهر را برای دلایل جنایی نصب کنند، مثلاً جهت سرقت معلومات یا هک کردن حساب های ایمیل، بانک و یا رسانه های اجتماعی. و یا لینک میتواند او را به وب سایت دیگری ببرد (مثلاً یک نسخه جعلی بانک) که احتمالاً از او آی دی، رمز عبور و جزییات بانکی را بخواهد. اگر او این معلومات را به وب سایت بدهد، یعنی خودش با دست خود حساب بانکی و پولش را به کلاهبرداران میدهد. بانک خود تان بخاطر جزییات شخصی تان توسط ایمیل، زنگ و پیام نوشتاری با شما تماس نخواهد گرفت.

اگر شما گاهی تردید دارید که آیا واقعا بانک خود تان برای تان تماس گرفته، و این یک فریبکاری صوتی نیست، تماس را خاتمه دهید و شماره خدمات مشتریان بانک را آنلاین جستجو کنید. قبل از تماس دوباره برای 5 دقیقه منتظر بمانید و یا از تلفن دیگری استفاده کنید چونکه کلاهبرداران می توانند خطوط تلفونی را بربایند.

بعد از صحبت کردن با شما:

زهره در اینترنت به دنبال شماره تماس خدمات مشتریان بانک می‌رود. بانک تایید می‌کند که این ایمیل جعلی بوده و حساب او مشکلی ندارد. آنها به او می‌گویند که لینک این ایمیل به وب سایت که گمان می‌شود وب سایت بانک است، رفته است. این بعضی اوقات برای قربانیان این نوع فریبکاری مشکل بوده می‌تواند تا پول شان را پس بگیرند، آن هم در صورتی که بانک متوجه شود در این موضوع خود بانک محتاط نبوده است.

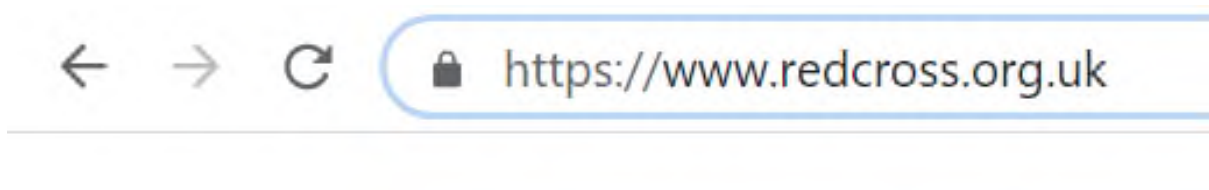
اطلاعات بیشتر در مورد ایمیل جعلی و کلاهبرداری در مرکز ملی امنیت سایبری می‌تواند دریافت گردد.

[www.ncsc.gov.uk/guidance/phishing](https://www.ncsc.gov.uk/guidance/phishing)

## وب سایت های محفوظ و غیر محفوظ

خیلی مهم است که هر وب سایتی را که بازدید می‌کنیم بتوانیم آنرا بررسی کنیم که آیا ایمن هست یا خیر. هر وب سایتی را که بازدید می‌کنید شاید ناامن ثابت شود، یا هکر های که به شما ایمیل های جعلی ارسال می‌کنند شاید شما را به وب سایتی جعلی هدایت کند که بسیار واقعی به نظر می‌رسد.

به این نشانی قفل  و یا این حروف <https://> در مرورگر تان نگاه کنید که به مفهوم مصون بودن وب سایت می‌باشد.



بعضی اوقات شما هم نشانی قفل و https را می‌بینید، و یا تنها نشانی قفل را می‌بینید، این بستگی به کمپیوتر یا مرورگر تان دارد. یک وب سایت که تنها http دارد شاید محفوظ نباشد بخاطریکه (s) نشان دهنده ایمن بودن می‌باشد.

اگر از شما تقاضا می‌گردد تا وارد یک حساب شوید، و یا جزییات پرداخت یا هر معلومات دیگر را تهیه کنید، خود را مطمئن بسازید که هر وب سایتی را که استفاده می‌کنید باید حروف "https" را در آغاز آدرس در مرورگر داشته باشد. جزییات ورود به سیستم تان را فقط وقتی وارد کنید که از بودن در وب سایت درست مطمئن هستید.

همیشه برای بازدید از صفحه اینترنتی بانک تان آدرس کامل وب را تایپ کنید، مخصوصا وقتی که به بانکداری آنلاین وارد می‌شوید. هرگز از ماشین جستجو برای دسترسی به وب سایت بانکی تان استفاده نکنید، زیرا این عمل می‌تواند توسط هکر ها جهت سازش با امنیت و سرقت جزییات تان استفاده شود.

## اقدام بر علیه ایمیل جعلی و سایت های کلاهبرداری

کوشش کنید تا خود را محافظت کنید و هدایات ذیل را به خاطر بسپارید:

- نرم افزار مرورگر، نرم افزار ضد ویروس و نرم افزار جاسوسی تان را بروز نگهدارید.
- از مراجعه به وب سایت های ریسک دار و آنهایی که نشانی قفل ندارند، جلوگیری کنید
- هرگز به یک لینک در ایمیل که از مرجع ناشناخته و مشکوک است، کلیک نکنید
- هرگز جزییات شخصی، رمز عبور و یا کد های امنیتی تان را از طریق ایمیل یا تلفون ندهید.

## وقتی که توسط یک کلاهبردار مورد هدف قرار می‌گیرید چی باید کرد

ایمیل، تماس صوتی، پیام صوتی و یا وب سایت را گزارش دهید.

اگر ایمیلی را دریافت می کنید و نسبت به آن مطمئن نیستید، می توانید آنرا به خدمات گزارش دهی ایمیل مشکوک (SERS) در [report@phishing.gov.uk](mailto:report@phishing.gov.uk) ارسال کنید. در صورتی که این یک ایمیل جعلی باشد و یا به نظر میرسد، آنها به شما مشوره میدهند.

اگر یک پیام نوشتاری مشکوک را دریافت می کنید، میتوانید به طور رایگان به شماره 7726 ارسال کنید. این امر به ارایه دهنده تلفون تان اجازه می دهد تا متن را بررسی کرده و در صورتی که کلاهبرداری باشد اقدام کند.

جزییات تان شریک نسازید بلکه در عوض همیشه آنرا چک نمایید. هرگز به شماره که در ایمیل است، تماس نگیرید و به روی لینک ها کلیک نکنید چونکه آنها می توانند شما را به یک حساب جعلی دیگر سوق دهند. در عوض به اینترنت بروید و شماره شناخته شده را پیدا کرده و با آن شماره به تماس شوید.

لینک ها را بدون پرسیدن اینکه شما را به کجا میبرند تعقیب نکنید. برای چک نمودن اینکه یک وب سایت واقعی است، مرورگر اینترنت را باز کنید و مستقیم نام را در میله (URL Bar) تایپ کنید.

هرگز رمز عبور و یا پین نمبر (Pin Number) تان را با کسی شریک نسازید. مهم نیست کسی که رمز عبور تان را می خواهد مادر و یا بهترین دوست تان است – رمز عبور تان را فاش نکنید.

اگر فریب خورده و جزییات بانکی تان را به کسی دادید، یکبار به بانک تان تذکر دهید.

اگر پول تان را از دست دادید، به بانک تان تذکر دهید و این عمل جرمی را به اقدام علیه فریبکاری (در انگلستان، ولز و ایرلند شمالی) و یا پولیس اسکاتلند (در اسکاتلند) گزارش دهید. با این کار شما به دیگران نیز کمک می کنید تا قربانی چنین کاری نشوند.

اقدام علیه فریبکاری [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

## روابط آنلاین

در این بخش در مورد تاثیر اینترنت در روابط شخصی بحث خواهیم کرد. فعالیت های را که بصورت آنلاین انجام میدهم میتواند مستقیما زندگی خصوصی ما را تحت تاثیر قرار دهد. بنابراین بسیار مهم است تا در قسمت شریک ساختن معلومات که با سایر اشخاص در اینترنت، محتاط باشیم.

ما همه می خواهیم تا با مردم در ارتباط باشیم، و این یکی از بهترین مزایای اینترنت است که به آسانی با دوستان، خانواده و مردم که در سراسر جهان با آنها علایق یکسان داریم، ارتباط برقرار کنیم. در عین زمان، مهم است تا بدانیم که ارتباطات آنلاین باید به طور دقیق مدیریت شود، مانند ملاقات با کسی در جاده، و اینکه دیگران شاید بخواهند تا با هدف بد با مردم ارتباط برقرار کنند که این حالت شاید منجر به سو استفاده شود.

سو استفاده آنلاین می تواند از جانب یک بیگانه و یا کسانی که شما میشناسید باشد. ما بعضی از مثال های سو استفاده میان فردی آنلاین را ذیلا به بحث می گیریم.

## فریبکاری عاشقانه

فریبکاری عاشقانه عبارت از عملی می باشد که کسی از یک وب سایت آنلاین و یا یک اپلیکیشن (app) استفاده می کند – یک رابطه میان فردی را ایجاد میکند تا اعتماد شخص مورد نظر را به دست بیاورد و بعدا پول و معلومات خصوصی را می خواهد. آنها احتمالا از پروفایل (profile) جعلی برای تشکیل دادن رابطه استفاده می کنند و آنها می توانند واقعی و مهربان به نظر برسند. اکثر اوقات این گونه اشخاص سوالات شخصی زیادی را می پرسند، اما در مورد خود چیز های زیادی نمی گویند. آنها منتظر میمانند تا وقتی که مطمئن شوند که آنها اعتماد را بوجود آورده و از وابستگی های احساسی برای کمک، معمولا پول، استفاده می کنند. آنها شاید تصاویر اشتباه خود شان را ارسال کنند، که اکثرا از جایی دیگر در اینترنت اخذ می گردد.

هرگز به کسی که آنلاین ملاقات می کنید پول را مبادله نکنید و یا جزییات بانکی تان را ندهید، مهم نیست که شما چقدر به آنها و به داستان شان باور دارید.

احساس فریب خوردن در رابطه و دوستی آنلاین می توانند واقعا ناراحت کننده و شرم آور باشد، اما شما می توانید آن را به اقدام علیه فریبکاری [www.actionfraud.police.uk](http://www.actionfraud.police.uk) گزارش دهید یا به شماره 0300 123 2040 به تماس شوید.

برای چک نمودن منبع یک تصویر شما می توانید یک جستجوی معکوس تصویر را انجام دهید که نظر به نام می توانید تصاویر مشابه به تصویر اصلی را در اینترنت دریابید. شما در [اینجا](#) می توانید جستجوی معکوس تصویر را انجام دهید.

## قلدری سایبری

قلدری سایبری یک اصطلاح معمول برای قلدری و اذیت آنلاین و یا با استفاده از تکنالوژی است. قلدری سایبری هرگونه سو استفاده آنلاین را شامل می شود که قصدا باعث ضرر، پریشانی یا خسارت شخصی دیگران می شود. اکثرا قلدران از سایت های شبکه های رسانه های اجتماعی مانند فیسبوک با تویتر، انجمن های تعاملی و پیام رسانی استفاده می کنند. قلدری سایبری مخصوصا می توانند ناراحت کننده باشند بخاطریکه به وسیله اینترنت و موبایل ها، نه تنها در حالات مشخص مانند مکتب یا کار، در هر زمانی می توانند به مردم دسترسی پیدا کنند.

اگر کسی موضوعات اشتباه و یا مخرب را در مورد شما در اینترنت یا در رسانه های اجتماعی پست می کند، این عمل می تواند اذیت تلقی شود که خود یک نوع جرم است. همچنان اگر شما تماس های تهدید آمیز و ترساننده دریافت می کنید، فاعلین چنین اعمال مرتکب عمل جنایی می شوند.

قلدری می تواند هر کسی را به شمو اطفال و جوانان تحت تاثیر قرار دهد، اما این زمانی بسیار مهم است که شما والدین و سرپرست اطفال هستید. اگر شما، طفل تان و یا کسی که میشناسید مورد قلدری، به شمول قلدری آنلاین، قرار می گیرد، می توانید به [خط تلفونی ملی مبارزه علیه قلدری](#) جهت مشوره با شماره **0300 323 0169** تماس بگیرید.

## بهره برداری (استثمار)

استثمار به چیزی گفته می شود که وقتی کسی با اشخاص دیگر رابطه مملو از اعتماد را می سازد تا بتواند از آنها بهره برداری نموده و کنترل شان کند. نگرانی ویژه در مورد استثمار آنلاین اطفال و جوانان وجود دارد، تا آنجایی که یک کودک برای اهداف چون سو استفاده جنسی (آنلاین و یا حضوری)، قاچاق مواد مخدر و یا سایر اهداف استثماری مورد بهره برداری قرار گرفته می تواند.

استثمار می تواند در محدوده زمانی کوتاه و یا طولانی اتفاق بیفتد و استثمارگران با خانواده طفل رابطه ایجاد می کنند تا در نظر آنان قابل اعتماد، با اعتبار و کمک کننده به نظر برسند. هرکسی بدون توجه به نژاد، جنس، سن و یا رابطه می تواند نسبت به یک طفل استثمارگر باشد.

استثمار می تواند به شکل آنلاین اتفاق بیفتد جایی که استثمارگران خود را به حیث همکار و همتا به طفل معرفی می کنند و تصاویر یا ویدیو های سایر اشخاص را برای شان ارسال می کند. آنها شاید با استفاده از بازی ها، نصیحت کردن، نشان دادن تفاهم و خریدن تحایف برای اشخاص جوان، جایگاه خود را به حیث یک دوست قابل اعتماد مستحکم بسازند، و یا کوشش به جدا ساختن طفل از خانواده و دوستانش کند، و یا با تهدید کوشش به شرماندن طفل بخاطر تنبلی وی کند و یا مفکوره اسرار را جهت کنترل طفل برایش معرفی نماید.

معلومات بیشتر در مورد استثمار در وب سایت [www.nspcc.org.uk](http://www.nspcc.org.uk) در کنار منابع دیگر که در مورد چگونگی صحبت کردن با طفل در باره سو استفاده و تهدید های آنلاین می باشد، قابل دسترس می باشد.

اگر شما گمان می کنید که یک طفل در خطر است، از زنگ زدن به پولیس دریغ نکنید. شما همچنان می توانید به [NSPCC](#) جهت مشوره و حمایت برای گزارش سو استفاده آنلاین به تماس شوید.

## سکستینگ و سکس انتقام جویانه

سکستینگ به مفهوم ارسال یک پیام، تصویر و یا ویدیو سکسی به شخص دیگر می باشد. یک شخص شاید یک تصویر خود و یا از کسی دیگر را ارسال کند. یک پیام سکسی (sexting) می تواند به یک دوست، همکار و یا کسی دیگر به شکل آنلاین باشد، و شاید برهنگی نیمه یا کامل، قرار گرفتن در حالت واضح سکسی و یا صحبت نمودن در مورد اعمال سکسی را در بر بگیرد.

در حالیکه یک پیام سکسی می تواند میان دو طرف موافق رد و بدل شود، تصاویر می توانند بدون رضایت شخص فاعل به سرعت در اینترنت منتشر شوند. وقتی که کسی تصویر یا ویدیو منتشر شده را داشته باشد، به هر کسی می تواند ارسال کنند. سکس انتقام جویانه چیزی است که وقتی کسی تصویر خصوصی جنسی یک شخص را به شخص دیگر نشان می دهد یا منتشر می کند، البته بدون رضایت شخص و به نیت پریشان ساختن آنها.

تهدید نمودن اشخاص به فاش نمودن معلومات خصوصی و تصاویر شان همچنان تهدید و عمل جرمی محسوب می شود.

معلومات بیشتر در مورد سکس انتقام جویانه در اینجا در دسترس است: خط تلفون سکس انتقام جویانه - 0845 6000 459

[www.revengepornhelpline.org.uk/](http://www.revengepornhelpline.org.uk/)

این هرگز برای کسی خوب نیست که کسی دیگر را جهت ارسال تصاویر برهنه تحت فشار قرار دهد.

این موضوع مهم است تا بدانید که تصاویر ارسال شده، حتی با استفاده از خدمات مانند اسنپ چت (snapchat)، می توانند اسکرین شات شده و ذخیره شوند. اگر شما یک تصویر برهنه یا سکسی را ارسال کرده اید و نگران هستید که چی اتفاق خواهد افتاد، می توانید از هدایات ذیل را انجام دهید:

- از جانب مقابل بخواهید تا تصاویر را حذف کند.
  - به تهدید ها پاسخ ندهید.
  - با کسی صحبت نموده و کمک بخواهید. شما می توانید به [خط تلفونی سکس انتقام جویانه](#) تماس بگیرید.
  - چیزی که اتفاق افتاده را گزارش دهید. شما می توانید وب سایت که تصویر در آن به نشر می رسد را گزارش دهید.
- اکثر سیستم عامل های رسانه های اجتماعی ابزاری را جهت گزارش محتوا دارند. شما همچنان این نوع اذیت را به پولیس گزارش دهید. اگر عاجل نیست به شماره 101 به تماس شوید.

این مهم است تا آگاه باشد که شریک ساختن تصویر برهنه به اشخاص پایین تر از 18 ساله نظر به قانون اعمال جنسی مصوب 2003 سو استفاده از طفل و عمل جرمی محسوب می شود.

عملی مانند عبور از پیام های سکسی شخص کمتر از 18 سال منجر به تحقیقات پولیس شده می تواند.

اگر شما نگران شریک ساختن تصاویر اطفال توسط دیگران هستید و یا نگرانی های دیگر در مورد محافظت اطفال در اینترنت دارید، می توانید به مرکز مصونیت اطفال از استثمار آنلاین گزارش دهید. [www.ceop.police.uk](http://www.ceop.police.uk)

## کمین های سایبری و نظارت

کمین عبارت از خصوصیات رفتاری یک شخص دیگر است و شما را بیمناک میسازد که مورد خشونت قرار می گیرید و باعث پریشانی شما شده و تاثیر جدی به فعالیت های روزانه تان دارد.

زمانیکه این عمل به شکل آنلاین اتفاق می افتد بنام کمین سایبری یاد می شود.

این می تواند معلومات تان را جمع آوری کند، هویت تان را جعل کند، پیام های ناخواسته و تهدید کننده را ارسال کند، شما را تماشا کند و یا به حساب آنلاین تان دسترسی پیدا کرده و معلومات نادرست در مورد تان منتشر کند.

یک کمین گر می تواند یک بیگانه یا شخص معلوم برای تان باشد. کمین سایبری تاثیری جدی روی هدف دارد و یک حمله جرمی محسوب می شود.

خط تلفون ملی کمین سایبری - 0808 802 0300

[www.stalkinghelpline.org/faq/about-the-law/](http://www.stalkinghelpline.org/faq/about-the-law/)

اگر نگران هستید که شما توسط یک سو استفاده کننده کمین شده اید و یا آنها شما را تماشای می کنند:

- از درگیر شدن با کمین گر جلوگیری نمایید که اکثرا این افراد می خواهد تا با شما صحبت نموده و یک رابطه میان تان ایجاد کند
- هرگز برای ملاقات و مواجه شدن با آنها موافقت نکنید.
- این موضوع را جدی گرفته و به پولیس گزارش دهید. شما می توانید به شماره 101 جهت صحبت نمودن مستقیم با پولیس به تماس شوید. اما اگر فکر می کنید که یک تهدید فوری و عاجل است به شماره 999 تماس بگیرید.
- تنظیمات حریم خصوصی تان را همیشه چک کنید، خود را مطمئن بسازید که حد اقل معلومات آنلاین قابل دسترس است یا خیر؟ و بخش موقعیت یابی را در دستگاه تان خاموش کنید.
- مردم اطراف تان را نیز آگاه بسازید. آنها شاید به چک نمودن چیز های که در مورد شما شریک ساخته می شود و یا ضرورت دارند، مجبور شوند. شاید شما مجبور شوید تا تنظیمات حریم خصوصی را هم چک کنید.
- یک سابقه از کار های که انجام می شود را نگهداری کنید - شما شاید بخواهید تماس های صوتی، پیام ها و یا پست های رسانه های اجتماعی تان را اسکرین شات بگیرید، به این مفهوم که در صورتی که عاملان پست ها و پیام های شان را بعدا حذف می کنند شما یک کاپی از شواهد را دارید.

### سو استفاده خانگی، اذیت و نظارت

- یک شخص سو استفاده جو به طور بالقوه از ویژه گی های دستگاه دارای اینترنت می تواند جهت تماشای، چک و کنترل نمودن یک هدف سو استفاده کند.
- این شامل نظارت بر مکاتبات شما با سایر مردم، پیگیری موقعیت شما از طریق دستگاه تان و یا چک نمودن مصارف مالی تان بوده می تواند.
- زمانیکه چنین اعمالی توسط همکار، همکار سابق، اعضای خانواده یا سرپرست انجام می شود، تمام آنها نظر به قانون بریتانیا انواع سو استفاده خانگی محسوب می شوند.
- اگر شما نگران هستید که کسی شاید موبایل و یا هر دستگاه دیگر تان را نظارت می کند، خط تلفونی ملی سو استفاده خانگی یک ابزاری به نام [walk-through tool](https://www.nationaldomesticviolencehelpline.org.uk) دارد برای کمک به شما جهت تغییر تنظیمات تلفون تا آنرا محفوظ تر بسازد.

خط تلفونی ملی سو استفاده خانگی (24 ساعت) 0808 220 0247

[www.nationaldomesticviolencehelpline.org.uk](https://www.nationaldomesticviolencehelpline.org.uk)

آیا شما با جملات ذیل موافق هستید؟

**تهدید های آنلاین واقعا مهم نیستند زیرا این جهان واقعی نیست.**

نخیر. سو استفاده آنلاین جدی است، تاثیر جدی روی زندگی انسان ها دارد و باید همیشه توسط مقامات جدی گرفته شود. کمین کردن، نظارت و اذیت همه رفتار های دارای ریسک بلند هستند که شما در آن تقصیری ندارید. شما حق دارید آنرا گزارش دهید، به دنبال مشوره باشید و برای دادن آدرس مرتکبین حمایت شوید.

**جنایت اذیت به مفهوم تهدید شدن با خشونت در زندگی واقعی می باشد.**

قانون تصریح می کند که اذیت وقتی اتفاق می افتد که کسی به طوری رفتار می کند تا موجب پریشانی و بیم به شما می گردد و این رفتار بیشتر از یک بار اتفاق می افتد. این عمل می تواند انواع مختلف رفتاری در موارد جداگانه باشد. به طور نمونه، یک پیام که به قصد پریشانی شما می باشد اذیت محسوب نمی شود. دو پیام می تواند اذیت تلقی شود، و یا ایمیل تهدید آمیز که به تعقیب تماس تلفونی می آید، شاید اذیت محسوب شود. فعالیت های دیگر که اذیت محسوب می شوند، شاید وقتی که کسی شما را تعقیب می کند، کسی خانه یا کار تان را نظارت می کند، دارایی تان خساره می بیند و یا کسی به اشتباه و به نیت بد شما را به پولیس گزارش می دهد، در حالیکه هیچ کاری انجام نداده اید.

زهره یک دختر خاله دارد که با او بسیار صمیمی است. در این اواخر دختر خاله زهره رفتارهای متفاوت می کند مثلا غمگین و زود رنج به نظر میرسد و زمانی که آنها با همدیگر می باشند همیشه با پریشانی تلفونش را چک می کند. بلاخره دختر خاله زهره می گوید که او خیلی وقت درست نخوابیده و تهدیدهای شوهر سابقش که می خواهد از او جدا شود پریشانش می کند. شوهر او به شکل مداوم برایش ایمیل می فرستد برای گفتن اینکه او یک زن و مادر بد است و مایه شرم به هردو خانواده است و باید برگردد و با او زندگی کند. دختر خاله زهره در این خصوص خیلی پریشان است.

او بیشتر توضیح می دهد که شوهر قبلی او یک تصویر برهنه او را دارد که قبلا زمانیکه رابطه شان خوب بود گرفته شده بود. شوهرش او را تهدید کرده است که در صورت عدم برگشت، آن تصویر برهنه را به فامیلش ارسال می کند.

### آیا دختر خاله زهره قربانی یک جرم است؟

بلی. دختر خاله زهره یک قربانی اذیت و کنترل اجباری است. این تهدیدها در برابر دختر خاله زهره به منظور بکار بردن کنترل نسبت به او استفاده می شود. قانون تصریح می دارد که این حمله وقتی اتفاق می افتد که یک شخص طوری رفتار می کند تا از روی قصد پریشانی و وحشت را ایجاد کند. این رفتار باید بیشتر از یک بار اتفاق بیفتد.

چون این رفتار توسط شوهر قبلی او انجام می شود، این نوع اذیت یک نوع کنترل اجباری (سو استفاده خانگی) محسوب می شود. این یک عمل جنایی است. او می تواند به پولیس گزارش دهد.

این همچنان یک تهدید سس انتقام جویانه است که با شریک ساختن تصاویر سکسی بدون رضایت شخص و با نیت ایجاد تحقیر و پریشانی در او انجام می شود. نفس عمل یک حمله نیست، در حالیکه اگر شوهر قبلی دختر خاله زهره این تصویر را از طریق ایمیل و یا رسانه های اجتماعی به شمول WhatsApp یا خدمات پیام رسانی دیگر شریک می ساخت، این می تواند یک عمل جنایی محسوب شود. شوهر دختر خاله زهره همچنان در مورد عزت خانواده و اینکه جدایی آنها مایه شرم خانواده های شان است، صحبت می کند. اصطلاح خشونت ناموسی یک نوع از سو استفاده است و زهره شاید بخواهد حمایت یک سازمان را که تخصص آن کار کردن با قربانیان سو استفاده ناموسی و تهدید می باشد، بدست بیاورد. کارما نیروانا Karma Nirvana روز جمعه به این خط تلفونی مراجعه کرد. 0800 5999 247

[www.karmanirvana.org.uk](http://www.karmanirvana.org.uk)

## خلاصه

- قبل از پست نمودن فکر کنید. چیزی را بدون در نظر گرفتن اینکه اگر به دسترس اشخاص بد قرار بگیرد چی احساس خواهید داشت، آپلود نکنید. یک بار که شما چیزی را پست می کنید کنترل آنرا از دست می دهید، مخصوصا اگر کسی دیگر آنرا اسکرین شات کند.
- را در رسانه های اجتماعی شریک نسازید. رسانه اجتماعی برای در ارتباط بودن با دوستان و فامیل عالی است اما در این مورد فکر کنید که آیا چیزی از بیشتر از خواست تان را به شاید مردم بگویید.
- با دقت متوجه باشید که چیزهای را در اینترنت شریک می سازید را کی ها دیده می توانند، ببینید که تنظیمات مربوط به حریم خصوصی تان در سطح بلند قرار دارد و در باره کسی با او صحبت می کنید فکر کنید.
- در مورد نشانه های کلاهبرداری و اینکه چگونه منتظر ایمیل ها و وب سایت های کلاهبرداری باشید، آگاه باشید.
- هرگز معلومات بسیار شخصی مانند آدرس، تصاویر، شماره تماس، نام کامل و تاریخ تولد تان را در اینترنت بیرون ندهید.
- هرگز جزییات ورود به سیستم و رمز عبور تان را بیرون ندهید.
- هرگز ایمیل های ناشناخته، فایل ها و الصاق ها را باز نکنید و از ایمیل های جعلی و کلاهبرداری با خبر باشید.

