

# زنان پناهجو



پروژه توانمندسازی دیجیتال و  
برقراری ارتباط

جلسه 3 – امنیت دیجیتال

# خوش آمدید!

امروز ما می‌خواهیم:

- در مورد مراحل ضروری امنیت دیجیتال و نکاتی در خصوص امنیت اینترنت گفتگو کنیم
- در مورد نحوه شناسایی انواع تهدیدهای آنلاین رایج صحبت کنیم
- در مورد نحوه ایجاد ارتباط بین مراحل امنیت آنلاین رسانه‌های اجتماعی و روابط میان فردی در دنیای واقعی گفتگو کنیم



# اصول پایه

- فضای محرمانه
- فضای امن
- قرار دادن گوشی در حالت سکوت
- احترام به دیگران
- قضاوت نکردن
- یکی یکی صحبت کردن
- قرار دادن Zoom در حالت سکوت وقتی صحبت نمی‌کنید
- اگر می‌خواهید مطلبی تکرار شود، آن را بخواهید!
- اینکه چیزی را ندانید عیب نیست



# امنیت دیجیتال

چرا مهم  
است؟

معنی آن  
چیست؟

# داشتن یک رمز عبور قوی

- از رمز عبور سخت استفاده کنید به طوریکه نتوان به راحتی آن را حدس زد

- رمز عبور خود را به طور منظم تغییر دهید

- برای همه حساب‌های کاربری از یک رمز عبور استفاده نکنید

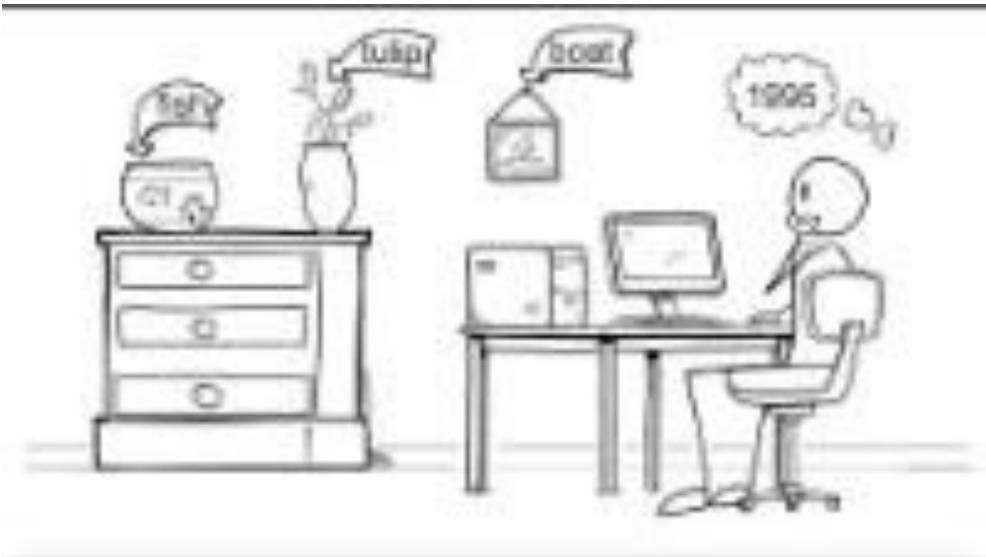
- برای مواقعی که رمز عبور خود را فراموش می‌کنید از پرسش‌های امنیتی استفاده کنید

- برای ایجاد یک رمز عبور قوی، توصیه ما این است که از سه کلمه تصادفی به همراه عدد، حروف بزرگ و علامت‌ها استفاده کنید، مثل؛ Cat!PotatoS0fa7

**The power  
of kindness**



See Metropolitan Police (2017) #threerandomwords  
[https://www.youtube.com/watch?v=3aY\\_EPgi0VU](https://www.youtube.com/watch?v=3aY_EPgi0VU)



# حفاظت از دستگاه در مقابل ویروس

- کامپیوتر، تلفن و وسایل دیگر ممکن است ویروسی شوند که این می‌تواند آسیب‌های زیادی وارد آورد
- نرم افزار آنتی ویروس یک برنامه کامپیوتری است که برای حفاظت در برابر ویروس، شناسایی ویروس و حذف ویروس مورد استفاده قرار می‌گیرد.
- لپ تاپ شما به مدت 12 ماه دارای آنتی ویروس Windows Defender است، پس از این مدت، شما مسئول حفاظت از لپ تاپ خود خواهید بود.
- نرم افزار آنتی ویروس باید به طور مرتب به روز شود.

# انواع رایج تهدیدات آنلاین

کلاهبرداری‌های ایمیلی	فیشینگ	نرم افزارهای مخرب - «بد افزار»
<ul style="list-style-type: none"><li>- ایمیل و یا پیام‌های متنی که اغلب سعی می‌کنند شما را متقاعد سازند روی یک لینک کلیک کنید.</li><li>- به محض کلیک کردن، شما احتمالاً به یک وب سایت غیر ایمن هدایت می‌شوید که می‌تواند روی کامپیوتر شما ویروس دانلود کند، یا رمز عبور و اطلاعات شخصی شما را بدزدد.</li><li>- ممکن است از متن‌هایی استفاده کنند که شما را ترغیب به «انجام یک عمل» مانند باز کردن لینک، ارائه اطلاعات یا کلیک روی یک فایل ضمیمه شده، می‌کنند.</li></ul>	<ul style="list-style-type: none"><li>- پیام‌هایی که سعی می‌کنند شما را گول بزنند اطلاعات حساس خود مانند اطلاعات شخصی‌تان را ارائه دهید؛</li><li>- ممکن است این پیام‌ها خیلی واقعی به نظر برسند و شما را متقاعد کنند، اغلب این پیام‌ها از طرف بانک یا منابع قابل اعتماد دیگر فرستاده می‌شوند.</li><li>- ممکن است از شما بخواهند رمز عبور خود را دوباره وارد کنید، تاریخ تولد خود را تایید کنید، یا شماره کارت بانکی خود را وارد کنید؛</li><li>- به محض اینکه مجرمین به اطلاعات شخصی شما دسترسی پیدا کنند، از آن برای انجام کلاهبرداری‌هایی مانند سرقت هویت و کلاهبرداری بانکی استفاده می‌کنند.</li></ul>	<ul style="list-style-type: none"><li>- نرم افزاری که توسط یک فرد به قصد آسیب زدن به دستگاه کاربرانش ساخته شده است.</li><li>- گاهی اوقات اطلاعات یا داده‌های موجود بر روی دستگاه شما را جمع آوری و انتقال می‌دهد.</li><li>- به این بدافزارها ویروس، کرم، تروجان، اسب، جاسوس افزار، بدافزار تبلیغاتی، باج افزار و جرم افزار هم گفته می‌شود.</li></ul>



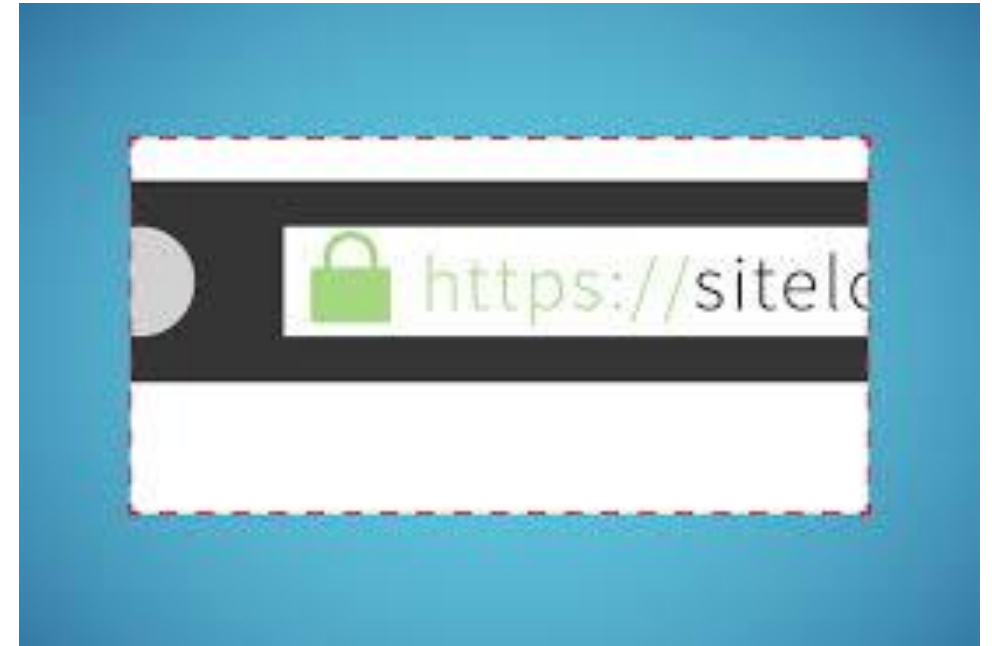
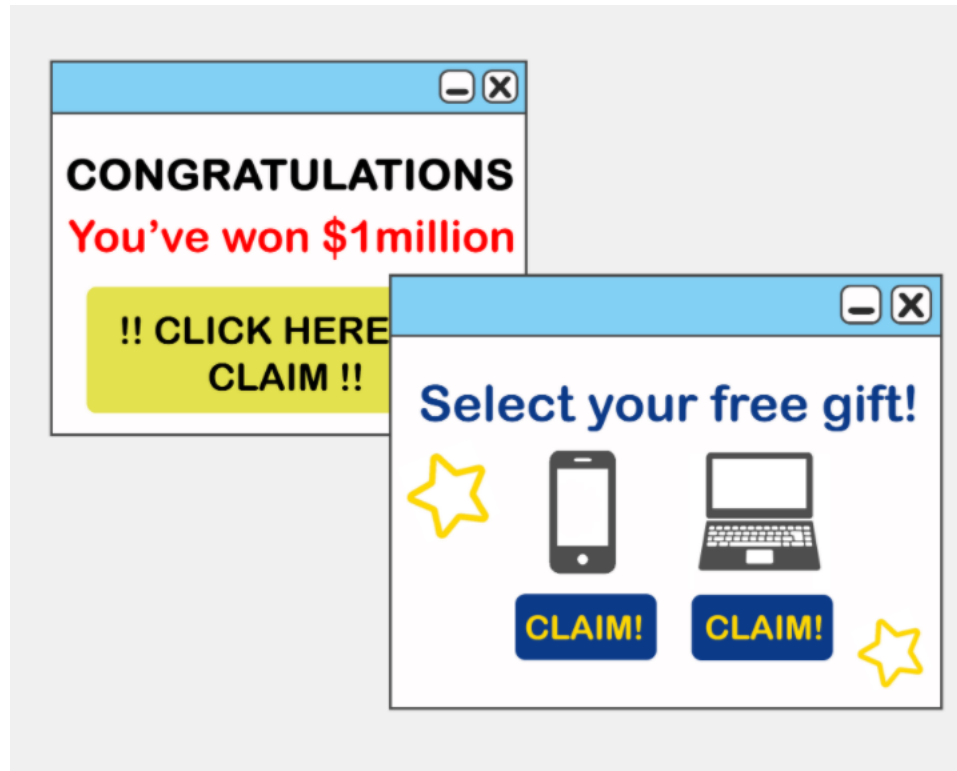
# تشخیص ایمیل‌های فیشنگ و کلاهبرداری

- آیا فرستنده را می‌شناسید؟ آیا آنها در ایمیل جویای احوال شما می‌شوند؟
- آیا اشتباهات املایی دارند و یا نگارش آنها ضعیف است؟
- آیا از شما می‌خواهند کاری انجام دهید یا حس فوریت در این پیام‌ها وجود دارد یا شما را تهدید می‌کنند؟
- آیا برای اینکه واقعی باشند زیادی خوب هستند؟
- آدرس ایمیل فرستنده را باز کنید. آیا آدرس دامین آن درست است؟
- آیا این ایمیل غیر منتظره است یا از سمت شرکتی ارسال شده است که تاکنون معامله‌ای با آن نداشته‌اید؟
- آیا شما را به یک وب سایت دیگر هدایت می‌کند؟



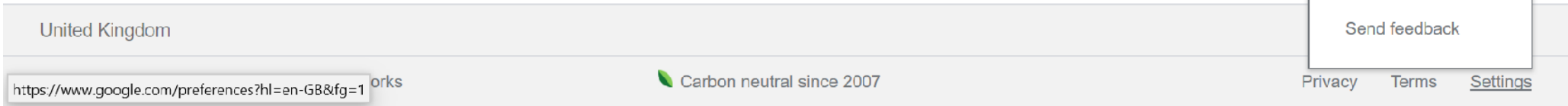
# وب سایت‌های امن

وب سایت‌های دارای تبلیغات «پاپ-آپ» معمولاً قابل اعتماد نیستند

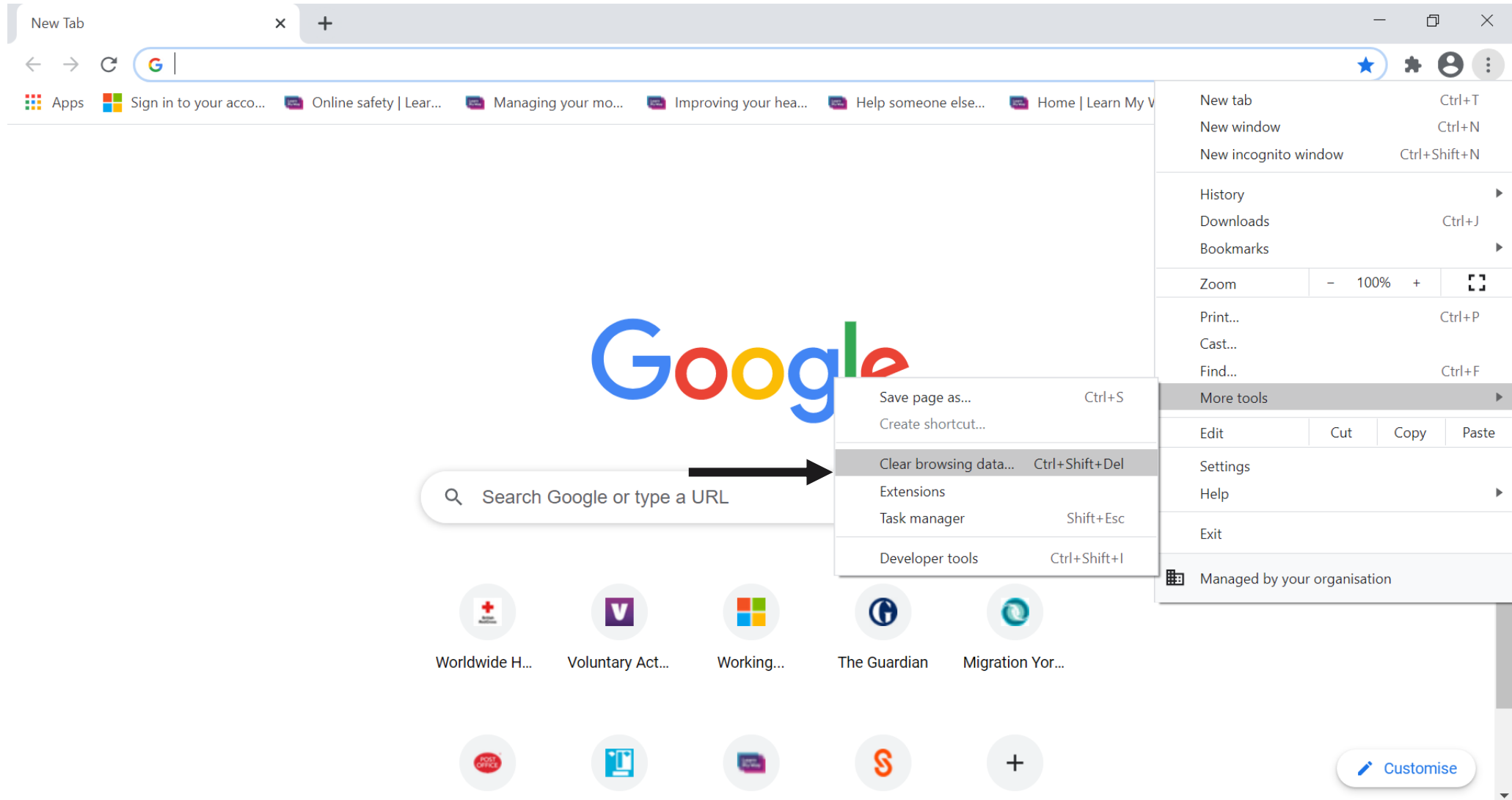


برای تشخیص امن بودن یک وب سایت، علامت قفل و یا https را چک کنید

The power  
of kindness



# پاک کردن تاریخچه جستجو



The power  
of kindness

## ارتباط آنلاین با مردم

- تنظیمات حریم خصوصی در رسانه‌های اجتماعی
- محتوای رسانه‌های اجتماعی در موتورهای جستجو



The power  
of kindness

Zahra دختر عمویی دارد که بسیار به او نزدیک است. دختر عموی او اخیرا رفتار عجیبی دارد، ناراحت است، زود رنج شده است، و هر وقت با هم هستند مدام با استرس در حال چک کردن گوشی خود است. در نهایت، دختر عموی Zahra به او می‌گوید که او شبها نمی‌تواند خوب بخوابد و به خاطر تهدیدات شوهر سابقش که از او طلاق گرفته است استرس دارد. شوهر سابقش مدام به او پیام و ایمیل می‌فرستند و می‌گوید که او همسر و مادری افتضاح است، و باعث شرمساری هر دو خانواده شده است، و اینکه باید دوباره با او زندگی کند. دختر عموی Zahra استرس زیادی دارد و هر روز بیشتر هم می‌شود.

او توضیحات بیشتری می‌دهد و می‌گوید که همسر سابقش یک عکس لختی از او دارد که مربوط به زمانی می‌شود که با هم زندگی می‌کردند. او تهدید کرده است که اگر به او برنگردد عکسش را برای خانواده‌اش ارسال می‌کند.

# بهبود امنیت دیجیتال

---

وسایل دیجیتالی چه هستند؟

---

از چه شبکه‌های اجتماعی استفاده می‌کنید؟

---

پیشنهاد شما چیست؟

### کلاهبرداری عشقی

- ایجاد یک رابطه شخصی برای جلب اعتماد و سپس مطالبه پول یا اطلاعات شخصی.
- از ایجاد اعتماد و تعلق عاطفی برای درخواست کمک، معمولاً پول، و یا گاهی اوقات دریافت یک بسته در آدرس، استفاده می‌کنند.

### زورگویی سایبری

- زورگویی‌ای که از طریق آنلاین یا استفاده از تکنولوژی انجام می‌شود.
- معمولاً زورگویان از شبکه‌های اجتماعی مانند Facebook یا Twitter، یا پیام و انجمن‌های تعاملی استفاده می‌کنند.
- می‌تواند هم بزرگسالان و هم کودکان را هدف بگیرد.

### اغفال

- ایجاد اعتماد و ارتباط با یک فرد به گونه‌ای که بتوان از او بهره برداری کرد و او را کنترل کرد، و اغلب با هدف سوء استفاده جنسی صورت می‌گیرد
- اغفال آنلاین کودکان و افراد جوان نوعی سوء استفاده از کودک محسوب می‌شود.

### ارسال محتوای پورن

- به اشتراک گذاری مطالب شخصی و جنسی، در قالب عکس یا فیلم افراد دیگر، بدون رضایت آنها و با هدف ایجاد ترس و اضطراب
- به اشتراک گذاری تصاویر افراد خردسال سوء استفاده از کودک محسوب می‌شود.

### تحت نظر گرفتن سایبری

- نظارت یک الگوی رفتاری از جانب یک فرد است که موجب ایجاد ترس یا اضطراب می‌شود. این کار وقتی به صورت آنلاین انجام شود به آن نظارت سایبری گفته می‌شود.
- نظارت سایبری می‌تواند تاثیری جدی بر قربانی خود بگذارد و یک جرم کیفری محسوب می‌شود.

### سوء استفاده خانگی

- سوء استفاده روانی، فیزیکی، عاطفی یا مالی که از طرف شریک زندگی، همسر سابق، اعضای خانواده، یا سرپرست انجام می‌شود.
- سوء استفاده کننده می‌تواند به صورت بالقوه از اینترنت یا وسایل متصل به اینترنت برای تماشای چک کردن و کنترل قربانی استفاده کند.

**روابط آنلاین**

**The power  
of kindness**



ضبط ویدئو

جمع آوری داده

حسابهای اشتراکی

یادگیری ماشینی

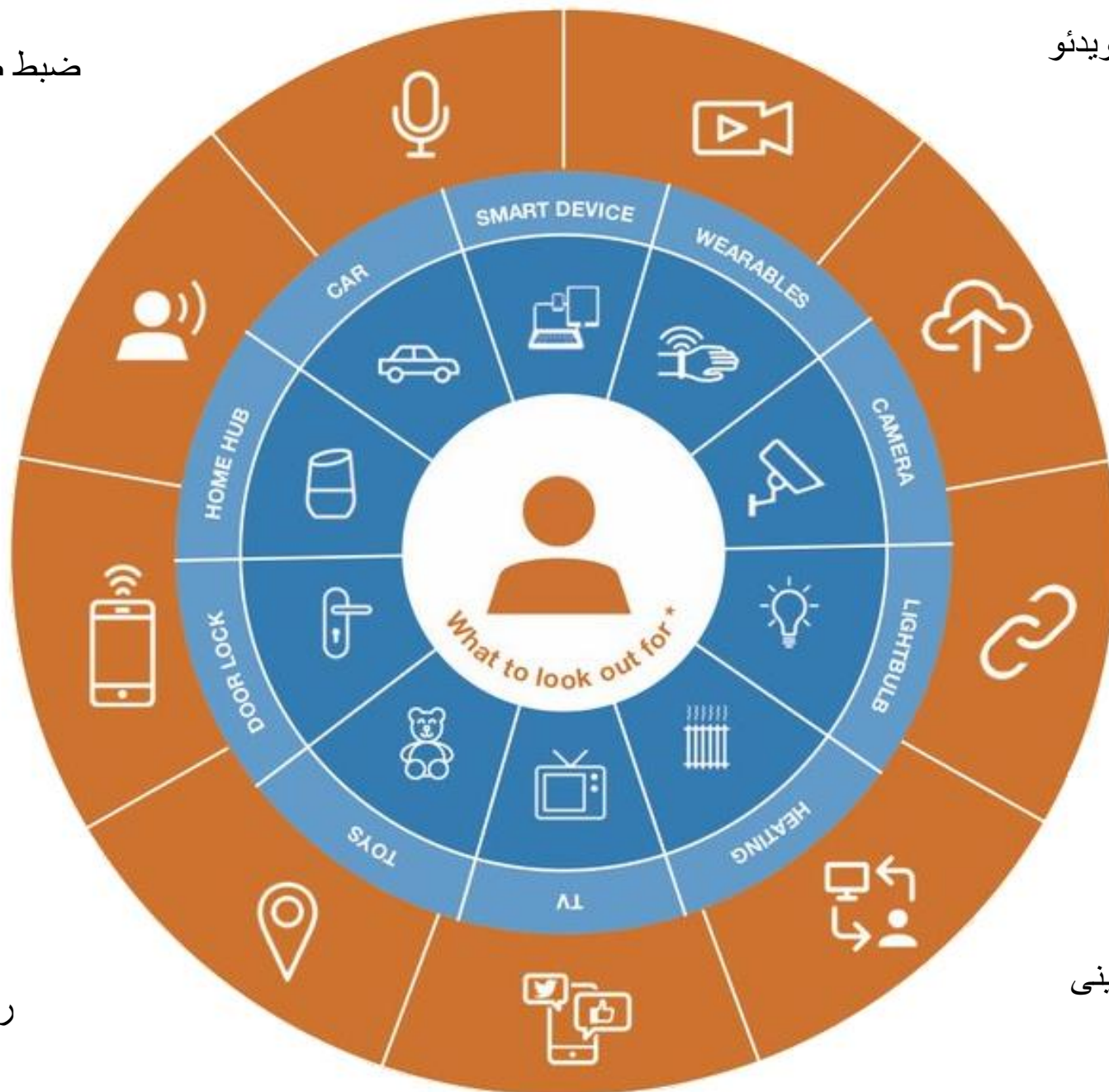
رسانه‌های اجتماعی

ردیابی مکان

کنترل از راه دور

کنترل صوتی

ضبط صدا



**The power  
of kindness**

# بهبود امنیت دیجیتال

ارزیابی	ارزیابی کنید و ببینید که چه اطلاعاتی در خصوص شما در فضای آنلاین مانند Facebook و Twitter موجود است
تغییر	رمز عبور و ایمیل حساب‌های کاربری کلیدی خود را تغییر دهید
حذف	حساب‌های کاربری آنلاین خود را حذف کنید، به خصوص اگر شامل مقادیر زیادی از اطلاعات یا عکس‌های مربوط به شما هستند.
بررسی	تمامی تنظیمات مربوط به حریم خصوصی و امنیت را بررسی کنید
اجتناب	از انجمن‌های عمومی اجتناب کنید
محدودیت	مطالبی که به اشتراک می‌گذارید را محدود کنید
حذف	می‌توانید تاریخچه جستجوی خود در Chrome، Firefox، Internet Explorer و Safari را حذف کنید.
تنظیم	بر روی کامپیوتر یا موبایل خود رمز عبور تنظیم کنید تا مطمئن شوید تنها شما به آنها دسترسی دارید.
ایمیل	ایمیل: مهم است رمز عبوری برای ایمیل خود در نظر بگیرید که احتمال اینکه دیگران بتوانند آن را حدس بزنند وجود نداشته باشد.

## خلاصه

امروز ما:

- در مورد توصیه‌های اساسی مربوط به امنیت دیجیتال صحبت کردیم
- در مورد برخی نمونه‌های تهدیدات آنلاین و نحوه تشخیص آنها صحبت کردیم
- در مورد پیشنهاداتی برای بررسی و بهبود حریم خصوصی آنلاین و امنیت دیجیتال صحبت کردیم.

نکته مهم اینکه امنیت دیجیتال به آگاهی آنلاین مربوط است.



# کلمات کلیدی

وسیله – تجهیزات الکترونیکی که امکان اتصال به اینترنت دارند

آگاهی دیجیتال – توسعه دانش در مورد خطرات و مزایای استفاده از اینترنت و وسایل متصل به اینترنت

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

سو استفاده آنلاین – رفتار ظالمانه و مخرب علیه دیگر افراد که از طریق اینترنت اتفاق می افتد

تهدید آنلاین – خطر و یا مشکلی که منجر به یک حادثه یا اقدام نامطلوب از طریق اینترنت می شود

رمز عبور – مجموعه ای از کاراکترهای مخفی که اجازه دسترسی به یک کامپیوتر یا سرویس را می دهند

تنظیمات حریم خصوصی – کنترل می کند که از چه گزینه هایی می شود برای باز کردن یا محدود کردن دسترسی به اطلاعات در شبکه های اجتماعی استفاده کرد

رسانه های اجتماعی – وب سایت ها و برنامه های کامپیوتری که مردم برای برقراری ارتباط و به اشتراک گذاری اطلاعات در اینترنت با استفاده از کامپیوتر یا گوشی موبایل از آنها استفاده می کنند.