



Australian Government

همین حالا اقدام کنید.  
ایمن بمانید.



# چطور می‌توانید آنلاین خود را مصون نگه‌دارید

نسخه آسان برای خواندن



## چطور از این رهنما استفاده کنید

ما حکومت استرالیا هستیم.

ما این رهنما را نوشتیم.



ما بعضی کلمه‌ها را به شکل **برجسته** (بولد) نوشتیم.

ما معنی این کلمه‌ها را توضیح می‌دهیم.

همچنان فهرست این کلمه‌ها در صفحه 28 موجود است.

می‌توانید از کسی که به او اعتماد دارید کمک بخواهید تا:

- این رهنما را بخوانید
- معلومات بیشتر پیدا کنید.



این یک خلاصه آسان برای خواندن از یک رهنمای دیگر است.

این فقط مهم‌ترین نکات را شامل می‌شود.



می‌توانید رهنمای دیگر را در وبسایت ما پیدا کنید.

[www.actnowstaysecure.gov.au](http://www.actnowstaysecure.gov.au)



# در این رهنما چه چیزهایی است؟

3 در این رهنما چه چیزهایی است؟

---

4 درباره این رهنما

---

6 حساب‌های خود را امن نگه‌دارید

---

10 تنظیمات خود را بررسی کنید تا معلومات‌تان را محافظت کنید

---

16 از دستگاه‌های خود محافظت کنید

---

20 کلاهبرداری‌ها

---

25 سخن بگویید

---

28 فهرست واژه‌ها

---

30 با ما تماس بگیرید

---

## درباره این رهنما

همه ما باید در مورد این فکر کنیم که چطور می‌توانیم در اینترنت مصون بمانیم.  
ما این را **امنیت سایبری** می‌نامیم.



سایبر یعنی چیزی که به اینترنت مربوط می‌شود.



این رهنما بعضی کارهایی را توضیح می‌دهد که می‌توانید انجام بدهید تا خود را در اینترنت محافظت کنید.  
برای مثال، از **جرم سایبری**.



جرم سایبری زمانی است که مجرم‌ها از اینترنت برای انجام جرم استفاده می‌کنند.



برای مثال، آن‌ها ممکن است از اینترنت استفاده کنند تا:

- معلومات شخصی شما را بدزدند
- حساب‌ها یا پروفایل‌های آنلاین شما را در اختیار بگیرند.

جرم سایبری می‌تواند در هر دستگاهی رخ بدهد.

این شامل موارد زیر می‌شود:

- کامپیوتر
- تلفون هوشمند
- ساعت هوشمند.



کارهایی وجود دارد که می‌توانید انجام بدهید تا از جرم‌های سایبری در امان بمانید.



ما در صفحه‌های بعدی توضیح می‌دهیم که چه کارهایی می‌توانید انجام بدهید.



## حساب‌های خود را امن نگه‌دارید

شما باید در مورد این فکر کنید که چگونه می‌توانید حساب‌های آنلاین خود را امن نگه‌دارید.



## از عبارات عبور ( پس فریز ) قوی و متفاوت استفاده کنید

یک پس‌فریز نوع قوی‌تر از رمز عبور است.  
حدس زدن آن برای افراد دیگر بسیار سخت است.



استفاده از رمزهای عبور قوی و متفاوت یکی از بهترین روش‌ها برای محافظت از حساب‌های شما است.



برای هر یک از حساب‌های آنلاین خود باید از یک رمز عبور متفاوت استفاده کنید.



عبارات عبور قوی شامل این‌ها هستند:

- ۴ یا بیشتر کلمه تصادفی
- ۱۵ یا بیشتر حرف و عدد.



می‌توانید بعضی حروف بزرگ را هم شامل کنید.



همچنان می‌توانید از علامت‌ها استفاده کنید، مثل:

- خط تیره
- علامت دالر
- علامت @ ایمیل.



نباید در عبارات عبور خود از هیچ معلومات شخصی استفاده کنید.



برای مثال:

- تاریخ تولد شما
- نام اعضای خانواده یا حیوانات خانگی شما.



## مراحل اضافی برای وارد شدن به حساب‌های خود اضافه کنید

می‌توانید حساب‌های آنلاین خود را با احراز هویت

چند مرحله‌ای (MFA) محافظت کنید.

MFA یعنی شما هر بار برای وارد شدن به حساب خود از ۲

یا بیشتر روش مختلف استفاده می‌کنید.



برای مثال، ممکن است اول لازم باشد عبارت عبور خود را

وارد کنید.

بعد یک کدی را وارد می‌کنید که به تلفون شما می‌آید.





ممکن است این انتخاب را داشته باشید که:

- یک اپلیکیشن روی تلفون خود بگیرید که کُد را برایتان بدهد



- کُد را در ایمیل دریافت کنید



- کُد را در پیام متنی دریافت کنید.



MFA باعث می‌شود که افراد دیگر نتوانند به آسانی وارد حساب‌های آنلاین شما شوند.  
حتی اگر عبارت عبور شما را پیدا کنند.



# تنظیمات خود را بررسی کنید تا معلوماتتان را محافظت کنید

می‌توانید بررسی کنید که تنظیمات شما معلوماتتان را  
در اینترنت محافظت می‌کند یا نه.



این شامل تنظیمات در موارد زیر می‌شود:

- حساب‌های آنلاین شما
- دستگاه‌های شما
- اپلیکیشن‌ها.



شما می‌توانید:

- تنظیمات خود را تغییر بدهید
- انتخاب کنید کدام اپلیکیشن‌ها می‌توانند از  
معلومات شما استفاده کنند.



ممکن است تنظیمات را در دستگاه خود از این طریق

پیدا کنید:

- پالیدن برای علامت چرخ‌دنده (gear icon)

یا

- تایپ کردن "تنظیمات" در بخش جستجوی دستگاه خود.



ممکن است تنظیمات را در یک اپلیکیشن یا حساب آنلاین از طریق باز کردن منو پیدا کنید.

منو معمولاً به شکل ۳ خط مستقیم دیده می‌شود.



بعضی از این تنظیمات می‌توانند معلومات را برای موارد

زیر شریک کنند:

- شما کی هستید
- شما کجا هستید
- شما کجا زندگی می‌کنید.



شریک کردن این معلومات در اینترنت می تواند شما را در  
خطر جرم های سایبری قرار بدهد.



مجرم های سایبری می توانند از معلومات شما استفاده  
کنند تا خود را به جای شما جا بزنند.



برای مثال، ممکن است از معلوماتی مثل این استفاده کنند:

- محل زندگی شما



- نام اعضای خانواده شما



- نام حیوانات خانگی شما.



می‌توانید حساب‌های خود را طوری تنظیم کنید که فقط افرادی که می‌شناسید بتوانند پروفایل‌های شبکه‌های اجتماعی شما را ببینند.

برای مثال، پروفایل فیسبوک شما.



این تنظیمات معمولاً تنظیمات حریم خصوصی نامیده می‌شوند.



همچنان می‌توانید **تنظیمات موقعیت مکانی** خود را کنترل کنید.

تنظیمات موقعیت مکانی نشان می‌دهد که دستگاه شما کجا قرار دارد.



می‌توانید تنظیمات موقعیت مکانی را روشن یا خاموش کنید.

همچنان می‌توانید انتخاب کنید کدام اپلیکیشن‌ها بتوانند از موقعیت مکانی شما استفاده کنند.



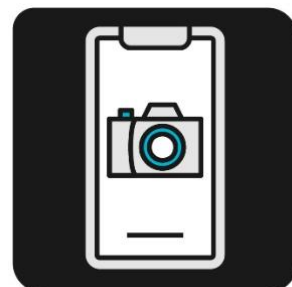
می‌توانید این کار را برای موارد زیر انجام دهید:

- حساب‌های آنلاین
- دستگاه‌ها
- اپلیکیشن‌ها.



بعضی اپلیکیشن‌ها ممکن است از شما بپرسند که آیا می‌توانند:

- از دوربین شما استفاده کنند



- عکس‌های شما را ببینند.



شما باید فقط به اپلیکیشن‌هایی که با آن‌ها آشنا هستید اجازه بدهید از دوربین و عکس‌های شما استفاده کنند.



## از دستگاه‌های خود محافظت کنید

شما باید در مورد این فکر کنید که چگونه می‌توانید از دستگاه‌های خود محافظت کنید تا در اینترنت مصون بمانید.



برای مثال، تلفون یا ساعت هوشمند شما.

این موضوع برای دستگاه‌هایی که به اینترنت وصل می‌شوند مهم است.



## دستگاه‌های خود را به‌روز کنید

می‌توانید دستگاه‌های خود را به‌روز کنید تا در اینترنت امن بمانند.



برای مثال، تلفون و لپ‌تاپ شما.

دستگاه شما ممکن است این را به روزرسانی نرم افزار بنامد.





به روزرسانی‌ها به دستگاه کمک می‌کنند تا از خود در برابر جرم‌های سایبری محافظت کند.



می‌توانید دستگاه را طوری تنظیم کنید که به صورت خودکار به روزرسانی شود.



می‌توانید درباره این که چگونه دستگاه‌های خود را به روز کنید در وبسایت ما بیشتر بیاموزید.

[www.actnowstaysecure.gov.au/  
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)



## شبکه‌های وای‌فای عمومی

باید هنگام استفاده از **وای‌فای عمومی** احتیاط کنید.



وای‌فای عمومی اینترنت بی‌سیم رایگان است که می‌توانید در مکان‌های عمومی از آن استفاده کنید.



برای مثال، در یک:

- کافه
- میدان هوایی
- هتل.



باید در مورد معلوماتی که هنگام استفاده از وای فای عمومی در یک وبسایت وارد می‌کنید احتیاط کنید.



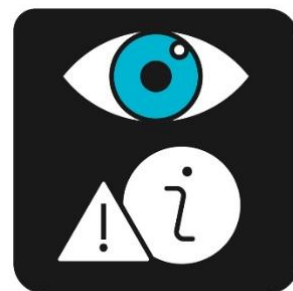
برای مثال:

- معلومات بانکی شما
- حساب‌های ایمیل شما
- پروفایل‌های شبکه‌های اجتماعی شما.



بعضی مجرم‌های سایبری می‌توانند از وای فای عمومی استفاده کنند تا:

- ببینند شما در اینترنت چه کار می‌کنید
- معلومات شما را بدزدند.



این به این دلیل است که:

- هر کسی می‌تواند از آن استفاده کند



- محافظت از دستگاه‌های شما در آن سخت‌تر است.



می‌توانید در وبسایت ما یاد بگیرید که چگونه هنگام استفاده از وای‌فای عمومی امن بمانید.

[www.actnowstaysecure.gov.au/  
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)



## کلاهبرداری‌ها

به آن "کلاهبرداری" می‌گوییم وقتی کسی تلاش می‌کند:

- شما را فریب بدهد
- پول شما را بگیرد.



کلاهبردار کسی است که کلاهبرداری انجام می‌دهد.



کلاهبردارها ممکن است از طریق موارد زیر شما را فریب دهند:

- پیام متنی یا تماس تلفنی
- ایمیل
- شبکه‌های اجتماعی
- یک وبسایت.



آنها ممکن است دوستانه به نظر برسند،

اما می‌توانند شما را فریب بدهند تا معلومات خود را در اختیارشان قرار دهید.



آنها می‌توانند از این معلومات برای این کارها استفاده کنند:

- وارد شدن به حساب‌های آنلاین شما



- وانمود کردن که خود شما هستید



- دزدی پول شما.



کلاهبردارها همچنان ممکن است:

- حساب‌های جعلی بسازند تا شما را فریب بدهند



- لینک‌ها و اعلان‌ها (تبلیغات) را برای شما شریک کنند تا روی آن‌ها کلیک کنید.



## چگونه یک کلاهبرداری را تشخیص بدهیم

ممکن است کلاهبرداری باشد اگر:

- از شما می‌خواهد که سریع کاری انجام دهید



- به شما پول زیاد وعده می‌دهد



- از شما پول درخواست می‌کند



- از شما می‌خواهد روی یک لینک کلیک کنید.



کلاهبردارها ممکن است همچنان خود را به شکل یک  
سازمانی که شما می‌شناسید و به آن اعتماد دارید نشان  
بدهند،

برای مثال، بانک شما.



کلاهبردارها این کار را می‌کنند تا شما معلومات شخصی  
خود را با آن‌ها شریک کنید.



اگر فکر می‌کنید کسی کلاهبردار است، باید صحبت با او را  
متوقف کنید.



باید بررسی کنید که آیا شخص همان کسی است که ادعا  
می‌کند.



می‌توانید با آن شخص یا سازمان از طریق معلوماتی که  
خودتان پیدا کرده‌اید و به آن اعتماد دارید تماس بگیرید.

اگر چیزی درست به نظر نمی‌رسد، سریع اقدام کنید تا از  
خودتان محافظت کنید.



## گزارش دادن یک کلاهبرداری

Scamwatch به مردم استرالیا کمک می‌کند تا:

- کلاهبرداری‌ها را بشناسند
- کلاهبرداری‌ها را گزارش دهند.



Scamwatch همچنان به افرادی در استرالیا کمک می‌کند

که با کلاهبرداری روبه‌رو شده‌اند.



می‌توانید یک کلاهبرداری را در وبسایت Scamwatch

گزارش دهید.

[www.scamwatch.gov.au/report-a-scam](http://www.scamwatch.gov.au/report-a-scam)





## سخن بگویند

باید درباره این که دیگران چگونه می توانند از خود در اینترنت محافظت کنند صحبت کنید.



این شامل موارد زیر می شود:

- گزارش دادن جرم های سایبری



- شریک ساختن معلوماتی که دارید با خانواده و دوستان.



در صفحات بعدی توضیح خواهیم داد که چگونه می توانید حرف خود را بزنید.



## گزارش دادن جرم‌های سایبری

گزارش دادن جرم‌های سایبری به دولت کمک می‌کند تا:

- یاد بگیرد که مجرم‌های سایبری چگونه تلاش می‌کنند به مردم حمله کنند



- از افراد بیشتری محافظت کند.



می‌توانید جرم‌های سایبری را در وبسایت ReportCyber گزارش دهید.

[www.cyber.gov.au/report](http://www.cyber.gov.au/report)



## با خانواده و دوستان درباره امن ماندن در اینترنت صحبت کنید.

شما باید راهنمایی های خود را درباره امن ماندن در اینترنت با خانواده و دوستان خود شریک کنید.  
شما هم می توانید از آنها یاد بگیرید.



شما می توانید با شریک کردن معلوماتی که درباره امن ماندن در اینترنت دارید، از خود و اطرافیانتان محافظت کنید.



این موضوع همچنان مهم است اگر شما دستگاه های خود را با دیگران شریک می کنید.



## فهرست واژه‌ها

این فهرست توضیح می‌دهد که کلمات **برجسته (بولد)** در این راهنما چه معنی دارند.

### سایبر (Cyber)



سایبر به این معنی است که چیزی مربوط به اینترنت باشد.

### جرم سایبری (Cyber crime)

جرم سایبری زمانی است که مجرم‌ها از اینترنت برای انجام

جرم استفاده می‌کنند.



برای مثال، آن‌ها ممکن است از اینترنت برای این کارها استفاده کنند:

- دزدیدن معلومات شخصی شما
- به‌دست گرفتن کنترل حساب‌های آنلاین شما.

### تنظیمات موقعیت مکانی (Location settings)



تنظیمات موقعیت مکانی نشان می‌دهد که دستگاه شما کجا قرار دارد.

## تصدیق هویت چندمرحله‌ای (Multi-factor authentication / MFA)

MFA زمانی است که شما هر بار برای وارد شدن به حساب خود از دو یا چند روش مختلف استفاده می‌کنید.



## عبارت عبور (Passphrase)

Passphrase یک نوع قوی‌تر از رمز عبور است. حدس زدن آن برای دیگران بسیار سخت است.



## وای‌فای عمومی (Public Wi-Fi)

وای‌فای عمومی اینترنت بی‌سیم رایگان است که می‌توانید در مکان‌های عمومی از آن استفاده کنید.



## کلاهبرداری‌ها (Scams)

به آن کلاهبرداری می‌گوییم وقتی کسی تلاش می‌کند:

- شما را فریب بدهد
- پول شما را بگیرد.



## کلاهبردارها (Scammers)

کلاهبردار کسی است که کلاهبرداری انجام می‌دهد.



## با ما تماس بگیرید

می‌توانید با خط تلفنی امنیت سایبری استرالیا تماس بگیرید.

1300 292 371



می‌توانید به وبسایت ما مراجعه کنید.

[www.actnowstaysecure.gov.au](http://www.actnowstaysecure.gov.au)



می‌توانید جرم‌های سایبری را در وبسایت

ReportCyber گزارش دهید.

[www.cyber.gov.au/report](http://www.cyber.gov.au/report)



---

این سند Easy Read توسط Information Access Group،  
با استفاده از عکس‌های آماده (stock photography) و تصاویر  
اختصاصی تدوین شده است. بدون اجازه، استفاده دوباره از این  
تصاویر مجاز نیست. اگر درباره تصاویر پرسشی دارید، لطفاً به  
وبسایت زیر مراجعه کنید: [www.informationaccessgroup.com](http://www.informationaccessgroup.com)  
لطفاً شماره وظیفه 6342 (job number) را ذکر کنید.

