



Australian Government

هم اکنون اقدام کن. ایمن بمان.



چگونه می‌توانید در فضای آنلاین ایمن بمانید

نسخه ساده شده



نحوه استفاده از این راهنما

ما دولت استرالیا هستیم.

ما این راهنما را نوشته‌ایم.



ما بعضی از کلمات را با **حروف پررنگ** نوشته‌ایم.

معنی این کلمات را توضیح داده‌ایم.

فهرستی از این کلمات در صفحه 28 نیز آمده است.



می‌توانید از فردی که به او اعتماد دارید کمک بگیرید تا:

- این راهنما را بخوانید
- اطلاعات بیشتری پیدا کنید.



این راهنما یک خلاصه ساده‌شده از یک راهنمای دیگر است.

فقط مهمترین نکات در این راهنما آمده است.



راهنمای دیگر را می‌توانید در وب سایت ما پیدا کنید.

www.actnowstaysecure.gov.au



این راهنما شامل چه مواردی است؟

4 درباره این راهنما

6 حساب‌های کاربری خود را ایمن نگه دارید

10 برای محافظت از اطلاعاتتان تنظیمات خود را بررسی کنید

16 از دستگاه‌های خود محافظت کنید

20 کلاهبرداری

25 آگاهی‌رسانی کنید

28 فهرست واژگان

30 تماس با ما

درباره این راهنما

همه ما باید به این فکر کنیم که چگونه می‌توانیم در فضای آنلاین ایمن بمانیم. ما به این «امنیت سایبری» می‌گوییم.



سایبر به معنای چیزی است که به اینترنت مرتبط است.



این راهنما توضیح می‌دهد که چه کارهایی می‌توانید انجام دهید تا از خود در فضای آنلاین محافظت کنید. برای مثال، محافظت در برابر **جرائم سایبری**.



جرم سایبری زمانی رخ می‌دهد که مجرمان از اینترنت برای انجام جرم استفاده می‌کنند

برای مثال ممکن است از اینترنت استفاده کنند تا:

- اطلاعات شخصی شما را سرقت کنند.
- به حساب های آنلاین یا پروفایل های شما دسترسی پیدا کنند.



جرائم سایبری می‌تواند روی هر دستگاهی رخ دهد.

این دستگاه‌ها شامل موارد زیر هستند:

- کامپیوتر
- تلفن هوشمند
- ساعت هوشمند.



کارهایی وجود دارد که می‌توانید برای ایمن ماندن در برابر جرائم سایبری انجام دهید.



در صفحات بعد توضیح خواهیم داد که چه اقداماتی می‌توانید انجام دهید



حساب‌های کاربری خود را ایمن نگه دارید

باید به این فکر کنید که چگونه می‌توانید حساب‌های آنلاین خود را ایمن نگه دارید.



از عبارت‌های عبور قوی و متفاوت استفاده کنید

عبارت عبور، یک نوع قوی‌تری از رمز عبور است.
حدس زدن آن برای دیگران بسیار دشوار است.



استفاده از عبارت‌های عبور قوی و متفاوت یکی از بهترین راه‌ها برای محافظت از حساب‌های کاربری شماست.



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



عبارت‌های عبور قوی شامل موارد زیر هستند:

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



می‌توانید از حروف بزرگ در زبان انگلیسی استفاده کنید.



همچنین می‌توانید از یکسری نماد مانند موارد زیر استفاده کنید:

- خط تیره
- علامت دلار
- علامت @ مربوط به ایمیل.



در عبارت عبور نباید از اطلاعات شخصی خود استفاده کنید.



برای مثال:

- تاریخ تولد
- نام اعضای خانواده یا حیوانات خانگی.



برای ورود به حساب کاربری خود مراحل بیشتری را اضافه کنید

شما می‌توانید با استفاده از احراز هویت چند عاملی

(MFA) از حساب‌های آنلاین خود محافظت کنید.

احراز هویت چند عاملی زمانی است که برای هر بار ورود

به حساب کاربری خود باید از ۲ یا چند روش مختلف

استفاده کنید.



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

وارد کنید.

و سپس کدی را که روی تلفن همراه خود دریافت می‌کنید را

وارد کنید.



ممکن است این انتخاب را داشته باشید که:

- یک برنامه بر روی گوشی خود نصب کنید تا کد را دریافت کنید



- کد را از طریق ایمیل دریافت کنید



- کد را از طریق پیامک دریافت کنید.



MFA دسترسی افراد دیگر به حساب‌های آنلاین شما را دشوارتر می‌کند.

حتی اگر آن‌ها عبارت عبور شما را پیدا کنند.



برای محافظت از اطلاعاتتان تنظیمات خود را

بررسی کنید

می‌توانید بررسی کنید که آیا تنظیمات شما از اطلاعاتتان در فضای آنلاین محافظت می‌کنند یا خیر.



این شامل تنظیمات موارد زیر می‌شود:

- حساب‌های آنلاین
- دستگاه‌ها
- برنامه‌ها.



شما می‌توانید:

- تنظیمات خود را تغییر دهید
- انتخاب کنید که کدام برنامه‌ها می‌توانند از اطلاعات شما استفاده کنند.



ممکن است بتوانید به روش‌های زیر تنظیمات دستگاه خود را پیدا کنید:

- به دنبال آیکون چرخ دنده بگردید یا



- کلمه «تنظیمات» را در نوار جستجوی دستگاهتان تایپ کنید.

در برنامه‌ها یا حساب‌های آنلاین ممکن است برای دسترسی به تنظیمات نیاز باشد منو را باز کنید. منو معمولاً به شکل سه خط افقی است.



برخی از این تنظیمات می‌توانند اطلاعاتی در رابطه با موارد زیر را به اشتراک بگذارند:

- هویت شما
- موقعیت مکانی شما
- محل زندگی شما.



به اشتراک گذاشتن این اطلاعات به صورت آنلاین می‌تواند شما را در معرض خطر جرایم سایبری قرار دهد.



مجرمان سایبری می‌توانند از اطلاعات شما استفاده کنند و خود را جای شما جا بزنند.



برای مثال ممکن است از اطلاعات زیر استفاده کنند:

- محل زندگی شما



- نام اعضای خانواده شما



- نام حیوانات خانگی شما.



می‌توانید حساب‌های کاربری خود را طوری تنظیم کنید که فقط افرادی که می‌شناسید بتوانند در رسانه‌های اجتماعی پروفایل‌های شما را ببینند.
مثلاً پروفایل فیس بوک شما.



این تنظیمات معمولاً تنظیمات حریم خصوصی نامیده می‌شوند.



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

تنظیمات موقعیت مکانی نشان می‌دهند که دستگاه شما کجاست.



می‌توانید تنظیمات موقعیت مکانی را روشن یا خاموش کنید.

همچنین می‌توانید انتخاب کنید که کدام برنامه‌ها به تنظیمات موقعیت مکانی شما دسترسی داشته باشد.



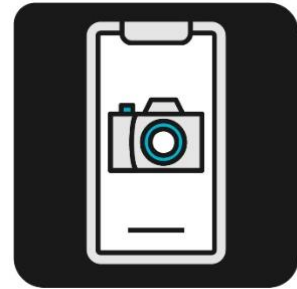
می‌توانید این کار را برای موارد زیر انجام دهید:

- حساب‌های آنلاین
- دستگاه‌ها
- برنامه‌ها.



برخی برنامه‌ها ممکن است درخواست کنند که:

- از دوربین شما استفاده کنند



- به عکس‌های شما دسترسی داشته باشند.



شما فقط باید به برنامه‌هایی که با آنها آشنا هستید اجازه دهید به دوربین و عکس‌های شما دسترسی داشته باشند.



از دستگاه‌های خود محافظت کنید

شما باید فکر کنید که چگونه می‌توانید از دستگاه‌های خود محافظت کنید تا به ایمن ماندن شما در فضای آنلاین کمک کنند.



برای مثال، تلفن همراه یا ساعت هوشمند شما.

این موضوع برای دستگاه‌هایی که به اینترنت متصل می‌شوند بسیار مهم است.



دستگاه‌های خود را به روز رسانی کنید

می‌توانید دستگاه‌های خود را به‌روزرسانی کنید تا آن‌ها را در فضای آنلاین ایمن نگه دارید. برای مثال، تلفن همراه و لپ‌تاپ را.



ممکن است در دستگاه شما به این کار به روز رسانی نرم‌افزار گفته شود.



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



می‌توانید دستگاه را طوری تنظیم کنید که به‌طور خودکار
به‌روزرسانی شود.



می‌توانید اطلاعات بیشتری درباره نحوه به‌روزرسانی
دستگاه‌های خود را در وب‌سایت ما بیابید.

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



شبکه‌های وای فای عمومی

در استفاده از **وای فای عمومی** باید احتیاط کنید.



وای فای عمومی اینترنت بی‌سیم رایگانی است که
می‌توانید در مکان‌های عمومی از آن استفاده کنید.



برای مثال در:

- کافه
- فرودگاه
- هتل.



هنگام استفاده از وای فای عمومی باید مراقب باشید که چه اطلاعاتی را در وب سایت‌ها وارد می‌کنید.



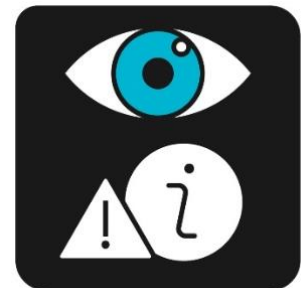
برای مثال:

- اطلاعات بانکی
- ایمیل
- پروفایل شبکه‌های اجتماعی.



برخی مجرمان سایبری می‌توانند از وای فای عمومی استفاده کنند تا:

- فعالیت‌های آنلاین شما را مشاهده کنند
- اطلاعات شما را سرقت کنند.



دلیل آن این است که:

- هر کسی می‌تواند از آن استفاده کند



- محافظت از دستگاهتان دشوارتر است.



در وبسایت ما می‌توانید نحوه ایمن ماندن هنگام استفاده
از وای فای عمومی را بیاموزید.

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



کلاهبرداری

کلاهبرداری زمانی است که فردی تلاش می‌کند:

- شما را فریب دهد
- پول شما را بگیرد.



به فردی که کلاهبرداری می‌کند **کلاهبردار** گفته می‌شود.



کلاهبرداران ممکن است سعی کنند از طریق موارد زیر

شما را فریب دهند:

- پیامک یا تماس تلفنی
- ایمیل
- شبکه‌های اجتماعی
- وبسایت‌ها.



آن‌ها ممکن است دوستانه به نظر برسند.

اما ممکن است شما را فریب دهند تا اطلاعات خود را به آن‌ها بدهید.



آنها می‌توانند از این اطلاعات استفاده کنند تا:

- وارد حساب‌های آنلاین شما شوند



- خود را به جای شما جا بزنند



- پول شما را سرقت کنند.



کلاهبرداران همچنین ممکن است:

- برای فریب دادن شما حساب‌های جعلی ایجاد کنند



- لینک و یا تبلیغاتی را با شما به اشتراک بگذارند که روی آن کلیک کنید.



چگونه کلاهبرداری را تشخیص دهیم

موارد زیر احتمال دارد کلاهبرداری باشند:

- از شما بخواهد کاری را سریع انجام دهید



- مبلغ زیادی پول به شما پیشنهاد دهد



- از شما درخواست پول کند



- از شما بخواهد روی یک لینک کلیک کنید.



کلاهبرداران همچنین ممکن است خود را به جای یک سازمانی که می‌شناسید و به آن اعتماد دارید جا بزنند. مانند بانک شما.



کلاهبرداران این کار را می‌کنند تا شما اطلاعات شخصی خود را در اختیارشان بگذارید.



اگر شک کردید که فرد کلاهبردار است، مکالمه را قطع کنید.



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

می‌توانید با استفاده از اطلاعات تماسی که به آن اعتماد دارید و خودتان پیدا کرده‌اید با آن شخص یا سازمان تماس بگیرید.



اگر احساس کردید مشکلی وجود دارد، سریعاً برای محافظت از خود اقدام کنید.



گزارش کلاهبرداری

Scamwatch به استرالیایی‌ها کمک می‌کند:

- کلاهبرداری‌ها را بشناسند
- کلاهبرداری‌ها را گزارش دهند.



Scamwatch همچنین به استرالیایی‌هایی که قربانی کلاهبرداری شده‌اند کمک می‌کند.



شما می‌توانید در سایت Scamwatch کلاهبرداری را گزارش دهید:

www.scamwatch.gov.au/report-a-scam



آگاهی‌رسانی کنید

شما باید درباره اینکه دیگران چگونه می‌توانند از خود در فضای آنلاین محافظت کنند آگاهی‌رسانی کنید.



این شامل موارد زیر است:

- گزارش جرایم سایبری



- به اشتراک گذاشتن آنچه می‌دانید با خانواده و دوستان.



در صفحات بعدی توضیح خواهیم داد که چگونه می‌توانید آگاهی‌رسانی کنید.



جرائم سایبری را گزارش کنید

گزارش جرائم سایبری به دولت کمک می‌کند:

- بفهمد که مجرمان سایبری چگونه سعی می‌کنند به مردم حمله کنند



- از افراد بیشتری محافظت کند.



شما می‌توانید جرائم سایبری را در وبسایت
ReportCyber گزارش کنید.

www.cyber.gov.au/report



با خانواده و دوستان خود درباره ایمن ماندن در فضای آنلاین

صحبت کنید

شما باید نکات خود درباره ایمن ماندن در فضای آنلاین را با خانواده و دوستانتان به اشتراک بگذارید. همچنین می‌توانید از آن‌ها یاد بگیرید.



با به اشتراک گذاشتن آنچه درباره ایمن ماندن در فضای آنلاین می‌دانید، می‌توانید از خود و اطرافیانتان محافظت کنید.



همچنین این موضوع در صورتی که دستگاه‌های خود را با دیگران به اشتراک می‌گذارید اهمیت دارد.



فهرست واژگان

این فهرست معنای کلمات **پررنگ** در این راهنما را توضیح می‌دهد.

سایبر



سایبر به معنای چیزی است که به اینترنت مرتبط است.

جرم سایبری

جرم سایبری زمانی رخ می‌دهد که مجرمان از اینترنت برای انجام جرم استفاده می‌کنند.



برای مثال ممکن است از اینترنت استفاده کنند تا:

- اطلاعات شخصی شما را سرقت کنند
- به حساب های آنلاین شما دسترسی پیدا کنند.

تنظیمات موقعیت مکانی

تنظیمات موقعیت مکانی نشان می‌دهند که دستگاه شما کجاست.



احراز هویت چند عاملی (MFA)

احراز هویت چند عاملی زمانی است که برای هر بار ورود به حساب کاربری خود باید از ۲ یا چند روش مختلف استفاده کنید.



عبارت عبور

یک نوع قوی‌تری از رمز عبور است. حدس زدن آن برای دیگران بسیار دشوار است.



شبکه‌های وای فای عمومی

وای فای عمومی اینترنت بی‌سیم رایگانی است که می‌توانید در مکان‌های عمومی از آن استفاده کنید.



کلاهبرداری

کلاهبرداری زمانی است که فردی تلاش می‌کند:

- شما را فریب دهد
- پول شما را بگیرد.



کلاهبردار

به فردی که کلاهبرداری می‌کند کلاهبردار گفته می‌شود.



تماس با ما

می‌توانید با خط تلفن امنیت سایبری استرالیا تماس بگیرید.

1300 292 371



می‌توانید از وبسایت ما بازدید کنید.

www.actnowstaysecure.gov.au



می‌توانید جرایم سایبری را در وبسایت ReportCyber

گزارش کنید.

www.cyber.gov.au/report



این نسخه ساده شده توسط Information Access Group و با استفاده از عکس‌های استوک و تصاویر اختصاصی تهیه شده است.

استفاده مجدد از این تصاویر بدون اجازه مجاز نیست. برای هرگونه

سوال درباره تصاویر، لطفاً به سایت

www.informationaccessgroup.com مراجعه کنید و شماره کار

۶۳۴۲ را ذکر کنید.