



Australian Government

همین حالا اقدام کنید.
ایمن بمانید.



چگونه می‌توانید امن بمانید

نسخه آسان خوان



چگونه از این راهنما استفاده کنید

مو دولت استرالیا هستیم.

مو این راهنما را نوشتیم.



بعضی کلمات را با خط **درشت** نوشته ایم.

مو توضیح می‌دهیم این کلمات چه معنی دارند.

فهرست این کلمات در صفحه 28 نیز موجود است.



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

- این راهنما را بخوانید.
- معلومات بیشتر پیدا کنید.



این یک خلاصه آسان خوان از راهنمای دیگر است.

فقط مهم ترین نکات را شامل می‌شود.



شما می‌توانید راهنمای دیگر را در وب سایت مو

پیدا کنید.

www.actnowstaysecure.gov.au



در این راهنما چه چیزهایی است؟

4

در باره این راهنما

6

حساب های خود را امن نگه دارید

10

تنظیمات خود را بررسی کنید تا معلومات شمو محافظت شود

16

از دستگاه های خود محافظت کنید

20

کلاهبرداری ها

25

صحبت کنید

28

فهرست کلمات

30

با مو تماس بگیرید

در باره این راهنما

همه مو باید فکر کنیم چگونه می‌توانیم آنلاین امن بمانیم.
مو این را امنیت **سایبری** می‌نامیم.



سایبری یعنی چیزی که مربوط به اینترنت باشد.



این راهنما بعضی کارهایی را توضیح می‌دهد که می‌توانید
بلدی محافظت از خود آنلاین انجام دهید.
بلدی مثال، در برابر **جرائم سایبری**.



جرم سایبری زمانی است که مجرمان از اینترنت بلدی جرم
استفاده می‌کنند.

بلدی مثال، ممکن است از اینترنت بلدی این کارها استفاده
کنند:



- دزدیدن معلومات شخصی شمو
- گرفتن کنترل حساب ها یا پروفایل های آنلاین شمو.

جرم سایبری می‌تواند در هر دستگاهی اتفاق بیفتد.

از جمله:

- کامپیوتر شمو
- تلفون هوشمند شمو
- ساعت هوشمند شمو.



کارهایی وجود دارد که می‌توانید بلدی محفوظ ماندن از جرایم سایبری انجام دهید.



ما در صفحات بعدی توضیح می‌دهیم چه کارهایی می‌توانید انجام دهید.



حساب های خود را امن نگه دارید

باید فکر کنید چگونه حساب های آنلاین خود را امن نگه دارید.



از عبارت رمز قوی و متفاوت استفاده کنید

عبارت رمز قوی تر پاسورد است.
حدس زدن آن بلدی دیگران بسیار سخت است.



استفاده از عبارت رمز قوی و متفاوت یکی از بهترین راه ها
بلدی محافظت از حساب های شماست.



باید بلدی هر حساب آنلاین خود عبارت رمز جداگانه داشته
باشید.



عبارت رمز قوی شامل این موارد است:

- 4 یا بیشتر کلمه تصادفی
- 15 یا بیشتر حرف و عدد.



می‌توانید از حروف بزرگ نیز استفاده کنید.



همچنین می‌توانید از علامت‌ها استفاده کنید، مانند:

- علامت فاصله
- علامت دالر
- علامت @



نباید از معلومات شخصی در عبارت رمز استفاده کنید.



بلدی مثال:

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



بلدی ورود به حساب های خود مراحل اضافی اضافه کنید.

می توانید حساب های آنلاین خود را با تایید **هویت چند**

مرحله ای (MFA) محافظت کنید.

یعنی هر بار بلدی ورود به حساب، از 2 یا MFA بیشتر روش

مختلف استفاده کنید.



بلدی مثال، ممکن است اول عبارت رمز خود را وارد کنید.

بعد کدی را وارد کنید که به تلفون شما فرستاده می شود.



ممکن است انتخاب داشته باشید که:

- برنامه ای در تلفون خود داشته باشید که کد بدهد



- کد را از طریق ایمیل دریافت کنید



- کد را از طریق پیامک دریافت کنید.



ورود دیگران به حساب شما را MFA سخت تر می کند.
حتی اگر عبارت رمز شما را بدانند.



تنظیمات خود را بررسی کنید تا معلومات شما محافظت شود

می‌توانید بررسی کنید که تنظیمات شما از معلوماتتان آنلاین محافظت می‌کند.



از جمله تنظیمات در:

- حساب های آنلاین
- دستگاه ها
- برنامه ها.



شما می‌توانید:

- تنظیمات خود را تغییر دهید
- انتخاب کنید کدام برنامه ها به معلومات شما دسترسی داشته باشد.



ممکن است تنظیمات دستگاه خود را این گونه پیدا

کنید:

- جستجوی علامت چرخ دنده

یا

- نوشتن کلمه "settings" در قسمت جستجو.



ممکن است تنظیمات در برنامه یا حساب آنلاین را باز

کردن فهرست (منو) پیدا کنید.

فهرست (منو) معمولا 3 خط مستقیم است.



بعضی از این تنظیمات می توانند معلومات زیر را

اشریک سازند:

- شمو کی هستید

- کجا هستید

- کجا زندگی می کنید.



شریک کردن این معلومات آنلاین می‌تواند شمو را در
خطر جرایم سایبری قرار دهد.



مجرمان سایبری می‌توانند از معلومات شمو استفاده
کنند تا خود را به جای شمو نشان دهند.



بلدی مثال، ممکن است از این معلومات استفاده کنند:

- محل زندگی شمو



- نام اعضای خانواده شمو



- نام حیوانات خانگی شمو.



می‌توانید حساب های خود را طوری تنظیم کنید که فقط کسانی که می‌شناسید پروفایل شبکه اجتماعی شمو را ببینند.

بلدی مثال، پروفایل فیسبوک شمو.



این تنظیمات معمولاً تنظیمات حریم خصوصی نامیده می‌شود.



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

تنظیمات موقعیت مکانی نشان می‌دهد دستگاه شما کجاست.



شما می‌توانید تنظیمات موقعیت مکانی را خاموش یا روشن کنید.

همچنین می‌توانید انتخاب کنید کدام برنامه‌ها از تنظیمات موقعیت مکانی شما استفاده کنند.



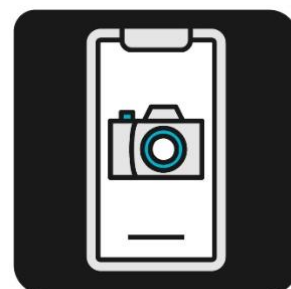
این کار را می‌توانید بلدی:

- حساب‌های آنلاین
- دستگاه‌ها
- برنامه‌ها انجام دهید.



بعضی برنامه ها ممکن است بپرسند آیا می‌توانند:

- از کمره تان استفاده کنید



- عکس های تانرا ببینید.



باید فقط به برنامه هایی که می‌شناسید اجازه استفاده از
کمره و عکس ها را بدهید.



از دستگاه های خود محافظت کنید

باید فکر کنید چگونه از دستگاه های خود محافظت کنید
تا آنلاین امن بمانید.

بلدی مثال، تلفون یا ساعت هوشمند شمو.



این موضوع بلدی دستگاه هایی که به اینترنت وصل
می شوند مهم است.



دستگاه های خود را به روزرسانی کنید

می توانید دستگاه های خود را بلدی امنیت آنلاین به روز
رسانی کنید.

بلدی مثال، تلفون یا ساعت هوشمند شمو.



ممکن است دستگاه شمو این را به نام به روز رسانی نرم
افزار یاد کند.





به روز رسانی ها به دستگاه کمک می‌کند تا از خود در برابر جرایم سایبری محافظت کند.



می توانید دستگاه را طوری تنظیم کنید که خود کار به روز رسانی شود.



در وبسایت مومی توانید معلومات بیشتر پیدا کنید.
www.actnowstaysecure.gov.au/cyber-safe-actions

شبکه های Wi-Fi عمومی



باید هنگام استفاده از **Wi-Fi عمومی** محتاط باشید.



Wi-Fi عمومی اینترنت بی سیم رایگان است که در مکان های عمومی استفاده می‌شود.

بلدی مثال در:

- قهوه خانه
- میدان هوایی
- هوتل.



باید در باره معلوماتی که هنگام استفاده از Wi-Fi عمومی وارد ویبسایت می‌کنید محتاط باشید.



بلدی مثال:

- معلومات بانکی
- حساب های ایمیل
- پروفایل های شبکه اجتماعی.



بعضی مجرمان سایبری می‌توانند از Wi-Fi عمومی بلدی

این کار ها استفاده کنند:

- دیدن فعالیت آنلاین شمو
- دزدیدن معلومات شمو.



زیرا:

- هر کسی می‌تواند از آن استفاده کند



- محافظت از دستگاه‌ها دشوارتر است.



شما می‌توانید در وب‌سایت [www.actnowstaysecure.gov.au/cyber-safe-](http://www.actnowstaysecure.gov.au/cyber-safe-actions) با استفاده از Wi-Fi عمومی امن بمانید.

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



کلاهبرداری ها

وقتی کسی تلاش کند، به آن **کلاهبرداری** می‌گوییم:

- شمو را فریب دهد
- پول شمو را بگیرد.



کلاهبردار کسی است که کلاهبرداری می‌کند.



ممکن است کلاهبرداران از این راه ها شمو را فریب دهند:

- پیامک یا تماس تلفونی
- ایمیل
- شبکه اجتماعی
- وب سایت.



ممکن است دوستانه به نظر برسند.

اما ممکن است شمو را فریب دهند تا معلومات خود را بدهید.



آنها می‌توانند از این معلومات بلدی این کارها استفاده کنند:

- ورود به حساب های آنلاین شمو



- خود را به جای شمو نشان دادن



- دزدیدن پول شمو.



کلاهبرداران همچنین ممکن است:

- حساب های جعلی بسازند



- لینک ها و اعلان هایی بلدی کلیک کردن بفرستند.



چگونه کلاهبرداری را تشخیص دهید

ممکن است کلاهبرداری باشد اگر:

- از شما بخواهد سریع کاری انجام دهید



- پول زیاد وعده بدهد



- از شما پول بخواهد



- از شما بخواهد روی لینک کلیک کنید.



کلاهبرداران ممکن است خود را سازمانی معرفی کنند که می‌شناسید و اعتماد دارید.

بلدی مثال، بانک شمو.



آنها این کار را می‌کنند تا معلومات شخصی خود را با آنان شریک سازید.



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



باید بررسی کنید شخص همان کسی است که می‌گوید. می‌توانید با استفاده از معلوماتی که خودتان پیدا کرده اید با شخص یا سازمان تماس بگیرید.



اگر چیزی نادرست به نظر می‌رسد، سریع اقدام کنید تا از خود محافظت نمایید.



گزارش کلاهبرداری

نظارت بر کلاهبرداری (Scamwatch) به استرالیایی ها

کمک می کند تا:

- کلاهبرداری ها را بشناسند
- کلاهبرداری ها را گزارش دهند.



نظارت بر کلاهبرداری همچنین به کسانی که قربانی

کلاهبرداری شده اند کمک می کند.



می توانید کلاهبرداری را در وب سایت نظارت بر

کلاهبرداری گزارش دهید.

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



صحبت کنید

باید در باره اینکه دیگران چگونه از خود آنلاین محافظت کنند صحبت کنید.



از جمله:

- گزارش جرایم سایبری



- شریک کردن معلومات خود با خانواده و دوستان.



مو توضیح خواهیم داد که چگونه میتوانید در صفحات ذیل صحبت کنید.



گزارش جرم سایبری

گزارش جرم سایبری به دولت کمک می‌کند تا:

- بفهمد مجرمان سایبری چگونه حمله می‌کنند



- از مردم بیشتری محافظت کند.



می‌توانید جرم سایبری را در وب سایت ReportCyber

گزارش دهید:

www.cyber.gov.au/report



با خانواده و دوستان در باره امنیت آنلاین صحبت کنید

باید نکات خود را با خانواده و دوستان در مورد امنیت آنلاین شریک کنید.

شما نیز می‌توانید از آنها یاد بگیرید.



شما می‌توانید با به اشتراک گذاشتن چیزی که در مورد امن ماندن آنلاین می‌دانید از خود و مردم اطرافتان محافظت کنید.



این موضوع همچنین مهم است که دستگاه‌ها را با دیگران شریک می‌کنید.



فهرست کلمات

این فهرست توضیح می‌دهد که کلمات **پررنگ** در این راهنما چه معنا دارند.

سایبری



سایبری یعنی چیزی که مربوط به اینترنت باشد.

جرم سایبری

جرم سایبری زمانی است که مجرم از اینترنت برای انجام جرم استفاده می‌کند.



بلدی مثال، ممکن است از اینترنت برای این کارها استفاده کنند.

- دزدی معلومات شخصی شمو
- تصرف حساب های آنلاین شمو.

تنظیمات موقعیت مکانی



تنظیمات موقعیت مکانی نشان می‌دهد دستگاه شمو کجا قرار دارد.

تأیید هویت چند مرحله ای (MFA)

زمانی است که شما هر بار بلدی ورود به MFA حساب خود از 2 یا بیشتر روش های مختلف استفاده می کنید.



عبارت رمز

عبارت رمز نوع قوی تر رمز عبور است. حدس زدن آن بلدی دیگران بسیار دشوار است.



Wi-Fi عمومی

Wi-Fi عمومی اینترنت بی سیم رایگان است که می توانید در مکان های عمومی از آن استفاده کنید.



کلاهبرداری ها

کلاهبرداری ها زمانی است که کسی تلاش می کند:

- شما را فریب بدهد
- پول شما را بگیرد.



کلاهبرداران

کلاهبرداران کسی است که کلاهبرداری می کند.



با مو تماس بگیرید

شماره می‌توانید با لین ویژه امنیت سایبری استرالیا تماس بگیرید.

1300 292 371



شماره می‌توانید از وب سایت مو دیدن کنید.

www.actnowstaysecure.gov.au



شماره می‌توانید جرم سایبری را در وب سایت ReportCyber گزارش دهید.

www.cyber.gov.au/report



گروه دسترسی معلومات (Information Access Group) این سند

آسان خوان را با استفاده از عکس های آماده و تصاویر سفارشی

تهیه کرده است. استفاده دوباره از این تصاویر مجاز نیست. بلدی هر

پرسشی در مورد عکس ها، لطفاً از

www.informationaccessgroup.com

دیدن نموده شماره کاری 6342 را ذکر کنید.

