



همین حالا اقدام کنید.
ایمن بمانید.



actnowstaysecure.gov.au

در فضای آنلاین چه چیزهای شما در معرض خطر قرار می‌گیرد؟

با پیشرفت سریع تکنولوژی و گذراندن وقت بیشتر در اینترنت، استرالیایی‌ها همچنان در برابر حملات سایبری آسیب‌پذیر هستند.

کمپاین همین حالا اقدام کنید. ایمن بمانید. به استرالیایی‌ها آموزش می‌دهد که چگونه با انجام چند کار ساده، خود را در فضای آنلاین محافظت کنند.

همین حالا اقدام کنید. ایمن بمانید.

چگونه در فضای آنلاین ایمن باشیم

برای هر حساب کاربری از یک عبارت عبور خاص و قوی استفاده کنید

استفاده از یک عبارت عبور خاص و قوی برای هر یک از حساب‌های آنلاین شما، یکی از مؤثرترین اقداماتی است که می‌توانید برای ایمن ماندن در فضای آنلاین انجام دهید.

عبارت عبور، رمز عبور امن‌تری است. این رمز عبور شامل سلسله‌ای از کلمات تصادفی است. به خاطر سپردن آنها برای شما آسان‌تر اما حدس زدن آنها برای مجرمان سایبری دشوارتر است.

برای قوی و خاص بودن، مطمئن شوید که عبارات عبور شما:

✓ چهار یا بیشتر کلمه تصادفی داشته باشند

✓ شامل 15 یا بیشتر حرف باشد

✓ برای هر حساب کاربری متفاوت باشد

✓ شامل معلومات قابل شناسایی مانند نام خانوادگی، تاریخ تولد یا آدرس نباشد

✓ سمبول‌ها، حروف بزرگ یا اعداد را، در صورتی که وبسایت یا خدمات تقاضا کند، شامل کنید.

برای ایجاد و ذخیره عبارات عبور خاص تان استفاده از مدیر رمز عبور را در نظر بگیرید.

برای ایمن نگه داشتن دستگاه‌های خود،

تمام به روزرسانی‌های نرم‌افزار را نصب کنید

برای ایمن نگه داشتن تان در فضای آنلاین بسیار مهم است که همیشه به‌روزرسانی‌های نرم‌افزاری را برای تمام دستگاه‌های متصل به اینترنت تان (مانند تلفون، لپ‌تاپ یا ساعت هوشمند) نصب کنید.

به‌روزرسانی‌های نرم‌افزاری، نقاط ضعف یا شکاف‌های امنیتی دستگاه‌های شما را برطرف می‌کنند. نصب منظم به‌روزرسانی‌ها نرم‌افزاری دستگاه‌های شما را ایمن نگه می‌دارد و دسترسی مجرمان سایبری به آنها را دشوارتر می‌کند.

به‌روزرسانی‌های خودکار را فعال کنید و حتماً در صورتی که درخواست شد، آن‌ها را نصب کنید.

همیشه تایید هویت چند عاملی را تنظیم کنید

در صورت امکان، تایید هویت چند عاملی را فعال کنید تا یک لایه امنیتی اضافی به همه حساب‌های آنلاین تان اضافه کنید.

تایید هویت چند عاملی برای ورود به حساب کاربری تان به دو یا چند روش تأیید ضرورت دارد. به عنوان مثال، پس از وارد کردن رمز عبور یا عبارت عبور، از شما خواسته می‌شود که یک تأیید هویت دوم مانند وارد کردن کدی را که از طریق یک برنامه تأیید هویت، ایمیل یا پیامک برای شما ارسال می‌شود ارائه دهید.

تایید هویت چند عاملی از حساب شما محافظت می‌کند حتی اگر یکی از روش‌های دیگر تایید هویت شما (مانند عبارت عبور) در معرض خطر قرار گیرد.

همین حالا اقدام کنید.
ایمن بمانید.



actnowstaysecure.gov.au



آیا راه‌های بیشتری برای امنیت آنلاین می‌خواهید؟

به دنبال راه‌های بیشتری برای حفظ امنیت سایبری هستید؟ در اینجا چند اقدام دیگر وجود دارد که می‌توانید برای محافظت از خود در فضای آنلاین انجام دهید.

هنگام استفاده از وای‌فای عمومی احتیاط کنید

وقتی از وای‌فای عمومی استفاده می‌کنید، از دسترسی به معلومات حساس یا خصوصی تان خودداری کنید، چون این نوع اتصال محفوظ نیست. این شامل حساب‌های رسانه‌های اجتماعی، ایمیل یا معاملات بانکی آنلاین شما می‌شود. هر معلوماتی را که شما وارد می‌کنید مجرمان سایبری می‌تواند با آن دسترسی پیدا کند.

تنظیمات حریم خصوصی و موقعیت مکانی خود را بطور منظم بررسی و به‌روزرسانی کنید

مهم است که تنظیمات حریم خصوصی و مکان خود را زیاد بررسی کنید تا مطمئن شوید که بطور تصادفی معلومات شخصی یا شناسایی خود را با عموم به اشتراک نمی‌گذارید.

تنظیماتی را که باید بررسی کنید شامل تنظیمات حریم خصوصی در حساب‌های رسانه‌های اجتماعی و ردیابی موقعیت مکانی در اپ‌ها و دستگاه‌های شما می‌شود.

با دوستان و خانواده تان در مورد چگونگی حفظ امنیت سایبری صحبت کنید

آموزش و آگاهی برای حفظ امنیت خود، خانواده و دوستان تان در فضای آنلاین بسیار مهم است - به خصوص اگر از دستگاه‌های متصل به اینترنت به صورت مشترک استفاده می‌کنید. صحبت در این مورد با اعضای شبکه تان، امنیت سایبری را در اولویت قرار می‌دهد و تضمین می‌کند که آنها آخرین معلومات را در مورد نحوه محافظت از خود در فضای آنلاین دریافت می‌کنند.

یاد بگیرید که چگونه یک کلاهبرداری را شناسایی کنید

کلاهبرداران مردم را فریب می‌دهند تا پول بپردازند یا معلومات شخصی خود را ارائه دهند.

اگر مطمئن نیستید که با چه کسی سرو کار دارید هرگز پول یا معلومات شخصی تان را به کسی ندهید. با استفاده از معلوماتی که از یک وب‌سایت یا اپ رسمی پیدا می‌کنید، با آن شخص یا سازمان تماس بگیرید و بررسی کنید.

حملات و حوادث سایبری را گزارش دهید

گزارش دادن کلاهبرداری‌ها یا حوادث سایبری خیلی مهم است تا دولت بتواند روال‌های جدید را شناسایی کند، جامعه را آگاه سازد و به شما کمک کند از حادثه سایبری بهبود یابید.

همین حالا اقدام کنید.
ایمن بمانید.



actnowstaysecure.gov.au

مراحل ساده برای محافظت از خود را در
actnowstaysecure.gov.au یاد بگیرید