Australian Government

actnowstaysecure.gov.au

Cosa rischi on-line?

Man mano che la tecnologia avanza rapidamente e si trascorre più tempo sulla rete, gli australiani rimangono vulnerabili agli attacchi cibernetici.

La campagna 'Act Now. Stay Secure' (Agisci subito. Rimani sicuro) educa gli australiani in merito a semplici azioni sicure in campo cibernetico che tutti possono adottare per proteggersi on-line.

Agisci subito. Rimani sicuro.

Come essere sicuro/a on-line

Usa una passphrase univoca e forte per ogni conto

L'uso di una passphrase univoca e forte per ciascuno dei tuoi conti on-line è una delle azioni più efficaci che puoi intraprendere per rimanere sicuro/a on-line.

Una passphrase è una password più sicura. Contiene una sequenza di parole randomizzate. Sono più facili per te da ricordare ma più difficili per i criminali cibernetici da indovinare.

Per essere forti e univoche, devi fare in modo che le tue passphrase:

- ✓ abbiano quattro o più parole randomizzate
- ✓ contengano 15 o più caratteri
- ✓ siano differenti per ogni conto
- ✓ non includano dati identificativi come nomi, date di nascita o indirizzi di familiari
- ✓ includano simboli, lettere maiuscole o numeri se richiesto dal sito web o servizio.

Considera l'uso di un password manager per creare e conservare le tue passphrase univoche.

Installa tutti gli aggiornamenti del software per tenere sicuri i tuoi dispositivi

L'installazione periodica di tutti gli aggiornamenti del software per tutti i tuoi dispositivi connessi a internet (come telefonino, computer portatile o smart watch) è di fondamentale importanza per tenerti al sicuro on-line.

Gli aggiornamenti del software aggiustano i punti deboli o le lacune nella sicurezza dei tuoi dispositivi. L'installazione periodica degli aggiornamenti terrà i tuoi dispositivi sicuri e renderà più difficile l'accesso agli stessi da parte di criminali cibernetici.

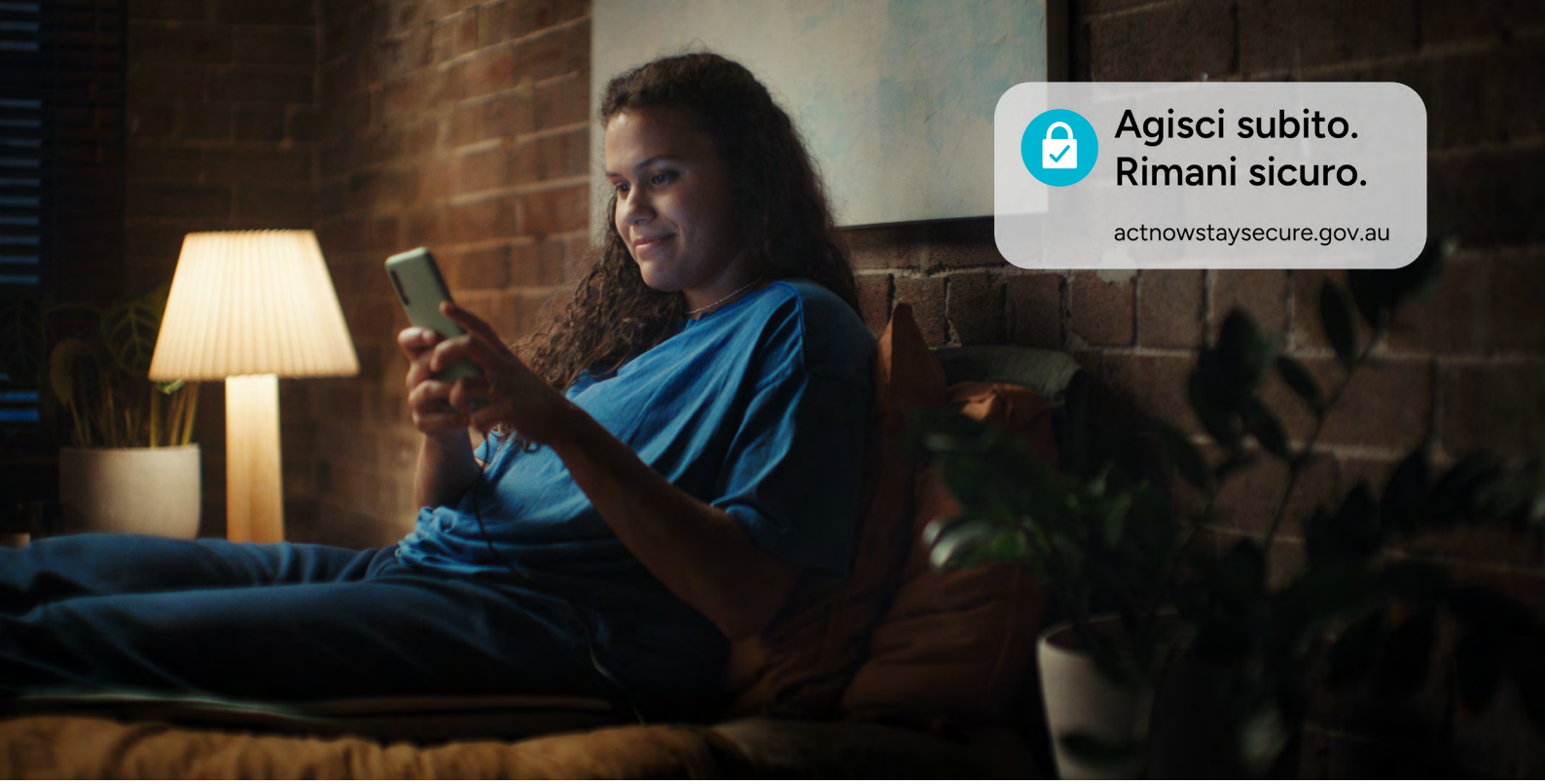
Attiva gli aggiornamenti automatici e sincerati di installarli quando vieni sollecitato/a a farlo.

Imposta sempre una autenticazione multifattoriale

Attiva l'autenticazione multifattoriale, ove disponibile, per aggiungere un ulteriore strato di sicurezza a tutti i tuoi conti on-line.

L'autenticazione multifattoriale richiede due o più metodi di verifica per accedere al tuo conto. Ad esempio, dopo avere inserito la tua password o passphrase, verrai sollecitato/a a fornire una seconda verifica come un codice inviatoti tramite una app autenticatrice, una mail o un messaggio testuale.

L'autenticazione multifattoriale protegge il tuo conto anche se uno degli altri tuoi metodi di autenticazione (ad esempio una passphrase) è compromesso.



Vuoi ulteriori modi di essere sicuro/a on-line?

Cerchi ulteriori modi di rimanere sicuro/a on-line? Ecco alcune altre azioni che puoi intraprendere per proteggerti on-line.

Fai attenzione quando usi un Wi-Fi pubblico

Quando usi un Wi-Fi pubblico, non accedere a informazioni sensibili o private in quanto la connessione non è sicura. Questo vale per i tuoi social, posta elettronica o operazioni bancarie on-line. Qualsiasi informazione che inserisci potrebbe essere accessibile a criminali cibernetici.

Controlla e aggiorna periodicamente le tue impostazioni in materia di privacy e posizione

È importante controllare con una certa frequenza le tue impostazioni in materia di privacy e posizione per sincerarti di non condividere accidentalmente con il pubblico dati che ti riguardano.

Le impostazioni da controllare comprendono le impostazioni relative alla privacy sui tuoi social e il tracciamento di geolocalizzazione sulle tue app e sui tuoi dispositivi.

Parla della sicurezza informatica con amici e familiari

Educazione e sensibilizzazione sono di fondamentale importanza per tenere te stesso/a, familiari e amici sicuri on-line – soprattutto se voi condividete dispositivi connessi a internet. Parlarne con la tua rete fa della sicurezza informatica un aspetto prioritario e fa in modo che gli appartenenti a tale rete ricevano le ultime informazioni su come proteggersi on-line.

Impara a individuare una truffa

I truffatori ingannano le persone a versare somme di denaro o a fornire i propri dati personali.

Non dare mai soldi o dati personali a nessuno se non sei sicuro/a della persona con cui stai trattando. Controlla rivolgendoti alla persona o all'ente usando i recapiti che trovi su un sito o app ufficiale.

Denuncia attacchi o incidenti cibernetici

La denuncia di truffe o incidenti cibernetici è di vitale importanza per aiutare il governo a individuare nuove tendenze, mettere in allerta la comunità e aiutarti a riprenderti da un incidente cibernetico.

Impara semplici misure da adottare per proteggerti visitando il sito actnowstaysecure.gov.au

Agisci subito.
Rimani sicuro.

actnowstaysecure.gov.au