



Australian Government



Agisci subito. Rimani sicuro.

Come proteggerti online

Versione facile da leggere



Come utilizzare questa guida



Noi siamo il governo australiano.

Siamo stati noi a scrivere questa guida.



Abbiamo scritto alcune parole in **grassetto**.

Ti spieghiamo cosa significano quelle parole.

C'è anche un elenco di tali parole a pagina 28.



Puoi chiedere ad una persona di fiducia di aiutarti a:

- leggere questa guida
- trovare maggiori informazioni.



Questa è una sintesi facile da leggere che riassume un'altra guida.

Contiene solo i concetti più importanti.



Puoi trovare l'altra guida sul nostro sito web.

www.actnowstaysecure.gov.au

Cosa contiene questa guida?

Informazioni su questa guida	4
------------------------------	---

Proteggi i tuoi account	6
-------------------------	---

Controlla le tue impostazioni per proteggere i tuoi dati	10
--	----

Proteggi i tuoi dispositivi	16
-----------------------------	----

Truffe	20
--------	----

Fai sentire la tua voce	25
-------------------------	----

Glossario	28
-----------	----

Contattaci	30
------------	----

Informazioni su questa guida



Tutti noi dobbiamo riflettere su come proteggerci online.

Si chiama sicurezza **informatica**.



Informatica vuol dire che ha a che fare con internet.



Questa scheda informativa spiega alcune cose che puoi fare per proteggerti online.

Ad esempio dal **cyber crime** (ovvero la criminalità informatica).



Il cyber crime avviene quando dei criminali usano internet per commettere reati.

Ad esempio, quando utilizzano internet per:

- rubare i tuoi dati personali
- appropriarsi dei tuoi profili e account online.

Il cyber crime può avvenire su qualsiasi dispositivo.



Incluso il tuo:

- computer
- telefono
- orologio smart.



Ci sono cose che puoi fare per proteggerti dal cyber crime.



Ti spieghiamo cosa puoi fare nelle pagine successive.

Proteggi i tuoi account



Dovresti pensare a come mantenere sicuri i tuoi account in rete.

Usa frasi di accesso forti e diverse



Una **frase di accesso** è un tipo di password più forte.

È molto difficile da indovinare per gli altri.



Usare frasi di accesso forti e diverse è uno dei modi migliori per proteggere i tuoi account.



Dovresti usare una frase di accesso diversa per ognuno dei tuoi account online.



Frasi di accesso forti comprendono:

- almeno 4 parole casuali
- almeno 15 tra lettere e numeri.



Puoi includere alcune lettere maiuscole.



Puoi anche usare dei simboli come:

- un trattino
- il simbolo del dollaro
- la chiocciola @ delle email.



Non dovresti mai usare dati personali nelle tue frasi di accesso.



Ad esempio:

- il tuo compleanno
- i nomi dei tuoi familiari o animali domestici.

Includi misure aggiuntive per accedere ai tuoi account



Puoi proteggere i tuoi account online con
l'autenticazione a più fattori (MFA).

MFA avviene quando utilizzi almeno 2 modi
diversi per accedere al tuo account



Per esempio, digitando prima la tua frase di
accesso.

Poi, digitando un codice che ti arriva sul telefono.

Potresti scegliere tra:



- scaricare un'applicazione sul tuo telefono per ricevere il codice



- ricevere il codice via email



- ricevere il codice in un messaggio di testo.



MFA rende più difficile per gli altri accedere ai tuoi account online.

Anche se scoprono la tua frase di accesso.

Controlla le tue impostazioni per proteggere i tuoi dati



Puoi controllare che le tue impostazioni stiano proteggendo i tuoi dati online.



Incluse le tue impostazioni di:

- account online
- dispositivi
- applicazioni.



Puoi:

- cambiare le tue impostazioni
- scegliere quali applicazioni possono usare i tuoi dati.

Per trovare le impostazioni sul tuo dispositivo puoi:



- cercare l'icona dell'ingranaggio
- oppure
- digitare 'impostazioni' nel campo di ricerca del tuo dispositivo.



Puoi trovare le impostazioni di un'applicazione o di un account online aprendo il menù.

Il menù ha spesso il simbolo con 3 linee dritte.



Alcune di queste impostazioni possono condividere informazioni su:

- chi sei
- dove sei
- dove vivi.



Condividere queste informazioni online può esporti a rischio di cyber crime.



I criminali informatici possono usare i tuoi dati per fingere di essere te.

Per esempio, potrebbero usare informazioni come:



- dove vivi



- i nomi dei tuoi familiari



- il nome dei tuoi animali domestici.



Puoi impostare i tuoi account in modo che solo le persone che conosci possano vedere i tuoi profili sui social.

Per esempio, il tuo profilo Facebook.



Queste impostazioni di solito si chiamano impostazioni sulla privacy.



Puoi anche gestire le tue **impostazioni di posizione**.

Le impostazioni di posizione mostrano dove si trova il tuo dispositivo.



Puoi attivare o disattivare le impostazioni di posizione.

Puoi anche scegliere quali applicazioni possono utilizzare le tue impostazioni di posizione.



Questo lo puoi fare per:

- i tuoi account online
- i tuoi dispositivi
- le tue applicazioni.

Alcune applicazioni potrebbero anche chiederti di poter:



- usare la tua fotocamera



- visualizzare le tue foto.



Dovresti consentire di visualizzare le tue foto solo alle applicazioni che conosci.

Proteggi i tuoi dispositivi



Dovresti pensare a come puoi proteggere i tuoi dispositivi per rimanere al sicuro online.

Ad esempio il tuo telefono o l'orologio smart.



Questo è importante per i dispositivi che si collegano a internet.

Aggiorna i tuoi dispositivi



Puoi aggiornare i tuoi dispositivi per mantenerli sicuri online.

Ad esempio, il tuo telefono ed il computer portatile.



Il tuo dispositivo potrebbe chiamarlo aggiornamento del software.



Gli aggiornamenti aiutano un dispositivo a proteggersi dal cyber crime.



Puoi impostare un dispositivo in modo che si aggiorni da solo.



Puoi saperne di più su come aggiornare i tuoi dispositivi sul nostro sito web.

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

Reti Wi-Fi pubbliche



Dovresti fare attenzione quando usi il **Wi-Fi pubblico**.



Il Wi-Fi pubblico è la connessione internet gratuita e senza fili che puoi usare nei luoghi pubblici.



Ad esempio in un:

- bar
- aeroporto
- albergo.



Dovresti fare attenzione alle informazioni che inserisci su un sito web quando usi il Wi-Fi pubblico.



Ad esempio i tuoi:

- dati bancari
- indirizzi email
- profili social.



Alcuni criminali informatici usano il Wi-Fi pubblico per:

- vedere cosa stai facendo online
- rubare i tuoi dati.

Questo perchè:



- chiunque può utilizzarlo



- è più difficile proteggere i tuoi dispositivi.



Puoi scoprire come rimanere protetto quando usi il Wi-Fi pubblico sul nostro sito web.

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

Truffe



Parliamo di **truffe** quando qualcuno cerca di:

- ingannarti
- prendere i tuoi soldi.



Un **truffatore** è qualcuno che commette truffe.

I truffatori potrebbero ingannarti attraverso:



- un messaggio di testo o una telefonata
- un'email
- i social media
- un sito web.



Potrebbero sembrare cordiali.

Ma ti potrebbero ingannare per farti dare i tuoi dati.

Possono utilizzare i tuoi dati per:



- accedere ai tuoi account online



- fingere di essere te



- rubare i tuoi soldi.

I truffatori potrebbero anche:



- creare account falsi per ingannarti



- condividere link e annunci pubblicitari da farti cliccare.

Come riconoscere una truffa

Potrebbe trattarsi di una truffa se:



- ti chiedono di fare qualcosa velocemente



- ti offrono molti soldi



- ti chiedono dei soldi



- ti chiedono di cliccare su un link.



I truffatori potrebbero anche fingere di essere un'organizzazione che conosci e di cui ti fidi.

Ad esempio, la tua banca.



I truffatori fanno questo per convincerti a condividere le tue informazioni personali con loro.



Dovresti smettere di parlare con la persona che pensi sia un truffatore.



Dovresti verificare che quella persona sia effettivamente chi dice di essere.

Puoi contattare la persona o l'organizzazione usando recapiti fidati e che hai trovato personalmente.



Se qualcosa ti sembra sospetto, agisci velocemente per proteggerti.

Segnalare una truffa



Scamwatch aiuta gli australiani a:

- capire le truffe
- segnalare le truffe.



Scamwatch aiuta anche gli australiani che sono stati truffati.



Puoi segnalare una truffa tramite il sito Scamwatch.

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

Fai sentire la tua voce



È importante parlare di come ci si può proteggere online.

Puoi:



- segnalare crimini informatici



- condividere quello che sai con familiari e amici.



Ti spiegheremo nelle prossime pagine come puoi far sentire la tua voce.

Segnala il cyber crime

Segnalare crimini informatici aiuta il governo a:



- capire come i criminali informatici cercano di attaccare le persone



- proteggere più persone.



Puoi segnalare un crimine informatico tramite il sito ReportCyber.

www.cyber.gov.au/report

Parla con familiari ed amici della sicurezza online



Dovresti condividere i tuoi consigli sulla sicurezza online con familiari ed amici.

Puoi anche imparare da loro.



Puoi proteggere te stesso e le persone vicino a te condividendo ciò che sai sulla sicurezza online.



Questo è anche importante se condividi dei dispositivi con altri.

Glossario

Questo elenco spiega il significato delle parole in **grassetto** contenute in questa scheda informativa.



Cyber

Cyber vuol dire che qualcosa ha a che fare con internet.



Cyber crime

Il cyber crime avviene quando dei criminali usano internet per commettere reati.

Ad esempio, quando utilizzano internet per:

- rubare i tuoi dati personali
- appropriarsi dei tuoi profili e account online.



Impostazioni di posizione.

Le impostazioni di posizione mostrano dove si trova il tuo dispositivo.



Autenticazione a più fattori (MFA).

MFA avviene quando utilizzi almeno 2 modi diversi per accedere al tuo account.



Frase di accesso

Una frase di accesso è un tipo di password più forte.

È molto difficile per gli altri da indovinare.



Wi-Fi pubblico

Il Wi-Fi pubblico è la connessione internet gratuita e senza fili che puoi usare nei luoghi pubblici.



Truffe

Parliamo di truffa quando qualcuno cerca di:

- ingannarti
- prendere i tuoi soldi.



Truffatori

Un truffatore è qualcuno che commette truffe.

Contattaci



Puoi chiamare la Australian Cyber Security Hotline (ovvero la linea di assistenza per la sicurezza informatica australiana).

1300 292 371



Puoi visitare il nostro sito web.

www.actnowstaysecure.gov.au



Puoi segnalare un crimine informatico tramite il sito ReportCyber.

www.cyber.gov.au/report



L'Information Access Group ha creato questo documento facile da leggere usando foto stock e immagini personalizzate. Le immagini potrebbero non essere riutilizzabili senza permesso. Per informazioni in merito alle immagini, visita www.informationaccessgroup.com. Cita il numero di riferimento 6342.
