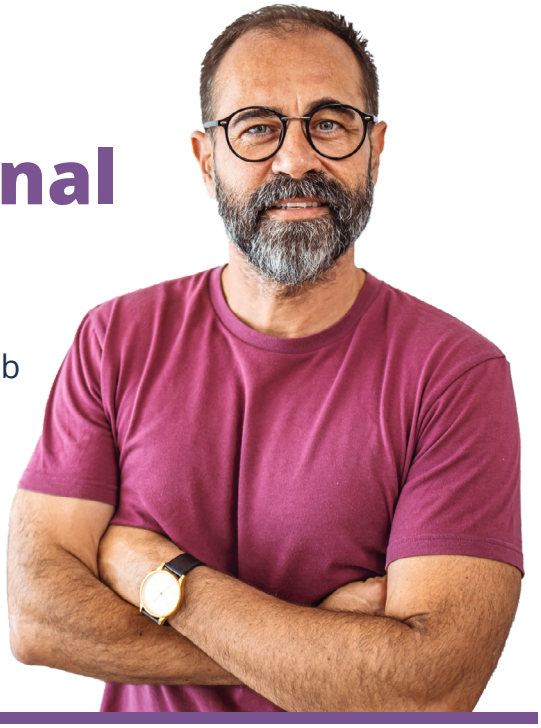
Riepilogo della presentazione online

Australian Government

Be Connected
Every Australian online.

Protezione dei tuoi dati personali online (Protecting your personal information online)



Quasi tutte le app, le piattaforme di social media o i siti web chiedono di condividere alcuni dati personali. I tuoi dati personali includono qualsiasi dato o informazione che può essere utilizzato per identificarti, come dati relativi a dove ti trovi o dove vivi e altri dati unici e specifici. Prima di condividere dati personali, è sempre importante pensarci due volte.

La protezione dei tuoi dati personali è importante

La protezione dei tuoi dati personali è molto importante in quanto truffatori e ladri di identità possono utilizzarli per fingere di essere te. I truffatori possono creare account falsi a tuo nome e agire in modi che potrebbero avere un impatto su di te ora o in futuro, Come per esempio compiendo delle frodi, sottraendoti denaro dal tuo conto bancario o sottoscrivendo un prestito a tuo nome.

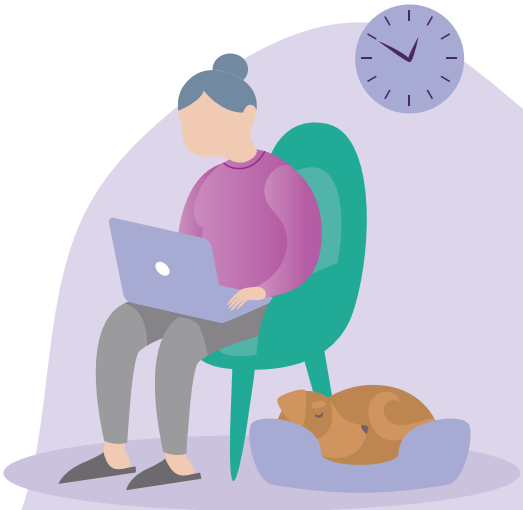
I truffatori possono utilizzare i tuoi dati da soli o nel contesto di altre informazioni. Ciò può includere informazioni che usi quotidianamente e che ti riguardano nello specifico, come ad esempio:

Dati personali

- Nome completo
- Indirizzo di residenza
- Numero di telefono
- Data di nascita
- Numero della patente di guida
- Coordinate bancarie
- Indirizzo e-mail
- Nomi utente e password

Documenti d'identità

- Patente di guida
- Passaporto
- Certificato di nascita
- Tessera Medicare
- Visto australiano o certificato di cittadinanza
- ImmiCard



Sii consapevole di ciò che condividi

Social media

Evita di condividere dati personali sui tuoi profili social. I truffatori possono imparare molto su di te dai dettagli che condividi online. A volte, i truffatori creano quiz o post contenenti domande progettati per indurti a condividere informazioni personali. Usano queste informazioni per indovinare le tue password o per prenderti di mira con altre truffe.

Utilizzo delle app

Scarica le app solo dagli app store ufficiali e leggi le politiche sulla privacy e le recensioni prima di scaricarle. Puoi anche decidere di limitare le informazioni a cui le app hanno accesso. Alcune app richiedono accesso non necessario all'elenco dei tuoi contatti, alla fotocamera, alla memoria, alla posizione GPS e al microfono. Controlla e modifica le autorizzazioni delle app nel menu delle impostazioni sul tuo dispositivo.

Ricorda: accetta solamente richieste di amicizia da persone che conosci nella vita reale, imposta i tuoi account sui social media come privati e verifica chi può vedere quello che condividi.

Mantieni le tue informazioni al sicuro

Utilizza i sistemi di sicurezza del tuo dispositivo

L'utilizzo di software di sicurezza sul tuo computer è uno dei modi più semplici per proteggere te e la tua privacy. Una buona sicurezza informatica include l'installazione di antispyware affidabili, così come quella di software antivirus e firewall. È inoltre una buona idea mantenere aggiornati i tuoi strumenti di sicurezza e le tue app abilitando gli aggiornamenti automatici. Utilizza il blocco dello schermo automatico e temporizzato oppure un salvaschermo protetto da password e imposta un blocco automatico quando vengono effettuati più tentativi di accesso non andati a buon fine.

Suggerimento: un'app di gestione delle password può anche aiutarti a creare e archiviare frasi di accesso complesse che sono difficili da indovinare o hackerare. Puoi trovare informazioni sui **gestori di password** e su come configurarli sul sito web di Be Connected.

Frasi di accesso

Mantieni i tuoi account al sicuro utilizzando frasi di accesso complesse. Le frasi di accesso sono una versione più sicura delle password e sono composte da quattro o più parole casuali.

Prova a pensare a una frase di accesso diversa per ciascuno dei tuoi account e non riutilizzare parti di frasi di accesso che hai già utilizzato.

Quando scegli la tua frase di accesso, rendila:

- **lunga:** utilizza almeno 14 caratteri;
- **imprevedibile:** utilizza quattro o più parole casuali con numeri, simboli e lettere maiuscole e minuscole;
- **unica:** non riutilizzare le stesse frasi d'accesso.

*Per esempio: Giallo Così Ciao Albero > Giallo!C*sì-Ciao @lbero!*

Suggerimento: controlla la sicurezza di una password utilizzando lo strumento ideato dal Governo del NSW per verificare la sicurezza delle password all'indirizzo **nsw.gov.au/id-support-nsw/be-prepared/passwords**

Autenticazione a più fattori

È sempre una buona idea attivare l'autenticazione a più fattori per i tuoi account. L'autenticazione a più fattori (nota anche come verifica in due passaggi) aggiunge un ulteriore livello di sicurezza. Ciò significa che quando accedi a un account utilizzando la tua password, ti potrebbe essere chiesto di effettuare un'ulteriore verifica per confermare che sia tu a richiedere l'accesso, come inserire un codice da un messaggio di testo o procedere con il riconoscimento facciale.

Acquista online in modo sicuro

Quando fai acquisti online, assicurati di utilizzare venditori affidabili e di consultare le recensioni dei clienti. Prima di inserire i tuoi dati personali, controlla che il sito web utilizzi "https" all'inizio del nome del suo dominio o abbia un'icona di sicurezza, di solito un piccolo lucchetto chiuso che puoi visualizzare nel browser e che indica che si tratta di un sito web più sicuro. Quando effettui un acquisto, utilizza un metodo di pagamento sicuro come PayPal, BPAY o la tua carta di credito.

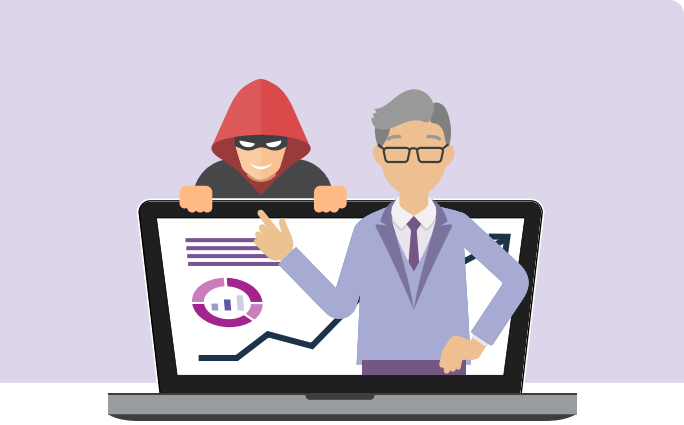
Usa una connessione sicura

Quando devi accedere ad account importanti, inviare informazioni sensibili o inserire password, utilizza una connessione internet affidabile, come quella che hai a casa o al lavoro, oppure utilizza i dati del tuo piano mobile, se disponibili. Il Wi-Fi pubblico non è sicuro come il Wi-Fi che hai a disposizione a casa o al lavoro.

Truffe e violazioni dei dati

Proteggiti dalle truffe

Essere consapevoli delle truffe e di come funzionano è una delle azioni importanti da intraprendere per evitarle. I truffatori fingono di appartenere a un'organizzazione o a una persona che conosci per cercare di indurti con l'inganno a consegnare i tuoi dati personali. Queste sono chiamate truffe di impersonificazione.



Ricorda:

Fermati: se non sei sicuro, non dare denaro e non condividere dati personali con nessuno
I truffatori spesso ti chiedono di verificare chi sei o di effettuare un pagamento.

Pensa: chiediti se il messaggio o la chiamata potrebbero essere falsi.
Fai attenzione a chiamate, messaggi ed e-mail inaspettate. Se non sei sicuro di un messaggio, chiama direttamente l'organizzazione utilizzando il numero di telefono che trovi sul suo sito web.

Proteggi: se senti che qualcosa non va, agisci rapidamente.
Se noti dell'attività insolita sul tuo conto corrente o se un truffatore riesce a sottrarti dei soldi o delle informazioni, contatta la tua banca.

Suggerimento: visita il sito web Be Connected per consultare la nostra **guida gratuita alle truffe** di impersonificazione sviluppata in collaborazione con Scamwatch.

Violazioni dei dati

Una violazione dei dati si verifica quando le informazioni personali detenute da un'organizzazione diventano accessibili o vengono divulgate senza autorizzazione oppure quando vengono perse. Molte organizzazioni e agenzie governative hanno la responsabilità legale di informarti se i tuoi dati personali fanno parte di una violazione che potrebbe causarti gravi danni.

Se i tuoi dati fanno parte di una violazione, assicurati di agire rapidamente e di ottenere consigli dall'**Office of the Australian Information Commissioner**. Le azioni che dovrai intraprendere dipenderanno dai dati compromessi. Tieni un registro di ciò che fai. Puoi ottenere supporto e consulenza gratuiti anche da **IDCARE**.

Per scoprire se un sito o un'app che utilizzi ha subito una violazione dei dati, puoi controllare servizi come **haveibeenpwned.com**. Se il servizio conferma che i tuoi dati sono stati violati, cambia subito le tue password.

Furto d'identità

Se sai o sospetti di essere vittima di un furto d'identità:

- fai una segnalazione all'Australian Cyber Security Centre dell'Australian Signals Directorate utilizzando **ReportCyber**;
- contatta la polizia al 131 444; chiedi alla polizia di rilasciarti un numero di riferimento come prova che hai effettuato una segnalazione;
- se conosci o sospetti il tipo di informazioni personali che sono state violate, contatta l'agenzia o l'organizzazione competente per farglielo sapere;
- comunicalo al tuo istituto finanziario il prima possibile;
- fai una segnalazione al National Anti-Scam Centre (Centro Nazionale Anti Truffa) di **Scamwatch** se il furto dei dati fa parte di una truffa.

Prenditi del tempo per scoprire Be Connected

Be Connected è un sito web completo con risorse gratuite specificamente progettate per supportare gli australiani anziani a connettersi online in modo sicuro e a navigare nel mondo digitale con fiducia. Il sito è utile anche per le famiglie e le organizzazioni comunitarie che vogliono aiutare i membri anziani della comunità ad accedere a tutti i vantaggi offerti da Internet.

Visita il sito beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Questo programma è stato sviluppato da eSafety nell'ambito dell'iniziativa Be Connected.