Riepilogo della presentazione online

Australian Government

Be Connected
Every Australian online.

Gestire le tue e-mail in sicurezza (Managing your emails safely)

Disporre di un indirizzo e-mail ti dà accesso al mondo online. Ti consente di rimanere in contatto con familiari e amici e di accedere a servizi come gli acquisti online e i servizi bancari. È importante mantenere il tuo account e-mail il più sicuro possibile, utilizzando una frase d'accesso difficile da indovinare e l'autenticazione a più fattori.

Modi per accedere alla posta elettronica

Ci sono molti modi per accedere alle tue e-mail. Puoi farlo tramite:

Un'app:

- utilizza l'app del fornitore di servizi di posta elettronica che puoi scaricare dall'App Store per dispositivi Apple o dal Play Store per dispositivi Android;
- collega il tuo account e-mail:
  - all'app di posta preinstallata sul tuo dispositivo;
  - all'app Mail o Outlook sul tuo computer.

Sito web:

- accedi al sito web del tuo fornitore di servizi di posta elettronica da un browser sul tuo computer o dal tuo dispositivo.

Fornitori di servizi di posta elettronica

Esistono molti fornitori di servizi di posta elettronica che offrono opzioni di account di posta elettronica gratuita e a pagamento, tra cui:

- **Gmail** Google
- **Outlook** Microsoft
- **Yahoo Mail** Yahoo
- **iCloud** Apple
- **ProntonMail** Proton AG

Visita il sito web Be Connected per **guide dettagliate** su come configurare e utilizzare Gmail, Outlook e Yahoo.

Suggerimento: potresti voler configurare un account di posta elettronica solo per la tua banca oppure da utilizzare solo per lo shopping online per aiutare a gestire le e-mail indesiderate.

Gestire il tuo account di posta elettronica

Impostazione di cartelle ed etichette

Configurare le cartelle nella tua casella di posta è un ottimo modo per mantenere organizzato il tuo account e rendere più facile individuare le e-mail importanti quando ne hai bisogno. Le cartelle sono talvolta chiamate etichette, a seconda del servizio di posta elettronica utilizzato.

Organizzare e archiviare le e-mail

Il tuo servizio di posta elettronica dispone di comodi comandi che ti aiutano a archiviare le e-mail in modi diversi e a ridurre al minimo lo spam e la posta indesiderata. Quando arriva una nuova e-mail e la apri per leggerla, alcuni comandi appaiono nella parte superiore dello schermo. Puoi fare clic su questi comandi per:

- **eliminare**: sposta l'e-mail nel cestino;
- **archiviare**: sposta l'e-mail in una cartella di archiviazione;
- **contrassegnare come non letto**: permette di fare in modo che l'e-mail appaia come se fosse stata appena ricevuta;
- **etichettare / catalogare**: permette di etichettare l'e-mail o di spostarla in una cartella.

Gestire le e-mail indesiderate (spam)

Il tuo servizio di posta elettronica rileva e sposta automaticamente le e-mail di spam in una cartella apposita, ma alcune e-mail posso essere in grado di superare i filtri impostati.

Se ritieni che un'e-mail nella tua casella di posta elettronica sia indesiderata o spam, puoi:

- **segnalare l'e-mail come spam**: questa azione comunica al tuo fornitore di servizi di posta elettronica che l'e-mail è indesiderata;
- **bloccare l'e-mail**: questa azione blocca la ricezione di e-mail da parte del mittente;
- **annullare l'iscrizione**: questa azione ti permette di non ricevere più le newsletter o le e-mail di marketing a cui avevi precedentemente effettuato l'iscrizione.

Se ritieni di aver annullato l'iscrizione ma continui a ricevere e-mail indesiderate, puoi presentare un reclamo all'**Autorità australiana per le comunicazioni e i media**.

> **Suggerimento:** per evitare di ricevere e-mail indesiderate, fai attenzione a non fornire le tue informazioni per concorsi o a dare inavvertitamente il tuo consenso per ricevere e-mail di marketing quando acquisti prodotti o servizi.

Mantieni al sicuro il tuo account e-mail

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

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.

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 i tuoi account e dispositivi. 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.

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.

Opzioni di recupero dell'account

Assicurati di impostare un numero di telefono di recupero o un indirizzo e-mail alternativo per tutti i tuoi account e-mail. Se perdi l'accesso al tuo account o nel caso in cui questo venga compromesso, puoi reimpostare la password utilizzando l'opzione di recupero.

Truffe tramite e-mail

Le truffe tramite e-mail sono progettate per sembrare provenienti da organizzazioni legittime che conosci. Possono sembrare reali grazie all'utilizzo di loghi e di un indirizzo e-mail simile a quello dell'organizzazione che stanno impersonando. Le e-mail di truffa possono sembrare provenienti dalla tua banca, da un fornitore di servizi Internet, da un'agenzia governativa, da un rivenditore o persino da un truffatore che finge di essere un amico o un familiare. Inviandoti un'e-mail che finge di provenire da qualcuno di cui ti fidi, i truffatori usano un senso di urgenza per indurti a pagare denaro o fornire informazioni personali, come password importanti, carte di credito o dati bancari.

Questi tipi di truffe sono chiamate truffe di impersonificazione o e-mail di phishing.

Suggerimenti per evitare le truffe tramite e-mail

- Presta attenzione ai segni di una truffa tramite e-mail. Queste e-mail possono:
  - cercare di comunicare un senso di urgenza o utilizzare tattiche intimidatorie, richiedere un pagamento o chiederti di confermare i dati personali;
  - utilizzare saluti generici come “Gentile cliente”, “Gentile utente” oppure nessun saluto;
  - chiederti di cliccare su un link o scaricare un file, che potrebbe indirizzarti a un sito web fraudolento o contenere un virus o un malware.
- Controlla sempre che l’indirizzo e-mail del mittente sia legittimo e contatta direttamente l’organizzazione cercando il suo sito web e il suo numero di telefono ufficiali.
- Non accedere mai ai tuoi account online,non verificare i dettagli tramite un link contenuto in un’e-mail, non fare clic su link e non aprire allegati inviati tramite e-mail da mittenti sconosciuti o sospetti.
- Elimina le e-mail sospette o che possono costituire una truffa, utilizza l’opzione “segnala spam” per classificarle come e-mail indesiderate.

Suggerimento: se non sei sicuro della provenienza di un’e-mail, parla con un amico fidato o un familiare e contatta l’organizzazione utilizzando il numero di telefono che trovi sul loro sito web.

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

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 dall’eSafety Commissioner nell’ambito dell’iniziativa Be Connected.