Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

COME USARE INTERNET IN MODO SICURO

GUIDA PER ANZIANI

cyber.gov.au

Introduzione

L'uso di internet ti consente di rimanere in contatto con amici e familiari, informarti su vari argomenti e persino cimentarti in giochi elettronici.

Così come ti allacci la cintura prima di metterti al volante, dovresti adottare precauzioni prima di usare internet in modo da essere più sicuro.

L'Australian Cyber Security Centre (ACSC) vuole fare in modo che tutti siano al sicuro quando usano internet. Questo documento tratta di alcuni semplici accorgimenti in materia di sicurezza informatica che puoi adottare per proteggerti quando vai su internet.

L'Australian Cyber Security Centre (ACSC), in veste di organo dell'Australian Signals Directorate (ASD), offre consigli, assistenza e risposte operative per prevenire, individuare e eliminare minacce informatiche a danno dell'Australia. Ruolo dell'ACSC è di rendere l'Australia il luogo più sicuro al mondo per chi usa internet.

Per maggiori informazioni, guide e consigli in materia di sicurezza informatica, visita il sito cyber.gov.au

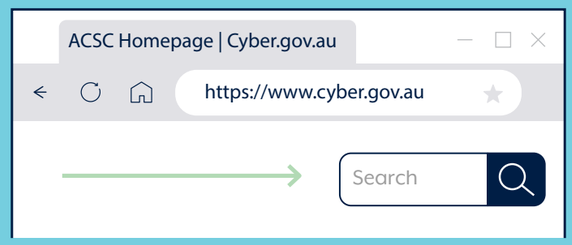
Sicurezza informatica per anziani

Suggerimento n. 1: Aggiorna il tuo dispositivo

Fare l'aggiornamento del tuo software è come fare la manutenzione della tua auto. In tal modo rendi il tuo dispositivo più efficiente e più sicuro.

I criminali informatici trovano sempre nuovi modi per attaccare i dispositivi elettronici. L'impostazione del tuo dispositivo in modo che installi gli aggiornamenti automaticamente, può rimediare a eventuali punti deboli nel software e tenere alla larga gli hacker.

Per maggiori informazioni, cerca "Updates" su cyber.gov.au



LO SAPEVI:

Gli aggiornamenti possono anche aggiungere nuove funzioni al dispositivo e renderlo più veloce.

Suggerimento n. 2: Attiva l'autenticazione a più fattori

Per il tuo account, l'autenticazione a più fattori è come una porta blindata per la tua casa.
Ti protegge da criminali che cercano di compiere un furto con scasso.

Con l'autenticazione a più fattori attivata, dovrai fornire molteplici informazioni per accedere al tuo account. Ad esempio, potresti dover inserire una password e un codice a messaggio testuale per entrare nel tuo profilo sui social media.

I molteplici strati rendono un attacco da parte di criminali informatici più difficile. Potrebbero riuscire a indovinare un fattore dell'autenticazione, ad esempio la password, ma dovranno pur sempre indovinare altre parti del 'rompicapo' per accedere al tuo account.

Per maggiori informazioni, cerca "Multi-factor authentication" o "MFA" su cyber.gov.au

RICORDA:

Se ti serve aiuto per attivare l'autenticazione a più fattori, rivolgiti ad un amico o familiare.

Suggerimento n. 3: Fai il backup del tuo dispositivo

Fare il 'backup' significa fare una copia dei file più importanti e metterli da qualche parte al sicuro. È come fotocopiare delle foto preziose da tenere in cassaforte nell'eventualità della perdita degli originali.

Quando fai il backup del tuo computer, telefonino o tablet, copie dei tuoi file vengono salvate on-line o su un dispositivo diverso. Avere copie salvate dei tuoi file più importanti e di foto preziose ti rende più tranquillo.

In caso di imprevisti a danno del tuo dispositivo oppure se vieni attaccato da criminali informatici, potrai facilmente recuperare i file del backup.

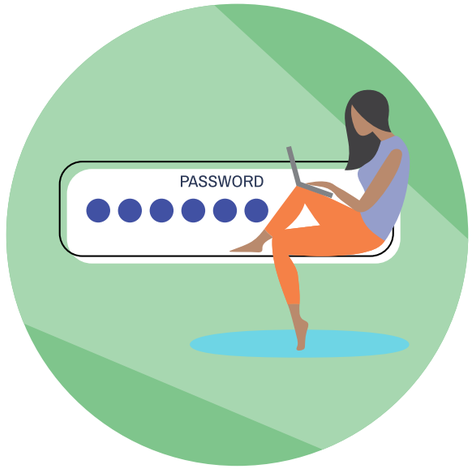
Per maggiori informazioni, cerca "Backups" su cyber.gov.au

LO SAPEVI:

Fare il backup del tuo dispositivo con una certa frequenza significa avere sempre accesso ai tuoi file più aggiornati.

Suggerimento n. 4: Usa una frase d'accesso

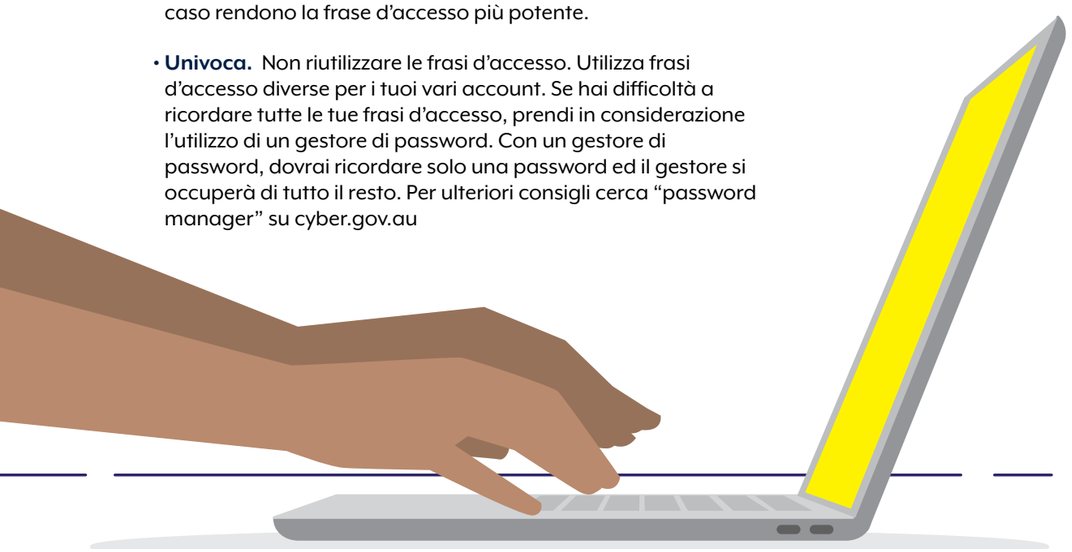
Se una password 'mette un lucchetto' sul tuo account, una frase d'accesso equivale a un completo impianto di vigilanza! Le frasi d'accesso sono versioni più potenti e più sicure di password.



Quando non puoi attivare la MFA, usa una frase d'accesso per proteggere il tuo account. Le frasi d'accesso usano quattro o più parole a caso come password. Ciò le rende difficili da indovinare per i criminali informatici ma facili per te da ricordare.

Quando crei una frase d'accesso, devi farla:

- **Lunga.** Più lunga è, meglio è. Cerca di crearla con una lunghezza di almeno 14 caratteri. Quattro o più parole a caso da ricordare sarebbero ideali. Ad esempio, 'viola oca patata barca'.
- **Imprevedibile.** Meno prevedibile è la frase d'accesso, meglio è. Frasi possono formare delle ottime frase d'accesso ma sono facili da indovinare. Un insieme di quattro o più parole scelte a caso rendono la frase d'accesso più potente.
- **Univoca.** Non riutilizzare le frasi d'accesso. Utilizza frasi d'accesso diverse per i tuoi vari account. Se hai difficoltà a ricordare tutte le tue frasi d'accesso, prendi in considerazione l'utilizzo di un gestore di password. Con un gestore di password, dovrai ricordare solo una password ed il gestore si occuperà di tutto il resto. Per ulteriori consigli cerca "password manager" su cyber.gov.au



Per saperne di più sulla creazione di frasi d'accesso sicure, cerca "Passphrases" su cyber.gov.au

Suggerimento n. 5: Riconosci e denuncia raggiri

Più velocemente denunci un raggiro, più prontamente potremo intervenire.

Se ritieni che qualcuno stia cercando di usare internet per raggirarti, è meglio essere proattivo e cauto piuttosto che farti truffare.

Se sembra troppo bello per essere vero, probabilmente lo è. Anche se un messaggio potrebbe dirti che hai vinto un premio o che il tuo computer contiene un virus, tale messaggio non è indirizzato solo a te.

Potrebbe provenire da un truffatore che vuole sfruttare la tua buona fede.

Ricorda che i truffatori spesso si fingono una persona o un'organizzazione di cui ti fidi. Fai attenzione quando ricevi un messaggio che sembra provenire da una persona di cui ti fidi ma che utilizza un nuovo numero di telefono, un nuovo indirizzo e-mail o un nuovo profilo sui social media. Prima di rispondere, verifica che la persona o l'organizzazione che ti sta inviando il messaggio sia davvero chi dice di essere, contattandola attraverso un canale di cui puoi fidarti. Ad esempio, se ricevi un messaggio di testo che sembra essere di uno dei tuoi figli, ma proviene da un nuovo numero, non rispondere. Invia loro un messaggio sui social media per verificare che abbiano davvero cambiato numero di telefono.

LO SAPEVI:

I criminali informatici sono furbi e potrebbero usare un nome e recapito di posta elettronica comuni. Stai all'erta se:

- **ti viene chiesto di pagare urgentemente una bolletta**
- **ti viene chiesto di cambiare i tuoi dati o la tua password**
- **Ti viene chiesto di cliccare su un collegamento o di aprire un allegato.**

Conclusione

Ora che sei dotato delle conoscenze per usare internet in modo più sicuro, puoi navigare con maggiore fiducia e continuare a goderti il tempo trascorso on-line.

Ma devi ricordare che i criminali trovano sempre nuovi modi per attaccare gli utenti.

Non è una cattiva idea ripassare di tanto in tanto le tue conoscenze in merito alla sicurezza informatica e apprendere nuovi modi per rimanere protetto.

Altri suggerimenti utili

Vuoi saperne di più su come rimanere protetto on-line? Adotta i seguenti suggerimenti utili.

Rifletti su cosa metti in rete.

Rifletti attentamente sulle informazioni che condividi in rete e su chi le vedrà. Accetta solo richieste di amicizia provenienti da persone che conosci nella vita reale.

Ricevi allerte di nuove minacce.

Iscriviti al nostro servizio gratuito di allerta. Questo ti farà sapere quando scopriamo una nuova minaccia informatica.

Inoltre ti fornirà consigli su cosa fare se subisci un attacco.

Parla di sicurezza informatica con familiari e amici.

Ora che te ne intendi di più in materia di sicurezza informatica, condividi ciò che hai appreso con familiari e amici. Le tue conoscenze potrebbero aiutarli a gestire in futuro una situazione difficoltosa!

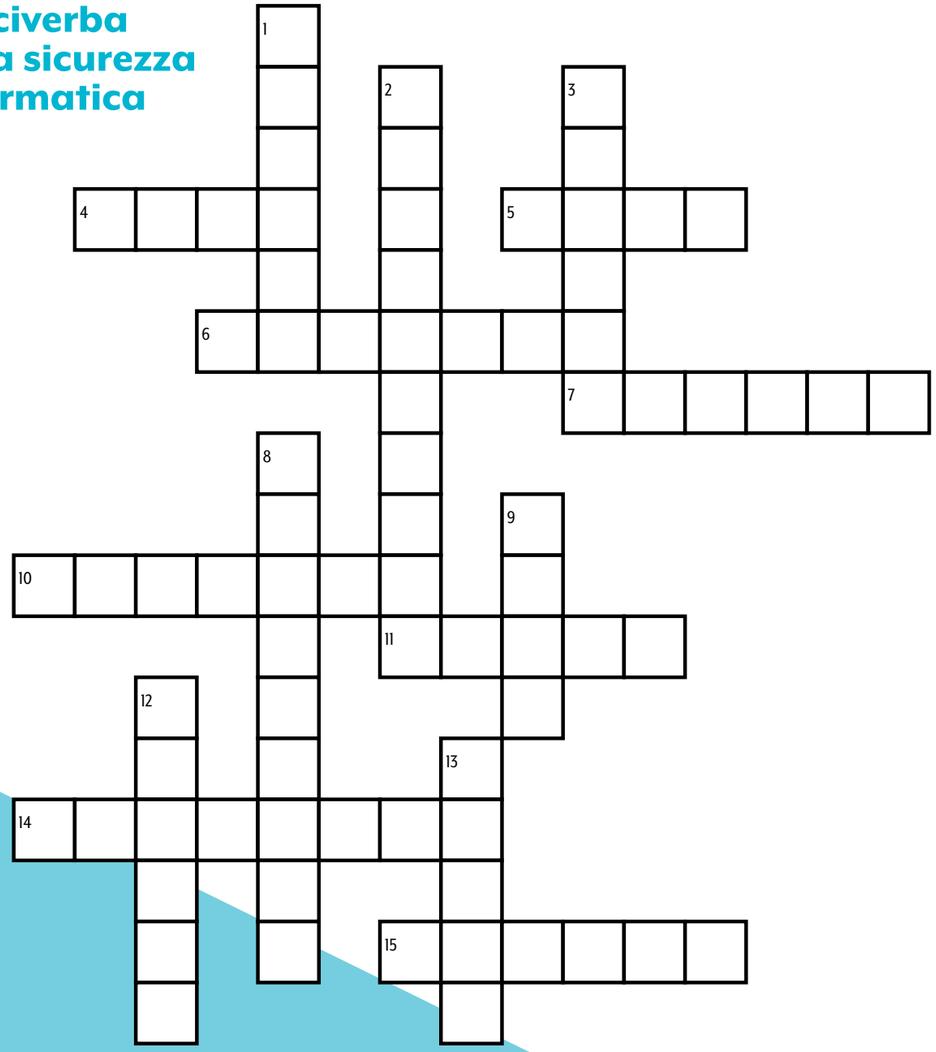
Evita di usare Wi-Fi pubblici quando svolgi operazioni bancarie o fai spese on-line.

I Wi-Fi pubblici sono convenienti per guardare video e leggere siti web ma riserva attività on-line che hanno per oggetto denaro alla tua connessione internet di casa. I Wi-Fi pubblici possono essere rischiosi.

Denuncia violazioni e crimini informatici per tenere l'Australia al sicuro.

Se ritieni di essere stato vittima di un reato informatico, agisci tempestivamente. Maggiori consigli si trovano sul sito cyber.gov.au

Cruciverba sulla sicurezza informatica



SENSO VERTICALE

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

SENSO ORIZZONTALE

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Guide supplementari

Per maggiori informazioni, consulta la nostra serie Personal Cyber Security: tre guide ideate per aiutare il pubblico australiano a comprendere i principi di base della sicurezza informatica e come agire per proteggersi dagli attacchi informatici più comuni.

Puoi consultare tutte e tre le guide sul sito **cyber.gov.au**

Soluzioni del cruciverba

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Note

Esclusione di responsabilità

Il materiale contenuto in questa guida è di natura generale e non deve essere considerato come una consulenza legale, né si deve fare affidamento su di esso per assistenza in qualsiasi circostanza particolare o situazione di emergenza. Per qualsiasi questione importante, è necessario richiedere un'adeguata consulenza professionale indipendente in relazione alla propria situazione.

Il Commonwealth non si assume alcuna responsabilità per eventuali danni, perdite o spese sostenute come conseguenza dell'aver fatto affidamento sulle informazioni contenute in questa guida.

Per maggiori informazioni o per denunciare un incidente in materia di sicurezza informatica, contattaci:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Questo numero è raggiungibile solamente da coloro che chiamano dall'Australia.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre