Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

SICUREZZA INFORMATICA PERSONALE

GUIDA BASE

cyber.gov.au

Serie sulla sicurezza informatica personale

Serie sulla sicurezza informatica personale

Sicurezza informatica personale: Guida Base è la prima di una serie di tre guide progettate per aiutare gli australiani a comprendere le basi della sicurezza informatica. Scoprite come potete agire per proteggervi dalle minacce informatiche più comuni.

Guida base

Guida intermedia

Guida avanzata

Indice dei contenuti

Introduzione

Cos'è la sicurezza informatica personale?

In un mondo sempre più guidato dalla tecnologia, utilizziamo ogni giorno dispositivi e account che sono vulnerabili alle minacce informatiche:

- I vostri dispositivi possono includere computer, telefoni cellulari, tablet e altri dispositivi connessi a Internet.
- Potreste anche utilizzare account online per e-mail, operazioni bancarie, acquisti, social media, giochi e altro ancora.

La sicurezza informatica personale è costituita da azioni continuative che potete intraprendere per proteggere i vostri account e i vostri dispositivi dalle minacce informatiche.

Cosa sono le minacce informatiche?

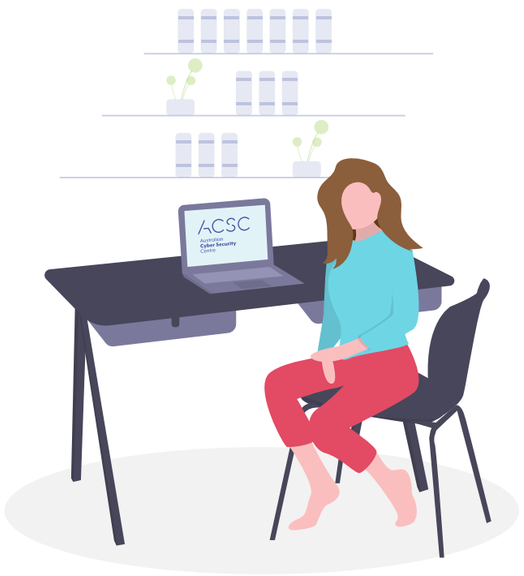
Le principali minacce informatiche che colpiscono gli australiani sono **le truffe e il malware**.

- **Malware è un termine generico utilizzato per descrivere software dannosi** progettati per causare danni. Il malware può includere virus, worm, spyware, trojan e ransomware. I criminali informatici utilizzano il malware per rubare informazioni e denaro e per controllare i vostri dispositivi e account.
- **Le truffe sono messaggi inviati dai criminali informatici** per indurvi a consegnare informazioni sensibili o ad attivare un malware sul vostro dispositivo.

Questi attacchi possono avere un impatto personale e finanziario significativo sulle vittime. Sono inoltre sempre più sofisticati e frequenti.

Come può questa guida aiutare a proteggermi dalle minacce informatiche?

Se state muovendo i primi passi nel mondo della sicurezza informatica o se vi state aggiornando su questo tema, questa guida è un ottimo punto di partenza. La guida Sicurezza informatica personale: Guida base è la prima di una serie di tre guide pensate per aiutarvi a comprendere le basi della sicurezza informatica.



Sicurezza Informatica Personale: Guida base

Attivazione degli aggiornamenti automatici

Cosa sono gli aggiornamenti?

Un aggiornamento è una versione migliorata di un software (programmi, app e sistemi operativi) installato sul vostro computer su un dispositivo mobile.

- **Gli aggiornamenti software aiutano a proteggere i vostri dispositivi** eliminando i "bug" del software (errori di codifica o vulnerabilità). I criminali informatici e i malware possono utilizzare questi "bug" per accedere al vostro dispositivo e rubare i vostri dati personali, i vostri account, le vostre informazioni finanziarie e la vostra identità.
- **I criminali informatici trovano sempre nuovi "bug" nei software** e li sfruttano a loro favore. L'aggiornamento del software sui vostri dispositivi vi aiuta a proteggervi dagli attacchi informatici.

Come si impostano gli aggiornamenti automatici?

Gli aggiornamenti automatici sono un'impostazione predefinita che installa nuovi aggiornamenti non appena sono disponibili.

- Attivate e controllate gli aggiornamenti automatici su tutti i vostri software e dispositivi.
- La modalità di attivazione degli aggiornamenti automatici può variare a seconda del software e del dispositivo.
- Se possibile, impostate un orario comodo per gli aggiornamenti automatici, ad esempio quando dormite o quando non state utilizzando abitualmente il dispositivo.

Il vostro dispositivo deve essere acceso, collegato alla rete elettrica e avere spazio di memoria inutilizzato.

Suggerimento: se vi viene richiesto di aggiornare il software del dispositivo, è necessario farlo il prima possibile.

Informazioni più dettagliate su come attivare gli aggiornamenti automatici possono essere trovate cercando " Updates " (Aggiornamenti) su cyber.gov.au

Cosa succede se l'impostazione di aggiornamento automatico non è disponibile?

Se l'impostazione di aggiornamento automatico non è disponibile, è necessario verificare regolarmente la presenza di nuovi aggiornamenti e installarli attraverso il software o il menu delle impostazioni del dispositivo.

Cosa succede se il mio dispositivo e il mio software sono troppo vecchi e non possono ricevere aggiornamenti?

Se il vostro dispositivo, sistema operativo o software sono troppo vecchi, potrebbero non essere più supportati dai produttori o dagli sviluppatori.

Quando i prodotti raggiungono questa fase di "fine supporto", non riceveranno più aggiornamenti. Questo può rendervi vulnerabili ad attacchi informatici. Esempi di prodotti che sono arrivati alla fase di "fine supporto" includono il sistema operativo Windows 7 e l'iPhone 7.

Se il vostro dispositivo, sistema operativo o software ha raggiunto la fase di "fine supporto" l'ACSC raccomanda di acquistare un nuovo dispositivo il prima possibile per rimanere al sicuro.

Per maggiori informazioni, cercate " End of support " (Fine supporto) su cyber.gov.au

Sicurezza Informatica Personale: Guida base

Attivazione dell'autenticazione a più fattori (MFA)

Che cos'è l'autenticazione a più fattori (MFA)?

È possibile utilizzare l'autenticazione a più fattori (Multi-Factor Authentication, MFA) per migliorare la sicurezza dei vostri account più importanti. L'MFA richiede una combinazione di due o più tipi di autenticazione prima di concedere l'accesso a un account.

- **Qualcosa che conoscete** (ad esempio, un PIN, una password o una frase d'accesso).
- **Qualcosa che avete** (ad esempio, una smartcard, un token fisico, un'app di autenticazione, un SMS o un'e-mail),
- **Qualcosa che siete** (ad esempio un'impronta digitale, un riconoscimento facciale o una scansione dell'iride).

L'MFA rende più difficile per i criminali informatici ottenere l'accesso iniziale al vostro account. Aggiunge più livelli di autenticazione, che richiedono tempo, sforzi e risorse supplementari per essere violati.

Come posso attivare l'MFA per proteggere i miei account più importanti?

I passaggi per attivare l'MFA sono diversi a seconda dell'account, del dispositivo o dell'applicazione. È consigliabile attivare subito l'MFA, iniziando dai vostri account più importanti:

- Tutti gli account bancari e finanziari online (ad esempio, la vostra banca, PayPal).
- Tutti gli account di posta elettronica (ad es. Gmail, Outlook, Hotmail, Yahoo!).

Se avete molti account di posta elettronica, date la priorità a quelli che sono collegati ai servizi bancari online o ad altri servizi importanti.

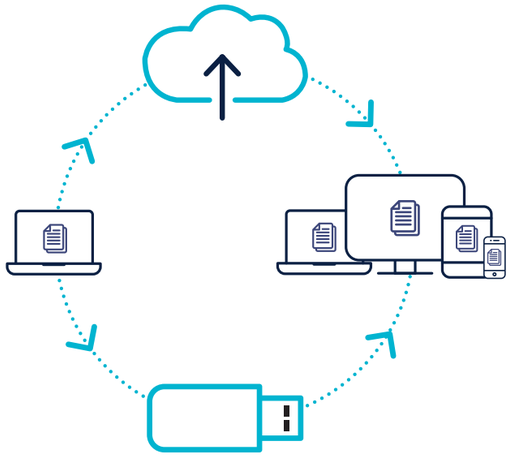
Potete ottenere maggiori informazioni su come attivare l'autenticazione a più fattori cercando "Multi-factor authentication" (Autenticazione a più fattori) o "MFA" su cyber.gov.au

Regolare esecuzione del backup dei dispositivi

Che cos'è un backup?

Un backup è una copia digitale delle vostre informazioni. Può trattarsi di foto, informazioni finanziarie o documenti salvati su un dispositivo di archiviazione esterno o sulla cloud.

Il backup è una misura precauzionale per poter recuperare le vostre informazioni o dati in caso di perdita, furto o danneggiamento.



Come si esegue il backup dei dispositivi e dei file?

L'esecuzione regolare del backup dei vostri dispositivi e dei file è un'azione altamente raccomandata. La modalità di esecuzione, sia essa giornaliera, settimanale o mensile, dipende in ultima analisi da voi. Il numero di volte che si esegue il backup può dipendere dal numero di:

- nuovi file caricati sul dispositivo,
- modifiche apportate ai file.

Suggerimento: Controllate regolarmente i backup in modo da avere familiarità con il processo di ripristino. Assicuratevi sempre che i backup funzionino correttamente.

Informazioni più dettagliate su come eseguire il backup dei propri dati sono disponibili cercando "Backup" su cyber.gov.au

Utilizzo di frasi d'accesso per proteggere i vostri account importanti

L'autenticazione a più fattori (MFA) è uno dei modi più efficaci per proteggere i vostri account dai criminali informatici. **Se l'MFA non è disponibile**, una frase d'accesso unica e complessa può proteggere meglio il vostro account rispetto a una semplice password.

Che cos'è una frase d'accesso?

Una frase d'accesso utilizza quattro o più parole casuali come password.

Ad esempio: "cristallo cipolla argilla pretzel".

- **Le frasi d'accesso sono più sicure** delle semplici password.
- Le frasi d'accesso sono difficili da decifrare per i criminali informatici, ma facili per voi da ricordare.

Come posso creare una frase d'accesso?

Create delle frasi d'accesso che siano:

- **Lunghe:** almeno 14 caratteri, utilizzando quattro o più parole casuali. Più lunga è la frase d'accesso, più è sicura.
- **Imprevedibili:** utilizzate un mix casuale di quattro o più parole non correlate. Niente frasi famose, citazioni o testi.
- **Uniche:** non riutilizzate la stessa frase d'accesso per più account.

Se un sito web o un servizio richiede una password complessa che include simboli, lettere maiuscole o numeri, potete includerli nella vostra frase d'accesso. La frase d'accesso deve comunque essere lunga, imprevedibile e unica per garantire la massima sicurezza.

Quali account devo proteggere con una frase d'accesso?

Se i vostri account più importanti non sono protetti con l'MFA, cambiate le vostre password con frasi d'accesso uniche e complicate, a partire da:

- Servizi bancari e account finanziari online
- Account di posta elettronica

Se avete molti account di posta elettronica, date la priorità a quelli collegati ai servizi bancari online o ad altri servizi importanti.

In genere è possibile modificare la password con una frase d'accesso unica e complessa attraverso il menu delle impostazioni dell'account.

Suggerimento: Se fate fatica a ricordare tutte le vostre frasi d'accesso, prendete in considerazione l'utilizzo di un gestore di password. Con un gestore di password, è sufficiente ricordare una sola password e il gestore di password si occupa di tutto il resto. Per maggior informazioni cercate "password manager" (gestore di password) su cyber.gov.au.

Informazioni più dettagliate su come creare frasi d'accesso sicure possono essere trovate cercando "Passphrase" (Frase d'accesso) su cyber.gov.au

Protezione del vostro dispositivo mobile

Smartphone e tablet sono ormai utilizzati nella vita di tutti i giorni. Li usiamo per comunicare, fare acquisti, lavorare, effettuare operazioni bancarie, monitorare il nostro benessere e completare centinaia di attività in qualsiasi momento e da qualsiasi luogo.

Cosa può succedere se il mio dispositivo mobile viene compromesso, perso o rubato?

- Il dispositivo può essere utilizzato da criminali informatici per rubare il vostro denaro o la vostra identità. A tal fine, i criminali utilizzano le informazioni memorizzate sul vostro dispositivo, compresi gli account di social media e di posta elettronica.
- Potreste perdere dati insostituibili come foto, appunti o messaggi (nel caso non abbiate effettuato il backup).
- Un criminale informatico potrebbe utilizzare il vostro numero di telefono per truffare altre persone.

Come posso proteggere il mio dispositivo mobile?

Sicurezza del dispositivo:

- **Bloccate** il vostro dispositivo con una frase d'accesso, una password, un PIN o un codice di accesso. Rendetela difficile da indovinare: la data di nascita o un semplice pattern sono facili da dedurre per i criminali informatici. Per una sicurezza ottimale, utilizzate una frase d'accesso (consultate la pagina 6). Potreste anche prendere in considerazione l'utilizzo del riconoscimento facciale o di un'impronta digitale per sbloccare il dispositivo.
- **Assicuratevi** che il dispositivo sia impostato per bloccarsi **automaticamente dopo un breve periodo di inattività.**
- **Non** ricaricate il vostro dispositivo in una stazione di ricarica pubblica ed evitate di utilizzare caricabatterie di persone terze.
- **Trattate** il vostro telefono come il vostro portafoglio. Tenetelo al sicuro e portatelo sempre con voi.

Sicurezza del software e delle applicazioni:

- **Utilizzate** la funzione di aggiornamento automatico del dispositivo per installare gli aggiornamenti delle applicazioni e del sistema operativo non appena sono disponibili.
- **Impostate** il dispositivo in modo che richieda una frase d'accesso/password prima di installare le applicazioni. A questo scopo si possono utilizzare anche i controlli parentali.
- **Controllate** attentamente le autorizzazioni sulla privacy quando si installano nuove applicazioni sul dispositivo, in particolare quelle gratuite. Installa solo applicazioni di fornitori affidabili.

Sicurezza dei dati:

- **Attivate** le funzioni di blocco e cancellazione nel caso il vostro dispositivo le supporti.
- **Assicuratevi** di rimuovere accuratamente i dati personali dal dispositivo prima di venderlo o di disfarvene.

Sicurezza della connettività:

- **Disattivate** il Bluetooth e il Wi-Fi quando non li state utilizzando.
- **Assicuratevi** che il vostro dispositivo non si connetta automaticamente a nuove reti Wi-Fi.

Informazioni più dettagliate su come proteggere il vostro dispositivo mobile sono disponibili cercando "Secure your mobile phone" (Protezione dei dispositivi mobili) su cyber.gov.au

Sicurezza Informatica Personale: Guida base

Sviluppo della capacità di pensare in termini di sicurezza informatica

La sicurezza informatica personale non consiste solo nel modificare le impostazioni, ma anche nel cambiare i propri pensieri e comportamenti.

Fate attenzione alle truffe informatiche

I criminali informatici sono noti per utilizzare e-mail, messaggi, social media o telefonate per cercare di truffare gli australiani. I truffatori potrebbero fingere di essere una persona o un'organizzazione che pensate di conoscere o di cui pensate di potervi fidare.

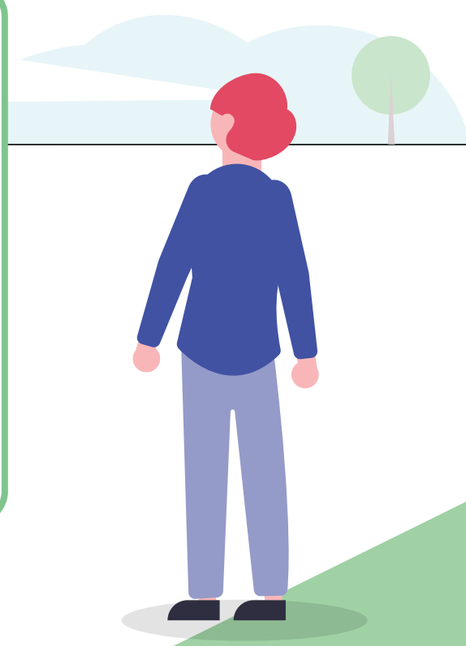
I loro messaggi e le loro chiamate tentano di ingannare l'utente per indurlo a compiere azioni specifiche, quali:

- Rivelare dettagli di conti bancari, password e numeri di carte di credito;
- Concedere l'accesso remoto al proprio computer;
- Aprire un allegato che potrebbe contenere malware;
- Inviare denaro o carte regalo.

Come posso riconoscere i messaggi di truffa?

Può essere difficile riconoscere i messaggi di truffa. I criminali informatici utilizzano spesso metodi per tentare di ingannarvi. I loro messaggi possono includere:

- **Autorità:** il messaggio sostiene di provenire da qualcuno di importante, come la vostra banca?
- **Urgenza:** vi viene detto che c'è un problema o che avete un tempo limitato per rispondere o pagare?
- **Emozione:** il messaggio suscita panico, speranza o curiosità?
- **Scarsità:** il messaggio offre qualcosa che scarseggia o promette un buon affare?
- **Attualità:** il messaggio riguarda una notizia di attualità o un grande evento?



Per sapere come riconoscere i messaggi di phishing o di truffa, visitate la sezione "Learn the basics" (Nozioni di base) su cyber.gov.au

Cosa devo fare se ricevo un messaggio di truffa?

Se ricevete un messaggio o una telefonata che cerca di truffarvi, ignoratela, cancellatela o segnalatela a Scamwatch dell'ACCC all'indirizzo scamwatch.gov.au

Se siete preoccupati per la vostra sicurezza informatica, potete anche contattare la linea diretta per la sicurezza informatica dell'ACSC al numero **1300 CYBER1** (1300 292 371).

Se avete subito una truffa e pensate che i vostri conti bancari, carte di credito o di debito possano essere a rischio, contattate immediatamente il vostro istituto finanziario. Potrebbero essere in grado di chiudere il conto o di bloccare una transazione.

Cosa devo fare se non sono sicuro che un messaggio sia una truffa?

Se pensate che un messaggio o una chiamata provengano davvero da un'organizzazione di cui vi fidate (come la vostra banca), trovate un metodo di contatto di cui vi potete fidare. Cercate il sito web dell'organizzazione, telefonate al suo numero di telefono pubblicizzato o visitate un negozio o una filiale. Non utilizzate i link o i dettagli di contatto contenuti nel messaggio che vi è stato inviato o che vi è stato dato al telefono, perché potrebbero essere fraudolenti.

Suggerimento:
Pensate prima di cliccare.

- **Pensate prima di cliccare sui link presenti nelle e-mail, nei siti web e negli SMS.**
- **Assumete sempre un atteggiamento scettico nei confronti degli allegati che ricevete.**
- **Se il vostro browser vi dice che un sito web non è sicuro, chiudetelo immediatamente.**

Ricordate: Nessun esperto informatico, dipartimento governativo o azienda vi contatterà per chiedervi di fornirgli i vostri dati di accesso.

Se pensate di essere vittime di un crimine informatico, denunciatelo attraverso il servizio ReportCyber dell'ACSC su cyber.gov.au/report o chiamate la nostra linea diretta per la sicurezza informatica al 1300 CYBER1 (1300 292 371).

Potete inoltre ricevere aggiornamenti sulle ultime minacce abbonandovi al servizio di allerta gratuito di ACSC. Cercate "Subscribe to the ACSC alert service" (Iscrizione al servizio di allerta ACSC) su cyber.gov.au Vi invieremo un avviso quando identificheremo una nuova minaccia informatica.

Sicurezza Informatica Personale: Guida base

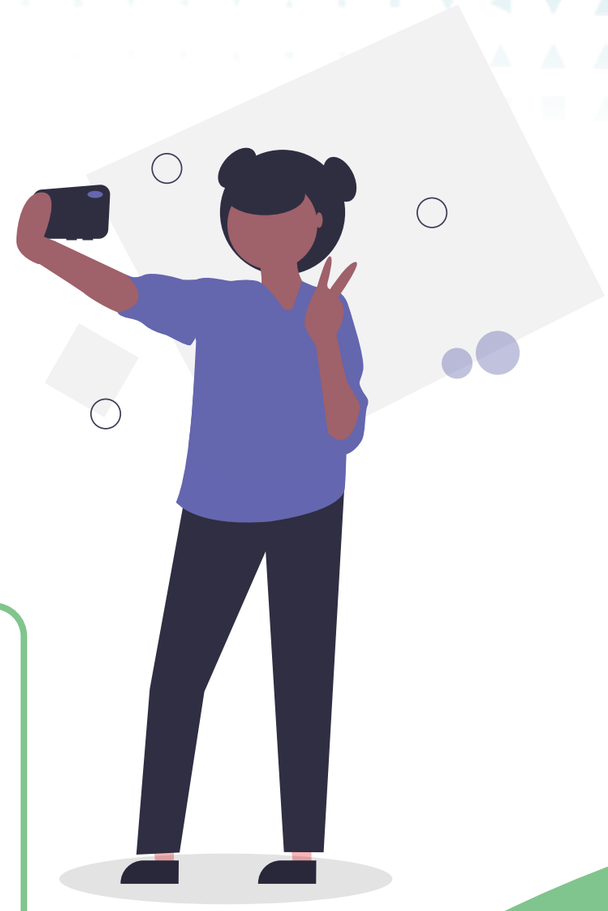
Fermatevi a pensare prima di condividere qualcosa sui social media

I criminali informatici possono utilizzare le informazioni che avete pubblicato pubblicamente sui vostri account di social media per le loro truffe e i loro attacchi informatici.

Ricordate che le informazioni su Internet sono permanenti e non è mai possibile rimuovere completamente ciò che è stato pubblicato.

In che modo posso fermarmi a pensare prima di postare?

- **Pensate:** come potrebbe un criminale informatico usare queste informazioni per prendere di mira me o i miei account?
- **Pensate:** mi sentirei a mio agio a mostrare queste informazioni o immagini a un perfetto sconosciuto?



Quali informazioni devo evitare di condividere?

Evitate di condividere online informazioni (comprese fotografie) che i criminali informatici possono utilizzare per identificarvi, manipolarvi attraverso una truffa o indovinare le domande di recupero dell'account. Queste informazioni possono includere:

- Luogo e data di nascita.
- Indirizzo e numero di telefono.
- Datore di lavoro e storia lavorativa.
- Dove avete frequentato la scuola.
- Qualsiasi altra informazione personale che possa essere utilizzata per individuare l'utente.

Lista di controllo riassuntiva

Avete completato tutte le azioni presentate in questa guida?

Utilizzate questa pratica lista di controllo per monitorare i vostri progressi:

- **Ho attivato gli aggiornamenti automatici per tutti i miei dispositivi:**
  - Computer (desktop e laptop).
  - Telefono cellulare.
  - Tablet.
- **Ho attivato l'autenticazione a più fattori per tutti i miei account più importanti:**
  - Tutti i miei servizi bancari e account finanziari online (ad esempio conto bancario, PayPal).
  - Tutti i miei account di posta elettronica (ad esempio Gmail, Outlook, Hotmail, Yahoo!).
- **Eseguo regolarmente il backup dei miei dispositivi:**
  - Computer (desktop e portatile).
  - Telefono cellulare.
  - Tablet.
- **Utilizzo frasi d'accesso uniche e complesse per i miei account più importanti che non sono protetti da MFA:**
  - Servizi bancari e account finanziari online.
  - Account di posta elettronica.
- **Ho messo al sicuro i miei dispositivi mobili:**
  - Computer portatile.
  - Telefono cellulare.
  - Tablet.
- **Utilizzo ogni giorno i principi di sicurezza informatica:**
  - So riconoscere i messaggi di truffa.
  - So cosa fare se ricevo un messaggio di truffa.
  - So come verificare se un messaggio è una truffa nel caso non ne sia sicuro.
  - Penso prima di cliccare su link e allegati.
  - Penso prima di condividere qualcosa sui social media.
- **So dove trovare aiuto se sono vittima di un crimine informatico o di una truffa.**

Glossario

Accesso remoto
Ottenimento dell'accesso e del controllo dei dispositivi e delle reti da una postazione esterna.

Allegato
Un file inviato con un messaggio di posta elettronica.

App
Chiamata anche applicazione mobile, app è un termine che indica un software comunemente utilizzato per uno smartphone o un tablet.

App di autenticazione
Un'app utilizzata per confermare l'identità di un utente di un computer per consentire l'accesso mediante l'autenticazione a più fattori (MFA).

Cloud
Una rete di server remoti che fornisce un'enorme potenza di archiviazione ed elaborazione.

Criminale informatico
Qualsiasi persona che accede illegalmente a un sistema informatico o a un account per arrecare danno o sottrarre informazioni.

Dispositivo
Un dispositivo informatico o di comunicazione. Ad esempio, un computer, un portatile, un telefono cellulare o un tablet.

Fine supporto
Il termine fine supporto si riferisce alla situazione in cui un'azienda cessa il supporto per un prodotto o un servizio. In genere si applica ai prodotti hardware e software quando un'azienda rilascia una nuova versione e termina il supporto per le versioni precedenti.

Malware
Software dannoso utilizzato per ottenere l'accesso e il controllo non autorizzato del computer di un utente, rubare informazioni e interrompere o disattivare le reti.

Recupero dell'account
Processo in cui si utilizzano una serie di domande o altri metodi di verifica per recuperare o riottenere l'accesso a un account o per modificare una frase d'accesso/password dell'account.

Sistema operativo
Software installato sul disco rigido di un computer che consente all'hardware di comunicare con i programmi del computer e di eseguirli. Esempi: Microsoft Windows, Apple macOS, iOS, Android.

Software
Comunemente chiamato programma, un software è una raccolta di istruzioni che consentono all'utente di interagire con un computer e il suo hardware o di eseguire determinate attività.

Token fisico
Un dispositivo fisico che di solito può essere inserito in un portachiavi e che genera un codice di sicurezza utilizzato per confermare l'identità di un utente di computer utilizzando l'MFA.

Esclusione di responsabilità
Il materiale contenuto in questa guida è di carattere generale e non deve essere considerato come una consulenza legale, inoltre non si deve fare affidamento su di esso per l'assistenza in particolari circostanze o situazioni 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 in seguito all'utilizzo delle informazioni contenute in questa guida.

Per maggiori informazioni o per segnalare un incidente di sicurezza informatica, contattateci:

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