DENUNCIA VIOLAZIONI E ATTACCHI INFORMATICI PER TENERE L'AUSTRALIA AL SICURO.

ISCRIVITI

Al nostro servizio gratuito di allerta
cyber.gov.au

DENUNCIA

Reati informatici a REPORTCYBER:
cyber.gov.au/report

CONTATTA

Chiama 1300 CYBER1 o
visita il sito cyber.gov.au

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

SEGUICI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. FAI ATTENZIONE A RAGGIRI

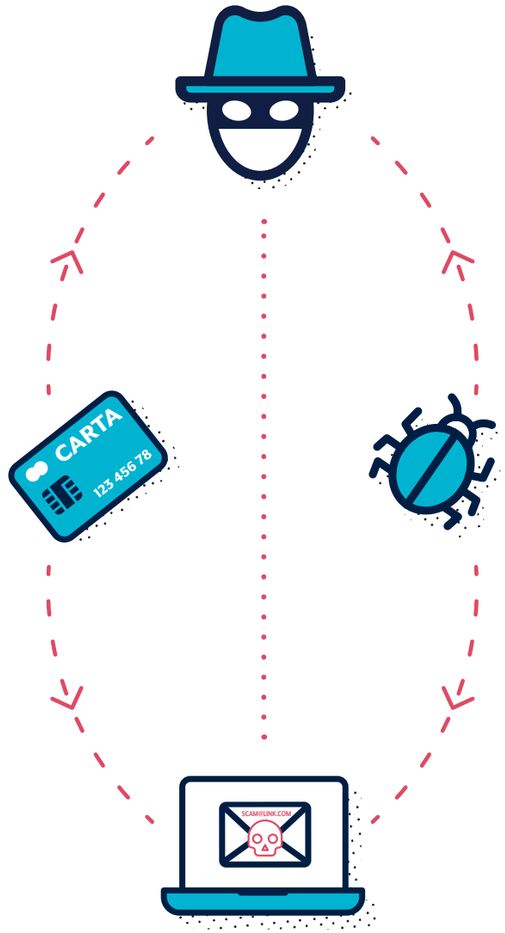
I criminali informatici usano posta elettronica, SMS, telefonate e social media per indurti, con l'inganno, ad aprire un allegato, visitare un sito web, rivelare i dati di login ad un conto, rivelare informazioni sensibili o trasferire soldi o carte regalo. I criminali fanno sembrare tali messaggi spediti da persone fisiche o giuridiche che credi di conoscere o di cui pensi di poterti fidare.

Per riconoscere messaggi truffaldini, fermati e rifletti:

- **Autorità:** Il messaggio sostiene di provenire da un soggetto ufficiale?
- **Urgenza:** Ti viene detto che hai tempo limitato per rispondere?
- **Emozione:** Il messaggio ingenera in te panico, paura, speranza o curiosità?
- **Scarsità:** Il messaggio offre qualcosa di cui vi è scarsità?
- **Attualità:** Il messaggio è legato a notizie di attualità, grandi eventi o periodi specifici dell'anno (come la dichiarazione dei redditi)?

Per controllare se un messaggio è legittimo:

- Consulta una fonte di cui ti fidi. Visita il sito ufficiale, accedi al tuo conto o chiama il numero di telefono ufficiale della banca. Non usare i collegamenti o recapiti contenuti nel messaggio che ti è stato inviato o comunicato al telefono.
- Controlla se la fonte ufficiale ti ha già comunicato ciò che non ti chiederà mai. Ad esempio, la banca potrebbe averti detto che non chiederà mai la tua password.



Per maggiori informazioni su come riconoscere messaggi truffaldini, consulta la pubblicazione 'Detecting Socially Engineered Messages' dell'Australian Cyber Security Centre (ACSC), e rimani informato iscrivendoti al servizio di allerta dell'ACSC sul sito **cyber.gov.au.**

SEMPLICI ACCORGIMENTI

PER PROTEGGERE I TUOI CONTI E DISPOSITIVI

RRIDUCI IL RISCHIO DI ATTACCHI DA PARTE DI CRIMINALI INFORMATICI ADOTTANDO I SEGUENTI ACCORGIMENTI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. AGGIORNA I TUOI DISPOSITIVI

I criminali informatici violano i dispositivi usando noti punti deboli in sistemi o applicazioni. Gli aggiornamenti contengono upgrade per rimediare a tali punti deboli. Attiva gli aggiornamenti automatici in modo che vengano installati senza il tuo intervento.

Attiva gli aggiornamenti automatici su tutti i tuoi dispositivi:

- Telefono cellulare
- Computer portatile
- Computer da scrivania

Controlla con una certa frequenza se ci sono aggiornamenti per le tue:

- Applicazioni
- Programmi
- Smart device

2. ATTIVA L'AUTENTICAZIONE MULTIFATTORE (MFA)

La MFA potenzia la tua sicurezza rendendo più difficile l'accesso da parte di criminali informatici ai tuoi file o conto.

Attiva l'MFA, partendo dai tuoi conti più importanti:

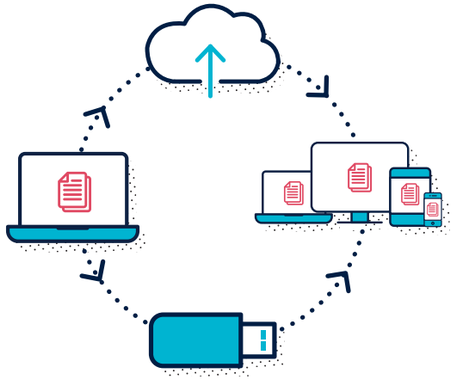
- Conti di posta elettronica
- Operazioni e conti bancari on-line con i dati dei pagamenti memorizzati
- Social media

3. FAI IL BACKUP DEI TUOI DISPOSITIVI

Il backup è una copia digitale delle informazioni memorizzate sul tuo dispositivo, ad esempio foto, documenti, video e dati tratti da applicazioni. Tali informazioni possono essere salvate su un dispositivo esterno di archiviazione o sul cloud. Facendo il backup puoi recuperare i tuoi file nell'eventualità che il tuo dispositivo sia smarrito, rubato o danneggiato.

Fai il backup dei tuoi dispositivi con una certa frequenza:

- Telefono cellulare
- Computer portatile
- Computer da scrivania
- Tablet



4. IMPOSTA PASSPHRASE SICURE

Nei casi in cui l'MFA non è disponibile, una passphrase sicura può spesso essere l'unica protezione da criminali dei tuoi conti e informazioni.

Una passphrase usa quattro o più parole a caso come password. Cambia le tue password a passphrase, accertandoti che siano:

- Lunghe: Più lunga la passphrase, meglio è. Creala con una lunghezza di almeno 14 caratteri
- Imprevedibili: Usa un insieme a caso di parole non correlate tra loro
- Univoche: Non usare la stessa passphrase su conti diversi