Osservatorio Cyber

CRIF-Mister Credit

I semestre 2024

Together to the next level

Italia al 5° posto

per furto di e-mail e password online

1 MILIONE

gli alert cyber di CRIF

90,7%

utenti allertati per dati sul **dark web**

e

9,3%

utenti allertati per dati sull'**open web**

+10% utenti allertati

per attacco informatico ai danni dei loro dati personali

Questi dati dimostrano quanto sia sempre più diffuso il **fenomeno** e la difficoltà per gli utenti di difendersi da attacchi quali **phishing**, **smishing**, **vishing**, **spear phishing** e l'emergente ***exploit zero-click***.

I DATI PIÙ VULNERABILI SUL WEB

PASSWORD
le più utilizzate:
123456
123456789
12345678

Password ed email si confermano i dati più vulnerabili insieme alla **username**, seguiti da numero di telefono e da nome e cognome.

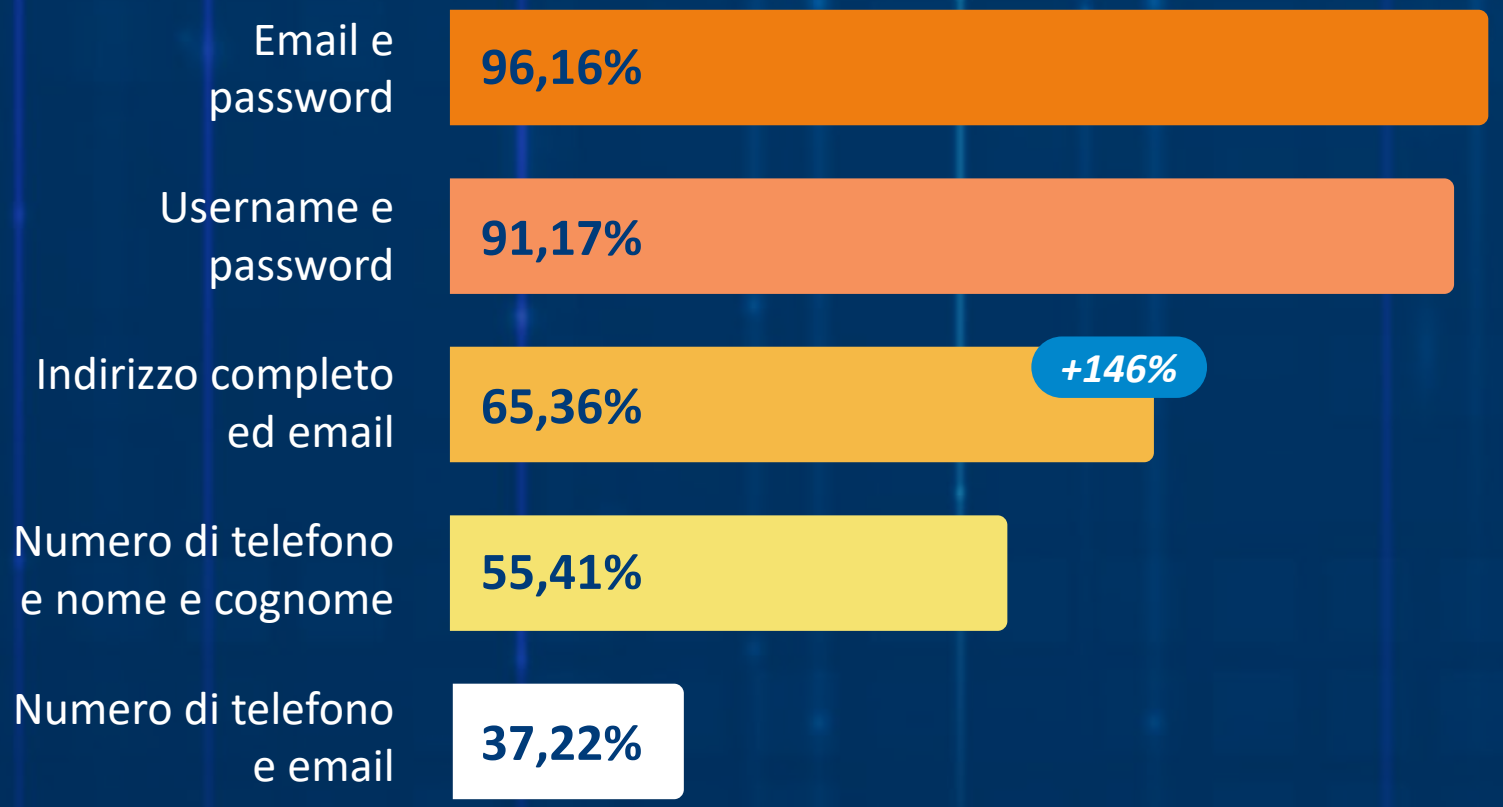
Email personali e aziendali

Numero di telefono

Email personali e aziendali

Username

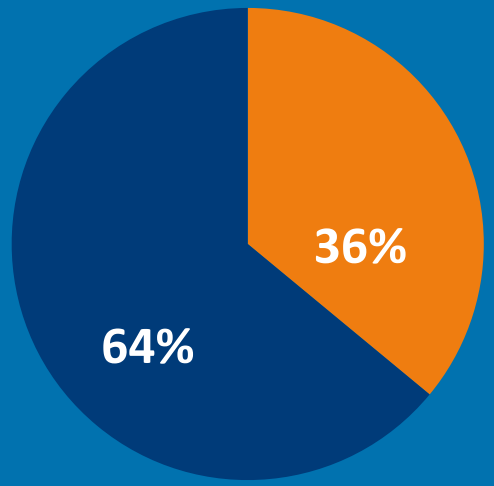
LE COMBINAZIONI DI DATI PIÙ ESPOSTE

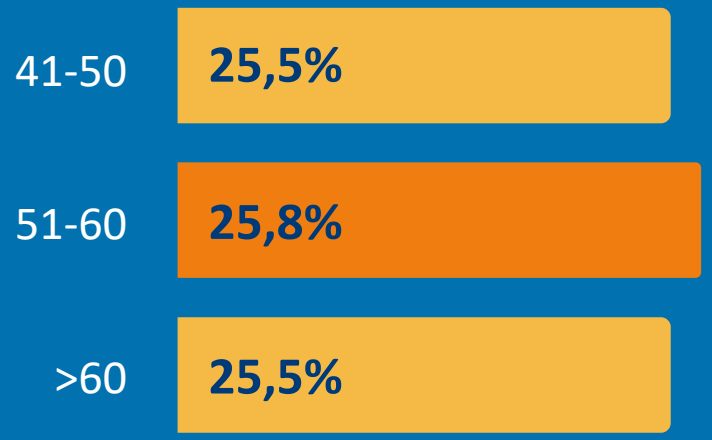


Preoccupa l'incremento registrato rispetto allo scorso semestre, +146%, relativo alla combinazione di **indirizzo completo più email**. Questo tipo di combinazione aumenta la vulnerabilità della vittima.

*Variazione I semestre 2024 vs II semestre 2023

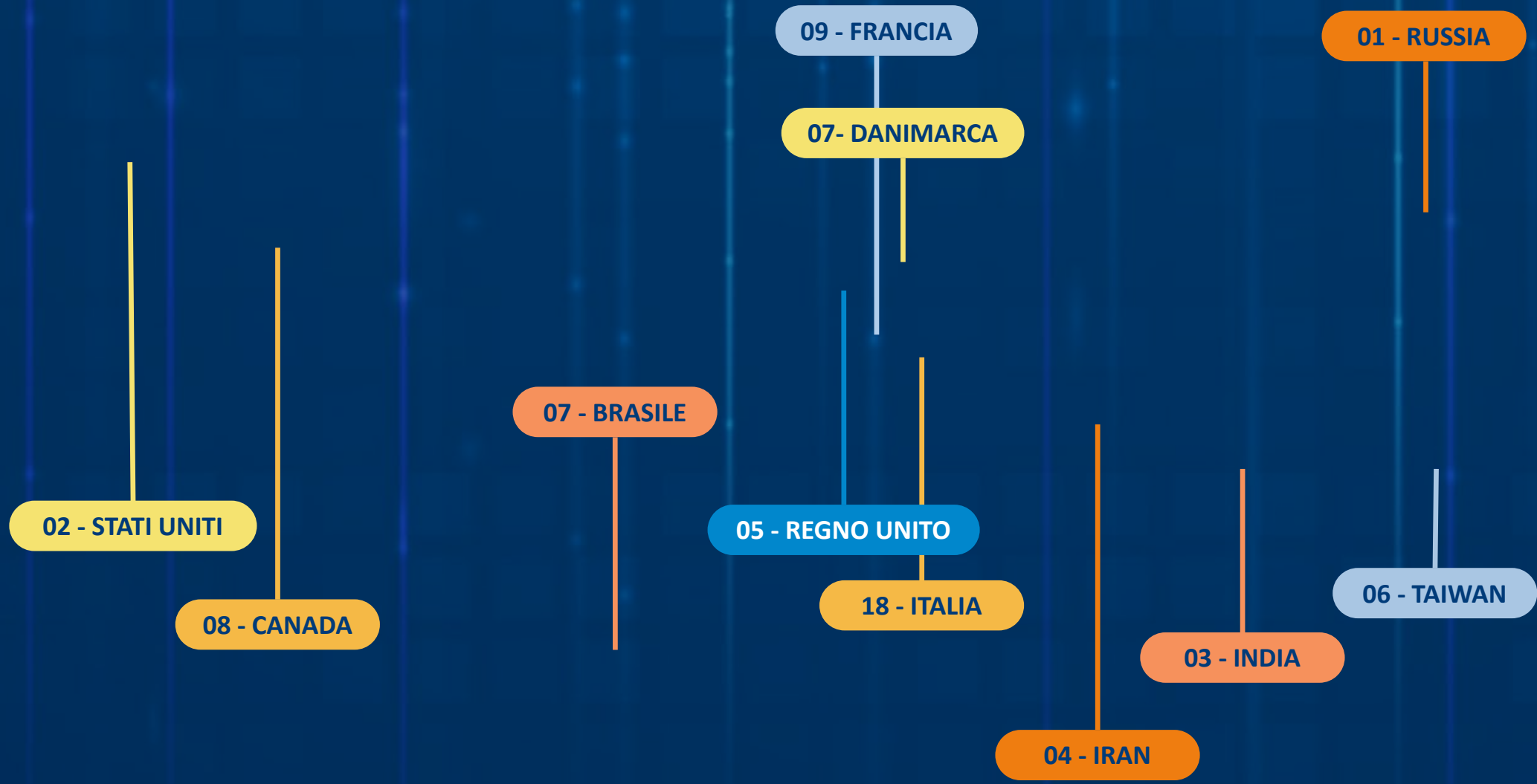
IL PROFILO DEGLI UTENTI PIÙ COLPITI



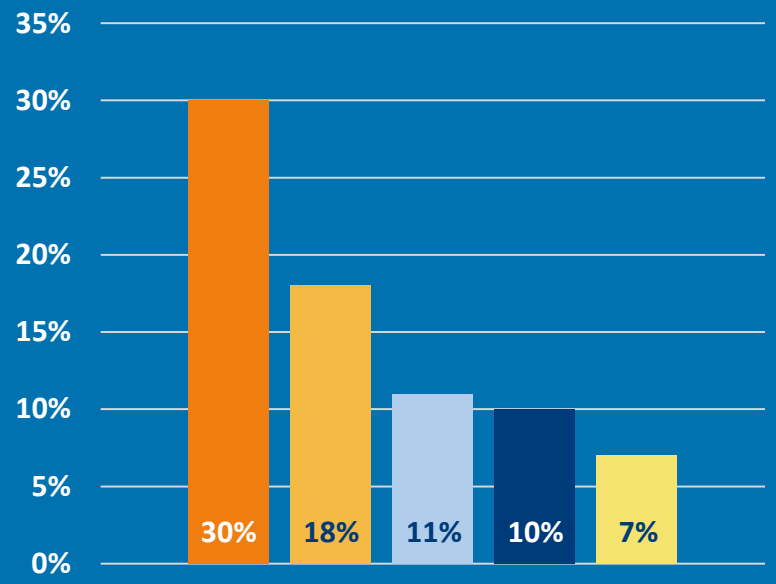


La fascia di età degli utenti maggiormente a rischio è quella dei **51-60**, seguita dai **41-50** a pari merito con gli **over 60**.

DOVE VENGONO RUBATI I DATI DELLE CARTE DI CREDITO



GLI ACCOUNT PIÙ RUBATI OLTRE ALLE EMAIL



- **Servizi di VPN**
- **Social network**
- **Siti internet**
- **Servizi finanziari**
- **E-commerce**

Escludendo i servizi di posta elettronica, la maggior parte degli account rubati sono relativi a **servizi di VPN, account di social network, siti internet e servizi finanziari.**
Il rischio di furto di tali account può portare a **conseguenze economiche dirette** per le vittime.

I dati che abbiamo raccolto nel primo semestre 2024 confermano un trend allarmante: attacchi sempre più sofisticati e personalizzati sul profilo delle vittime consentono di carpire dati personali e scambiarli attraverso il dark web allo scopo di ottenere un vantaggio economico a danno delle vittime stesse. Questo evidenzia l'importanza di mantenere alta l'attenzione ogni qualvolta veniamo invitati a fornire dati personali e di adottare strumenti di protezione in grado di intercettare la presenza dei dati sul dark web. In uno scenario così complesso, e di fronte a dei trend negativi ormai consolidati, l'educazione relativa alle opportunità e ai rischi dei servizi digitali è fondamentale per aiutare i cittadini a difendersi. Da diversi anni portiamo avanti progetti per sensibilizzare e coinvolgere le persone su tematiche legate ai rischi cyber. In questo ambito abbiamo di recente realizzato il cortometraggio "Il Furto", che racconta due storie sulle potenziali conseguenze del furto d'identità, mostrando come questo crimine possa avere un impatto significativo sulla vita delle persone.

– *Beatrice Rubini* - ***Executive Director di CRIF***

L’Osservatorio Cyber analizza la vulnerabilità agli attacchi cyber di persone e aziende, interpreta i trend principali che riguardano i dati scambiati sul web e offre spunti per fronteggiare i rischi cyber.

UNO STUDIO CHE VA IN PROFONDITÀ, ESPLORANDO GLI AMBIENTI DEL WEB SIA OPEN CHE DARK.

OPEN WEB

In chiaro, indicizzato dai motori di ricerca
Accessibile a tutti tramite i browser più diffusi

DARK WEB

Nascosto, non indicizzato dai motori di ricerca
Accessibile tramite software di navigazione criptata per garantire l’anonimato

LUOGO PRIVILEGIATO PER ATTIVITÀ DI HACKER E CRIMINALI INFORMATICI

CONSIGLI PER PROTEGGERSI DA FURTI D’IDENTITÀ E TRUFFE DIGITALI

Scegli password complesse
È importante usare password lunghe e diverse per ogni account, con combinazioni prive di legami con informazioni personali.

Installa un antivirus e aggiorna i software
Per migliorare costantemente la sicurezza dei dispositivi è fondamentale mantenerli aggiornati e protetti.

Fai il backup dei dati
Esegui regolarmente un backup completo per evitare la perdita dei dati. In aggiunta, fai una copia dei tuoi documenti, almeno di quelli più importanti o più utilizzati, in modo che siano sempre recuperabili via internet.

Proteggi i tuoi dispositivi
Pin, password, touch o face ID: i blocchi per l’accesso ai dispositivi, anche con controllo remoto, impediscono che vengano usati da altri senza consenso.

Fai attenzione a messaggi, email e telefonate sospette
Diffida di qualsiasi tentativo di contatto che richieda informazioni personali o finanziarie.

Affidati a servizi di Monitoraggio
Scegli soluzioni specifiche per il controllo della circolazione dei propri dati sul web, per avere una protezione più completa.