

OSSERVATORIO CYBER CRIF

PRIMO SEMESTRE 2020

Cybercrime: conoscere l'attacco per impostare la difesa



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

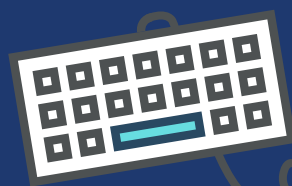
In chiaro, indicizzato dai motori di ricerca
Accessibile a tutti tramite i browser più diffusi



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



IL PERICOLO CORRE SULLA TASTIERA

GLI ALERT CYBER DI CRIF



+ 26,6% utenti allertati

per attacco informatico ai danni dei loro dati personali

Primo semestre 2020 vs secondo semestre 2019

Quali sono i dati più vulnerabili sul web?

EMAIL



PERSONALE 82%
BUSINESS 18%

PASSWORD



Le più utilizzate

01 **123456**
02 **123456789**
03 **QWERTY**

USERNAME



NUMERO DI TELEFONO



CARTE DI CREDITO



Quali sono le combinazioni di dati più intercettate?



EMAIL + PASSWORD

99,6%



NUMERO DI TELEFONO + PASSWORD

99,2%



CARTA DI CREDITO COMPLETA CON CVV E DATA DI SCADENZA

91,4%



USERNAME + PASSWORD

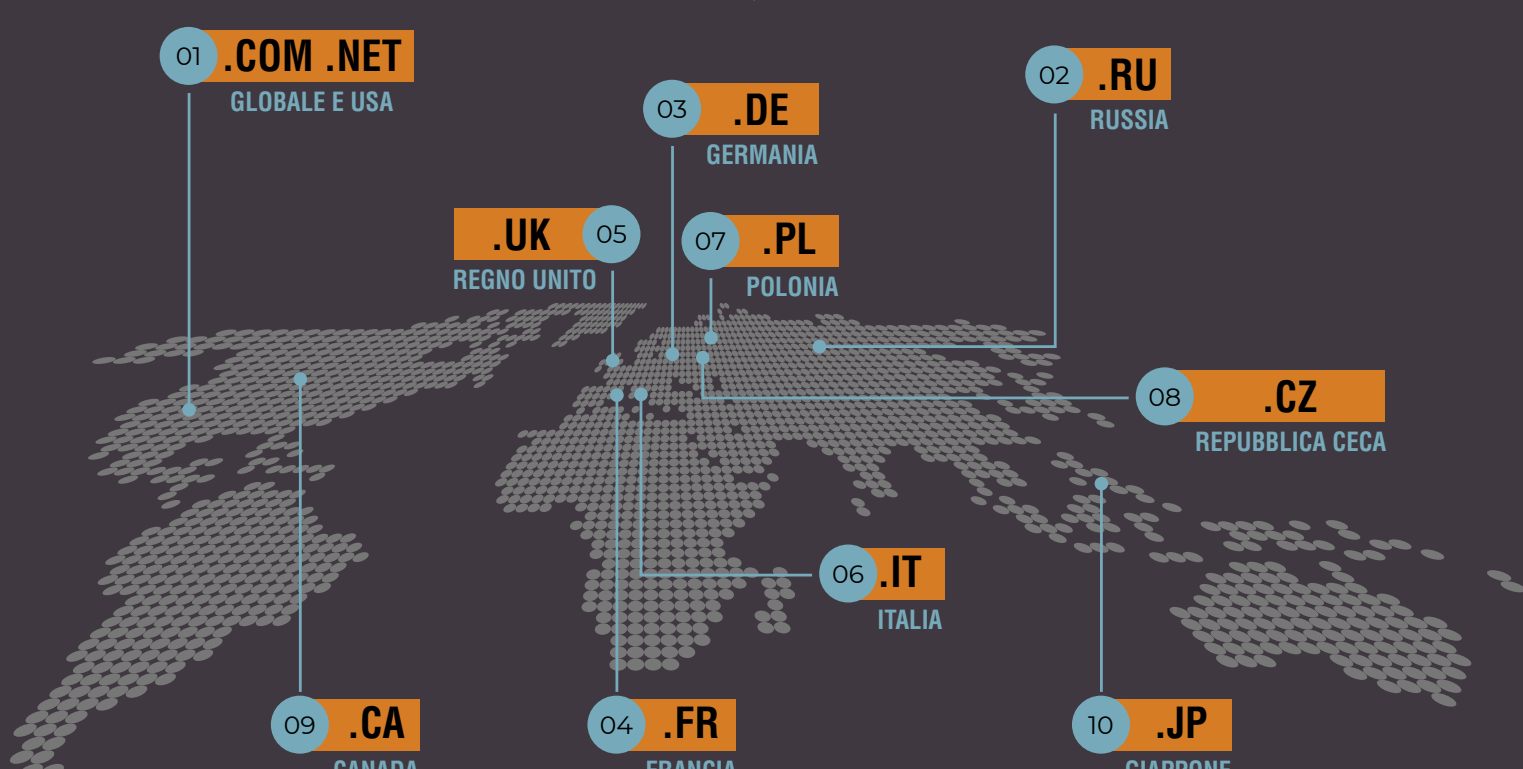
89,8%



CARTA DI CREDITO COMPLETA CON NOME E COGNOME

11,3%

Domini e Paesi più colpiti



Tipi di account più rubati

1,6%
SOCIAL MEDIA



73,2%
INTRATTENIMENTO
soprattutto giochi online e streaming

6,5%
E-COMMERCE

18,7%
SERVIZI FINANZIARI
in particolare banking, criptovalute o pagamenti



NAVIGARE AD OCCHI APERTI

Consigli per proteggersi da furti d'identità e truffe digitali



Aggiornare i software

L'update permette di migliorare costantemente la sicurezza di sistemi operativi e programmi, oltre che aggiungere funzionalità extra.



Installare un antivirus

I programmi specializzati che difendono i dispositivi dall'attacco di virus e altre minacce sono determinanti per mantenere al sicuro i propri dati.



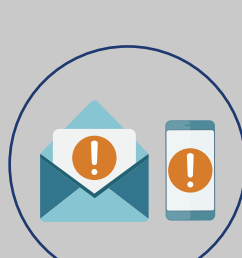
Fare il backup dei dati

Un regolare backup dei dati più importanti è fondamentale per poterli ripristinare in caso di necessità e non rischiare di perderli.



Proteggere i 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.



Attenzione a messaggi, email e telefonate sospette

Diffidare di qualsiasi tentativo di contatto che richieda informazioni personali o finanziarie è una regola da tenere sempre a mente.



Affidarsi a servizi di monitoraggio

Scegliere soluzioni specifiche per il controllo della circolazione dei propri dati sul web è la strategia ideale per avere una protezione più completa.

Per maggiori informazioni:
marketing@crif.com