Osservatorio Cyber

CRIF-Mister Credit

Analisi delle attività cyber nel 2025

Marzo 2026

CRIF
Together to the next level

Indice

Analisi delle attività cyber nel 2025

L'Osservatorio Cyber mira ad analizzare la vulnerabilità delle persone e delle aziende agli attacchi cyber e interpretare i trend principali che riguardano i dati scambiati in ambienti Open Web e Dark Web, la tipologia di informazioni, gli ambiti in cui si concentra il traffico di dati e i paesi maggiormente esposti, offrendo alcuni spunti per fronteggiare il rischio cyber.

I dati sono il frutto di una attività di analisi e studio svolta sugli ambienti web dove i dati vengono condivisi e scambiati. Si tratta non solo di siti web ma di gruppi, forum e comunità specializzate del cosiddetto "**Dark Web**".

Il Dark Web è **un insieme di ambienti web che non appaiono attraverso le normali attività di navigazione in Internet** e necessita di alcuni browser specifici, tecniche e ricerche mirate. Proprio per questa sua natura, viene sfruttato dagli hacker per scambiare dati, ottenuti attraverso attività di phishing o altre tipologie di attacchi.

Nel 2025 l'ecosistema delle minacce cyber ha subito una trasformazione profonda, guidata da nuovi equilibri geopolitici, da tecniche di attacco sempre più automatizzate e dall'arricchimento dei dati scambiati su dark web e public web.

Rispetto all'anno precedente, il numero di **segnalazioni inviate** in merito all'**esposizione dei dati sul dark web** è aumentato del **+5,8%, raggiungendo oltre 2.200.000 alert nel 2025.** Inoltre, c'è stato un **incremento nella quantità e nella pericolosità dei dati esposti**, con un impatto diretto sia sugli utenti privati sia sulle aziende.

1. Geopolitica e nuovi epicentri del rischio

Il ranking globale dei paesi più colpiti mostra l'emergere di nuovi attori: l'**Iran passa dalla posizione 124ª alla 3ª**, ridefinendo significativamente la distribuzione mondiale delle e-mail compromesse.

L'Italia mantiene un ruolo di rilievo (**6° posto per e-mail compromesse; 23° per dati di carte di credito**), ma in un contesto di crescita delle minacce che colpiscono i paesi più coinvolti nello scenario geopolitico attuale.

2. Aumento dell'esposizione e crescita della severity

Nel dark web sono state rilevate **combinazioni di dati sensibilmente più ricche e complete rispetto al 2024**, con un conseguente aumento della **gravità media degli alert (+22%)**. Questi dataset permettono frodi più mirate e automatizzabili: combinazioni come **carta di credito completa + nome e cognome (94%)** o **e-mail + password (91,5%)** sono ormai uno standard.

Sul fronte utenti, **1 persona su 2 ha ricevuto almeno un alert nel 2025**, e l'**85,6% degli alert riguarda dati rilevati sul dark web**, segno della crescente maturità dei mercati criminali.

3. Password: una vulnerabilità strutturale e non risolta

La classifica delle password più diffuse sul dark web continua a evidenziare combinazioni banali ("123456", "password"), **compromettibili in meno di un secondo**. La tecnologia ha introdotto soluzioni più sicure (password manager, autenticazione multifattoriale), ma la **frizione d'uso rimane elevata**.

Il 2025 conferma quindi un tema critico di **usabilità**: all'utente medio viene richiesto di ricordare decine di password, un compito insostenibile che ne favorisce il riutilizzo e la semplificazione, a discapito della sicurezza.

4. Evoluzione delle minacce: dall'AI all'omni-phishing

Il 2025 segna il consolidamento di attacchi potenziati dall'intelligenza artificiale:

- **deepfake audio e video**
- e-mail o messaggi perfettamente plausibili, generate da modelli linguistici
- campagne coordinate su più canali (**omni-phishing**), dove SMS, e-mail e messaggi social raccontano la stessa storia con coerenza assoluta.

Parallelamente, cresce il rischio di **account takeover**, favorito dalla combinazione di credenziali sottratte e **social engineering** iper-personalizzato.

5. Impatti sulle aziende e ampliamento del target business

Sebbene la maggioranza degli account esposti sia ancora di tipo personale, nel 2025 si registra una **crescita degli account business compromessi (dall'8,7% al 9,8%)**. Questo indica che le imprese, pur dotandosi di controlli sempre più avanzati, sono sempre più nel mirino di attori ostili.

Secondo l'Osservatorio cybersecurity & data protection del POLIMI school of management, il **contesto italiano** risulta caratterizzato da una pressione crescente: il **34%** delle organizzazioni ha gestito **incidenti con oneri significativi**, con conseguente revisione dei piani di **incident response** nel **57%** dei casi. Il **fattore umano** rappresenta il principale elemento di vulnerabilità (**96%**), seguito dalle **azioni malevole dei criminali** (**83%**) e dall'utilizzo dell'**AI da parte degli attaccanti** (**71%**).

6. Carte di credito: geografie del rischio

L'**Europa si conferma il continente più colpito** nello scambio illecito di dati di carte di credito (+32%), seguita da Asia e Nord America. A livello di paesi, **Russia, India e Stati Uniti** guidano la classifica, mentre l'Italia si posiziona al 23° posto, pur rimanendo in un'area di rischio significativa.

Da questa panoramica iniziale, emerge chiaramente un contesto che richiede monitoraggio costante, educazione digitale, strumenti di protezione evoluti e un forte intervento sul tema dell'usabilità della sicurezza.

Il fenomeno e i dati “più appetibili”

Il 2025 conferma che i cyberattacchi non solo sono in crescita, ma diventano sempre più difficili da individuare e contrastare. I criminali sfruttano una disponibilità di dati senza precedenti, resa possibile da esposizioni più ricche e da tecniche di compromissione sempre più sofisticate.

Attacchi sempre più credibili: smishing, phishing e AI-driven fraud

Le campagne di **smishing** sono aumentate in modo significativo, soprattutto attraverso SMS e app di messaggistica come WhatsApp. In Italia si sono registrati episodi particolarmente sofisticati, come falsi messaggi relativi a **pagamenti autostradali non saldati**, che reindirizzavano le vittime verso siti clonati del portale delle autostrade, oppure messaggi con falsi **problemi di consegna di pacchi,** apparentemente da parte dei principali corrieri, sempre col fine di **sottrarre dati personali e informazioni di pagamento**.

Accanto allo smishing, restano diffuse forme “note” di minaccia come **phishing**, **vishing** e **spear phishing**, ora potenziate dall’uso dell’**intelligenza artificiale**, diventata una nuova e pericolosissima **minaccia**: l’AI consente di generare **deepfake audio e video**, con voce e aspetto ormai indistinguibili da quelli di una persona reale.

A livello aziendale, l’AI permette di creare e-mail impeccabili, in stile professionale e senza errori, rendendo difficilissima la distinzione dai messaggi autentici.

È sempre più diffuso **l’approccio** definito “**omni-phishing**”, in cui si può ricevere contemporaneamente un’e-mail ben scritta, un SMS di verifica, un messaggio LinkedIn coerente con la stessa storia. Grazie all’AI è possibile orchestrare tutto, risultando credibili su ogni canale.

Stealers-as-a-service: la nuova industria del furto dati

La continua proliferazione e rapida diffusione degli **stealers-as-a-service** ha messo gli utenti in grave pericolo a causa della ricchezza di dati (e di informazioni contestuali) che il malware stealer può acquisire, creando pacchetti di dati completi e quindi estremamente preziosi per il mercato criminale.

Web pubblico vs dark web: quali dati vengono scambiati

Nel 2025, il numero di **alert inviati in relazione all'esposizione dei dati sul web pubblico** è stato di 55.000, in calo del -6,6% rispetto al 2024. Tra i dati più frequentemente rilevati sul web pubblico vi sono **numeri di identificazione personale, indirizzi e-mail e numeri di telefono**.

Questi dati si trovano spesso su elenchi e graduatorie ministeriali, tra cui conferimenti di onorificenze, o su albi di consulenti bancari e altre professioni, nonché elenchi e graduatorie di concorsi di ammissione per enti pubblici

Combinazioni di dati sempre più ricche e pericolose

Le analisi mostrano un **incremento del 22%** nella **gravità media degli alert** relativi alle combinazioni di dati che circolano sul dark web.

Tale aumento è dovuto in particolare all'individuazione di **combinazioni di dati più complesse e pericolose**, che associano in misura crescente **indirizzi e-mail a password** e riferimenti **precisi agli account compromessi**.

La posizione dell'Italia nel contesto internazionale

L'Italia rimane un bersaglio non trascurabile. Nel 2025, il nostro paese si è classificato:

- **6° posto mondiale** per indirizzi **e-mail** compromessi sul dark web
- **23° posto** per dati di **carte di credito** circolanti, una posizione comunque significativa (5° a livello europeo)
- **65° posto** per **numeri telefonici** rilevati (17° in Europa).

Glossario

Smishing: truffa informatica tramite SMS o app di messaggistica come WhatsApp.
Phishing: truffa informatica che mira a rubare informazioni personali tramite e-mail ingannevoli.
Deepfake: tecnica di intelligenza artificiale che crea video, immagini o audio falsi ma realistici.
Stealer-as-a-Service: malware per rubare informazioni, come credenziali e dati finanziari.

Osservatorio Cyber
CRIF-Mister Credit

Analisi delle attività cyber nel 2025

Italia al 6° posto
per furto di e-mail e password online

2,2 MILIONI
gli alert cyber di CRIF

+5,8%
rispetto al 2024

85,6%
utenti allertati per dati sul **dark web**

e

14,4%
utenti allertati per dati sull'**open web**

+4,6% 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'emergere di **attacchi guidati dall'intelligenza artificiale**.

TOP 5 DEI DATI PIÙ VULNERABILI SUL WEB

1. PASSWORD
le più utilizzate:
123456
123456789
12345678

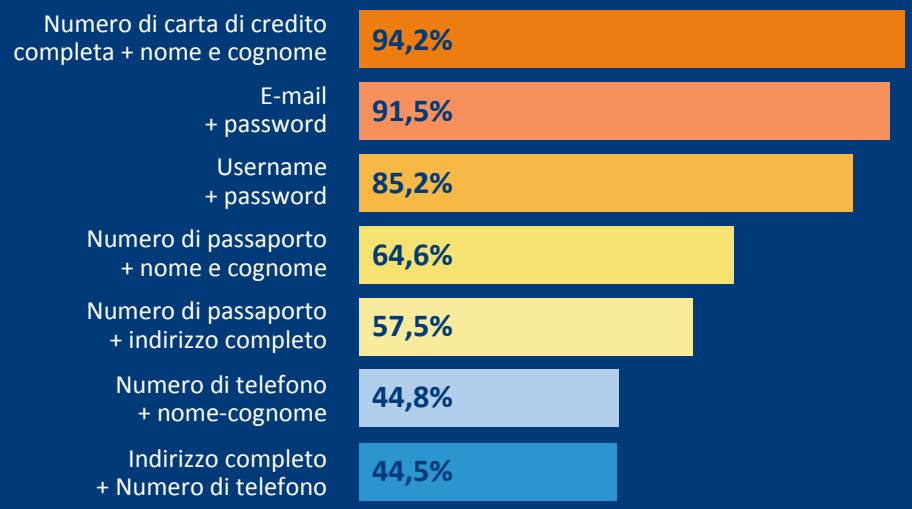
2. E-MAIL
Personali e aziendali
*Crescono gli account business compromessi (dall'**8,7%** al **9,8%**)*

3. Username

4. Indirizzo

5. Nome e cognome

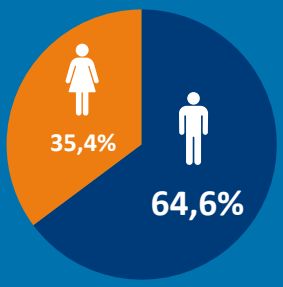
LE COMBINAZIONI DI DATI PIÙ ESPOSTE

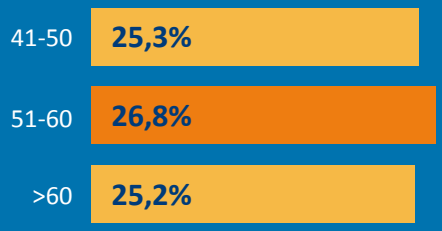


+22% gravità
media degli alert

relativi alle combinazioni di dati che circolano sul dark web.
Tale aumento è dovuto in particolare all'individuazione di combinazioni di dati più complesse e pericolose, che associano in misura crescente indirizzi e-mail a password e riferimenti precisi agli account compromessi.

IL PROFILO DEGLI UTENTI PIÙ COLPITI

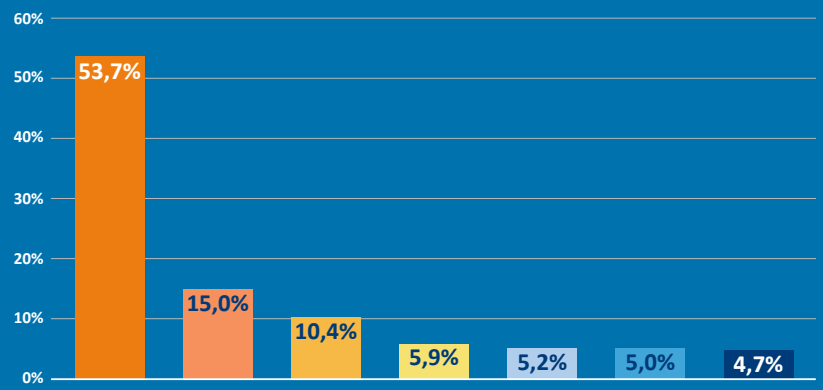




La fascia di età degli utenti maggiormente a rischio è quella dei **51-60 anni**, seguita dai **41-50 anni** e dagli **over 60**.

DOVE VENGONO RUBATI I DATI DELLE CARTE DI CREDITO

GLI ACCOUNT PIÙ RUBATI OLTRE ALLE E-MAIL



- Servizi online
- Social network
- Siti internet
- Gaming
- Enti pubblici / istituzioni
- Piattaforme e-commerce
- Servizi finanziari

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.

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

1. Il fenomeno cyber: analisi dei dati

1.1. Quali sono i dati più vulnerabili

Sono bersaglio di attacchi diverse categorie di dati, ma si osserva che **indirizzi e-mail, password, nomi utente, indirizzi di residenza, nomi e cognomi** sono i più diffusi sul dark web e quindi più vulnerabili. Anche i dati relativi ai **numeri di telefono**, ai **codici identificativi personali** e alle **carte di credito** sono comunemente **esposti** e a rischio di compromissione**.**

E-mail e numero di telefono possono essere utilizzati per inviare e-mail o sms di phishing altamente personalizzati e quindi credibili, che inducono la vittima a cliccare su link malevoli più facilmente.

Con l'uso dell'Intelligenza Artificiale, questi messaggi risultano ancora più convincenti: gli attaccanti possono generare notifiche perfettamente plausibili, aumentando drasticamente il rischio che la vittima cada nel tranello.

Più informazioni i truffatori hanno su un obiettivo, più l'attacco può essere personalizzato e convincente, aumentando le probabilità di successo.

Banche, aziende o enti non richiederanno mai dati personali o credenziali tramite SMS o messaggi di questo tipo. Davanti a comunicazioni sospette, la regola è semplice: **non cliccare, non rispondere e contattare direttamente l'istituto o l'azienda** attraverso i canali ufficiali.

TOP 10 dei dati più vulnerabili nel 2025

1. Password
2. E-mail
3. Username
4. Indirizzo
5. Nome e cognome
6. Numero di telefono
7. Data di nascita
8. Codici identificativi personali
9. Indirizzo IP
10. Carta di Credito

Fonti: Osservatorio Cyber CRIF

Le combinazioni di dati più esposte

L'analisi delle principali **combinazioni principali di dati ritrovati** nel 2025 rivela un quadro chiaro delle informazioni più vulnerabili agli attacchi informatici.

Dai dati emerge un incremento del 22% nella gravità media degli alert relativi alle combinazioni di dati che circolano sul dark web. Tale aumento è dovuto in particolare all'individuazione di combinazioni di dati più complesse e pericolose, che associano in misura crescente indirizzi e-mail a password e riferimenti precisi agli account compromessi.

Altre tipologie di dati hanno contribuito ad aumentare il livello medio di allerta, come la diffusione di **carte di credito complete di dettagli** e **riferimenti ai titolari** nonché la presenza di **pacchetti di informazioni** in formato "**Fullz**" (**Full Identity Profile**). Questi ultimi rappresentano **profili identitari completi** poiché includono nome, data di nascita, codice fiscale e indirizzo. Tali pacchetti di dati possono essere sfruttati dai criminali informatici per impersonificare totalmente le persone, ad esempio per fare acquisti e-commerce, aprire conti correnti o richiedere prestiti fraudolenti, con un **impatto crescente sulla sicurezza delle vittime** spesso ignare.

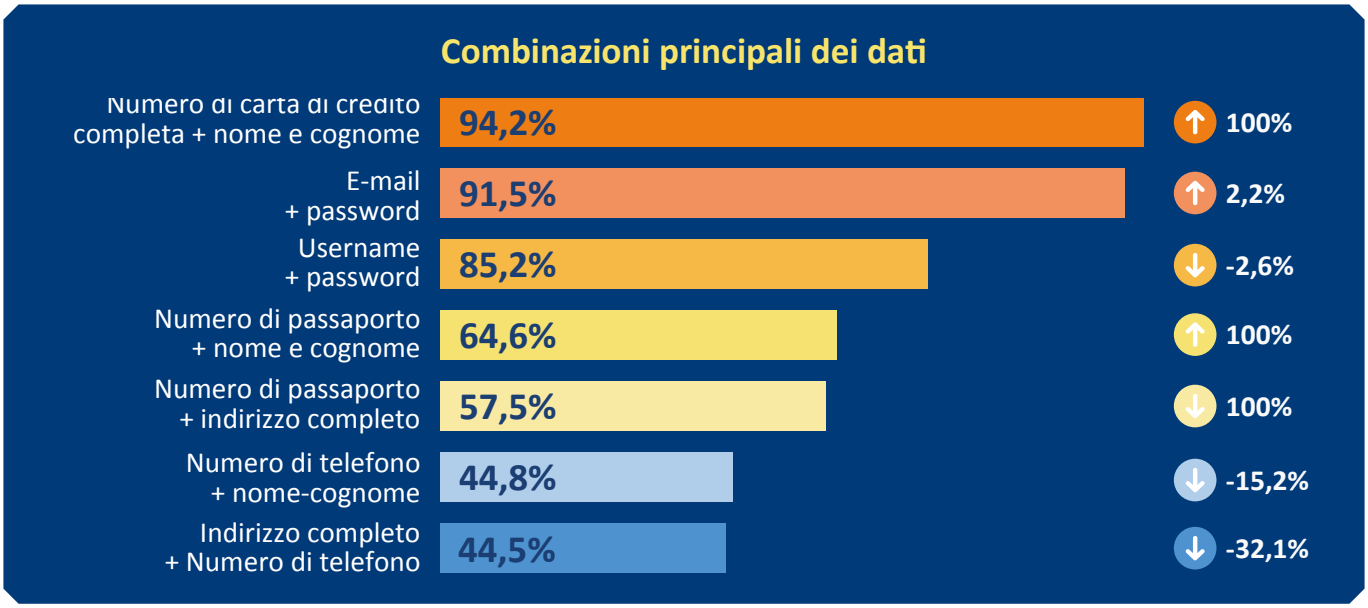
È particolarmente preoccupante la combinazione di numeri di carta di credito completa con nome e cognome, trovati insieme nel 94,2% dei casi, a causa del grave rischio di frode finanziaria.

Nel 2025 la presenza dei riferimenti al titolare della carta rende questa combinazione più forte e preziosa rispetto al 2024. La combinazione di **e-mail e password** rimane estremamente comune, con la password che appare accanto alla e-mail nel 91,5% dei casi, e nell'85,2% dei casi, è anche associata alla username. La combinazione di **username e password** è principalmente legata agli account aziendali, mettendo in evidenza le potenziali vulnerabilità delle aziende.

Questi dati confermano che il **furto di account** rimane un obiettivo primario per gli hacker, sottolineando la necessità di adottare pratiche corrette di gestione delle password (ad esempio, utilizzando una password diversa per ogni account, cambiando frequentemente le password, impiegando un gestore di password, ecc.).

Un'altra preziosa informazione per i criminali informatici è **l'indirizzo** residenziale completo, associato al **numero di telefono** nel 44,5% dei casi. L'elevata percentuale di **numeri telefonici** con nomi e cognomi (44,8%) è preoccupante perché fornisce agli attaccanti informazioni sufficienti per creare messaggi di smishing altamente personalizzati e convincenti.

Nel 2025 la combinazione **numero di passaporto con nome e cognome** presenta un'incidenza **molto elevata (64,6%)**, indicando che nella maggior parte dei casi il numero di passaporto circola insieme ad altri dati personali dell'individuo. Questo incremento di esposizione amplifica notevolmente il rischio di **furto d'identità**, poiché nome e cognome abbinati al documento costituiscono un set di dati utile per impersonificazioni. D'altro canto, la combinazione **numero di passaporto con indirizzo completo** mostra un'incidenza inferiore **(57,5%)**, pur rimanendo molto significativa. Il legame tra documento e indirizzo fisico abilita scenari di profiling avanzato e **social engineering** mirato.



Fonte: Osservatorio Cyber CRIF

1.2. Finalità di utilizzo degli account più rilevati

Attraverso una analisi qualitativa dei contesti in cui i dati circolano, si è cercato di comprendere le tipologie di servizi a cui corrispondono le username ritrovate sul dark web.

Escludendo i servizi di posta elettronica, al primo posto tra le categorie più colpite figurano i **servizi online** in generale, seguiti dagli **account dei principali social network**. Al quarto e quinto posto emerge invece il furto di credenziali legate ai **siti di e-commerce** e agli **enti pubblici e alle istituzioni**. In crescita gli account di **gaming** e i **servizi finanziari** (come piattaforme di pagamento)**.**

Le credenziali rubate possono essere utilizzate per diversi scopi, ad esempio per entrare negli account delle vittime, utilizzare servizi in modo fraudolento, inviare messaggi con richieste di denaro o link di phishing, diffondere malware o ransomware per estorcere o rubare denaro.

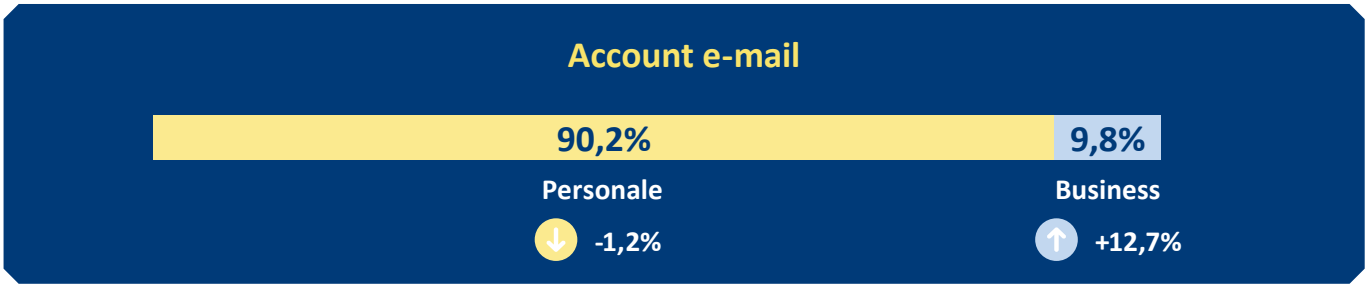
In questo scenario, il "**fattore umano**" continua a giocare un ruolo cruciale in questa tipologia di furto di dati: la disattenzione degli utenti e l'uso di password deboli o riutilizzate sono infatti tra le cause più comuni.

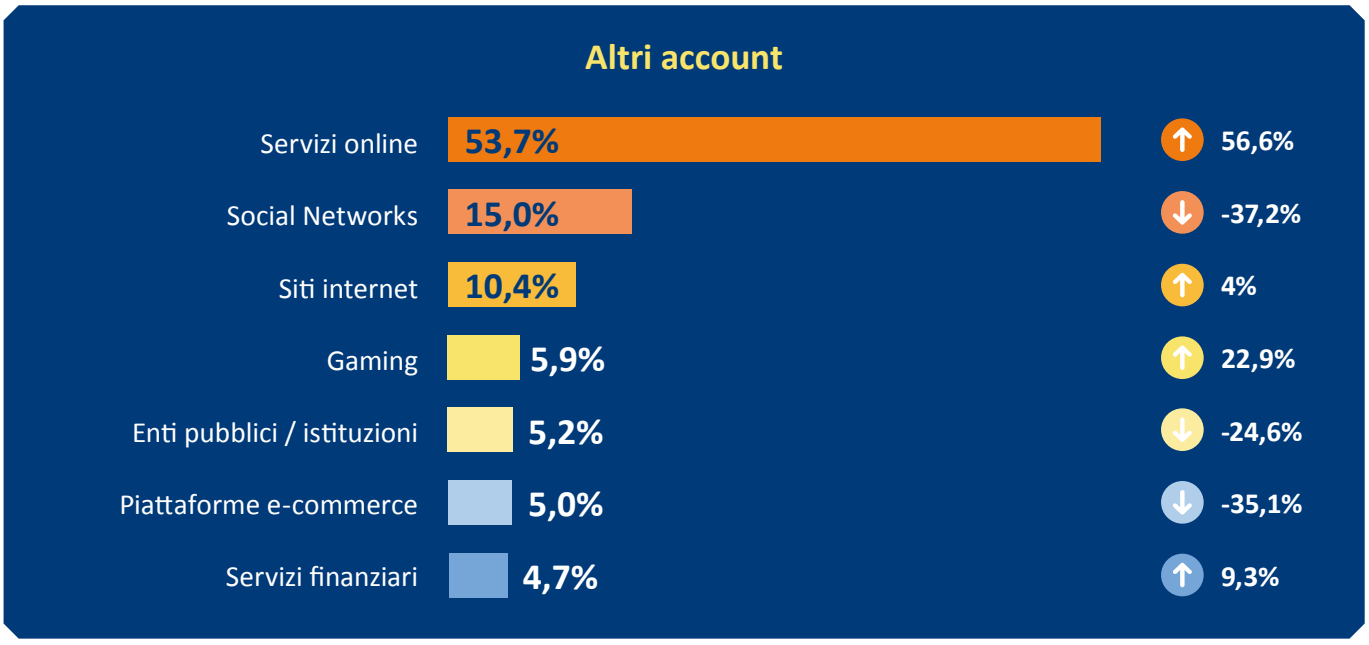
A questa dinamica, si aggiunge la crescente diffusione degli **attacchi di Account Takeover (ATO)**, che colpiscono non solo gli account più tradizionali, ma anche servizi di messaggistica come **WhatsApp**. L'Account Takeover si presenta spesso come un avviso di accesso sospetto a un servizio, ad esempio l'online banking, da un dispositivo sconosciuto. L'utente viene spinto a cliccare su un link per 'mettere in sicurezza' l'account, ma la pagina di destinazione è progettata per sottrarre credenziali e dati personali utilizzabili per frodi mirate.

Un altro aspetto rilevante e che accomuna alcuni tipi di account (come i social network, le piattaforme di streaming e di gioco) è la tendenza degli utenti a fornire le proprie credenziali a servizi apparentemente innocenti che offrono omaggi come elementi di gioco, classifiche di musica in streaming e così via – ma che spesso si rivelano strumenti per raccogliere credenziali.

L'analisi qualitativa dei domini associati agli account e-mail esposti sul dark web mostra una netta prevalenza di indirizzi personali, che rappresentano il 90,2% del totale. Tuttavia, gli account business, pur costituendo al momento il 9,8%, mostrano una crescita nel tempo.

Questa dinamica suggerisce da un lato che gli utenti privati continuano a prestare una protezione insufficiente ai propri dati digitali, rimanendo così il bersaglio preferito dei criminali informatici; dall'altro lato, indica che le aziende, pur investendo sempre di più in misure di sicurezza, non sono immuni. È essenziale non abbassare la guardia rispetto alle minacce informatiche al fine di proteggere i propri account.





Fonti: Osservatorio Cyber CRIF

1.3. Classifica delle password più trovate sul dark web

L'analisi delle password rilevate fa riflettere sulla vulnerabilità degli account a cui le stesse sono associate.

L'analisi delle password più diffuse sul dark web nel 2025 mostra un persistente utilizzo di **combinazioni di caratteri estremamente semplici** e prevedibili da parte degli utenti, rendendo gli account più vulnerabili agli attacchi informatici. Nella top 10 troviamo password come "123456", "Password" e " qwerty ", **che possono essere hackerate in meno di un secondo**.

Questa scelta, spesso dettata dalla comodità di ricordare una password breve e facile, espone gli utenti a un rischio elevato di accesso non autorizzato ai propri dati personali e di furto d'identità. Molti utenti sottovalutano **l'importanza di una password forte e unica per ogni account**, per cui è consigliabile utilizzare strumenti come i password manager.

Il fenomeno non riguarda un solo Paese. In Italia, ad esempio, tra le password più comuni rintracciate nel dark web ci sono semplici sequenze numeriche come "123456" o "123456789", nomi propri come "Francesco", "Alessandro", "Giuseppe" e altri, riferimenti calcistici quali "Juventus" e "Napoli", oltre a termini banali come "ciaociao", "cambiami" e "amoremio". Tutti esempi che confermano una scarsa attenzione globale alla sicurezza delle credenziali.

Diventa essenziale far capire agli utenti che **una password poco sicura costituisce un facile accesso per i cybercriminali**. Per tutelare i dati personali è indispensabile adottare pratiche responsabili: creare credenziali complesse e diverse per ogni profilo, servirsi di un gestore di password, abilitare l'autenticazione a due fattori ove possibile e attivare il monitoraggio dei propri dati, così da poter reagire prontamente e ridurre eventuali rischi economici e danni alla reputazione.

Top 10 Password
in circolazione sul dark web nel 2025

1	123456
2	123456789
3	12345678
4	password
5	12345
6	qwerty
7	1234567890
8	qwerty123
9	Password
10	1234567

Fonte: Osservatorio Cyber CRIF

Ma esiste un problema strutturale spesso sottovalutato: **le password davvero sicure — lunghe, complesse, uniche per ogni servizio — sono difficili, se non impossibili da ricordare per una persona**. Non sorprende quindi che molti continuino a scegliere password semplici o a riutilizzarle su più piattaforme: non è solo superficialità, ma una scorciatoia dettata dalla necessità. Se le soluzioni non sono usabili, le persone ricorreranno inevitabilmente a metodi più facili da ricordare, sacrificando però la protezione dei propri dati.

La crescente quantità di servizi online porta ogni utente a gestire decine di credenziali diverse; chiedere di crearle tutte robuste e uniche è impraticabile senza strumenti di supporto. Per questo è essenziale progettare la sicurezza tenendo conto dell'esperienza dell'utente.

1.4. Classifica e-mail più rilevate per dominio e paesi maggiormente colpiti dal fenomeno

Come già detto, gran parte dei dati trovati fa riferimento ad account di posta elettronica.

La classifica delle e-mail più rilevate sul dark web, per quanto riguarda la composizione dei domini, ci permette di localizzare il provider dell'e-mail, ad esclusione del ".com" e ".net" che hanno copertura globale.

Il dominio .com, oltre ad essere il più utilizzato negli **USA**, è diffuso in tutti i paesi; nel caso in cui vengano ritrovati più dati (es. indirizzo postale), è possibile risalire al paese della vittima.

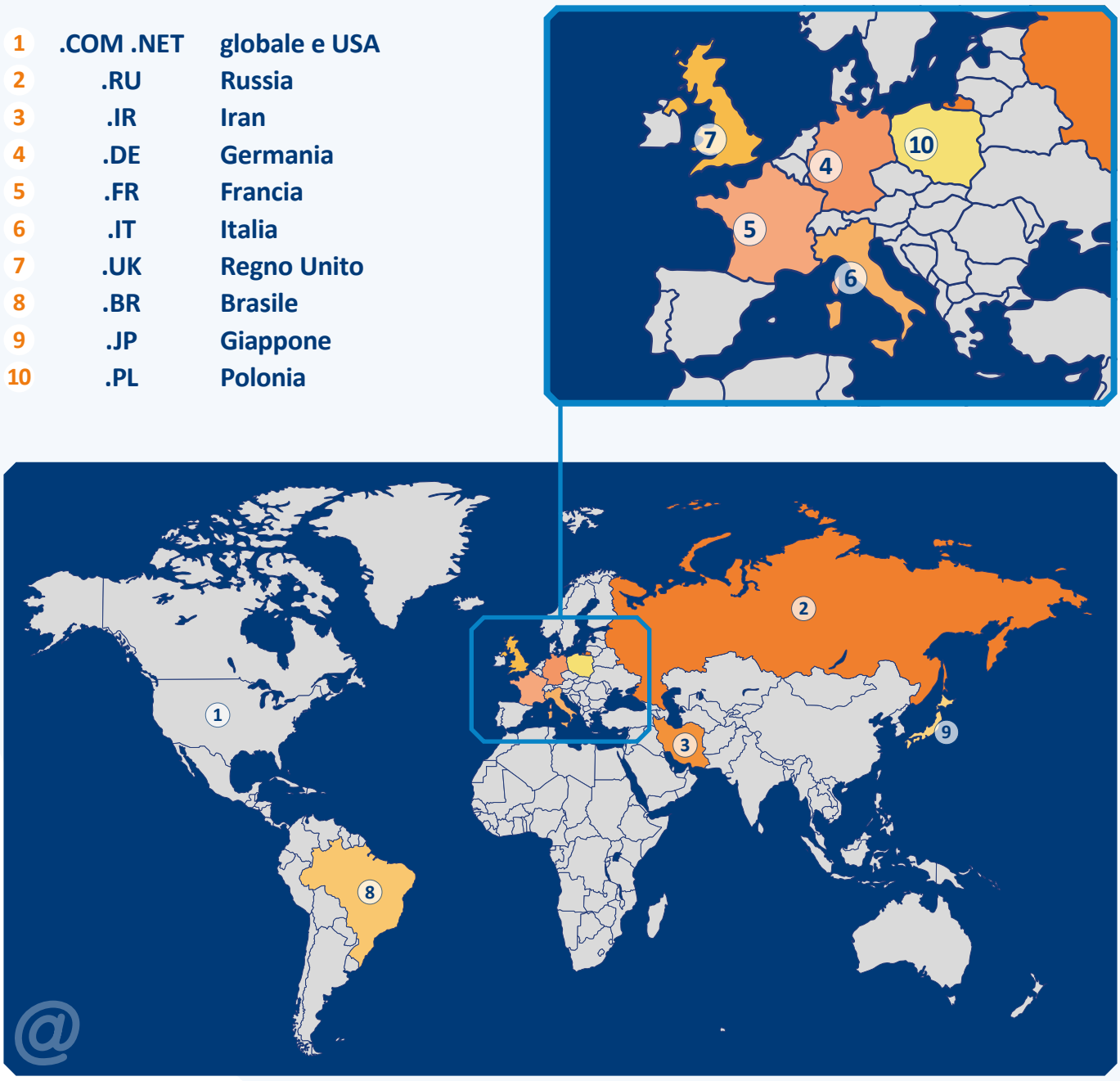
Si può quindi desumere che i paesi maggiormente colpiti dal fenomeno del furto di e-mail e password online, oltre agli stessi **USA**, sono **Russia, Iran, Germania e Francia**. Segue **l'Italia**, che occupa la sesta posizione, seguita dal **Regno Unito**.

Gli altri paesi che completano la top 10 dei domini maggiormente colpiti nel furto di password online sono **Brasile, Giappone e Polonia**.

Da segnalare la **scalata dell'Iran** che passa dalla posizione 124 al terzo posto. L'aumento degli account iraniani può essere attribuito in gran parte alle tensioni geopolitiche in Medio Oriente. In particolare, sono state prese di mira le agenzie governative.

Top 10 Paesi maggiormente colpiti nel 2025

1	.COM .NET	globale e USA
2	.RU	Russia
3	.IR	Iran
4	.DE	Germania
5	.FR	Francia
6	.IT	Italia
7	.UK	Regno Unito
8	.BR	Brasile
9	.JP	Giappone
10	.PL	Polonia



Fonte: Osservatorio Cyber CRIF

1.5. Dove vengono carpiti più dati di carte di credito?

La classifica dei continenti più soggetti a scambio di **dati illeciti di carte di credito** vede in testa **l'Europa**, con una significativa crescita rispetto al periodo precedente (+32%) seguita dall'Asia, che col 13,1% supera il Nord America (5,7%). L'Africa supera il Sud America, mentre l'Oceania rimane fanalino di coda di questa poco invidiabile classifica.

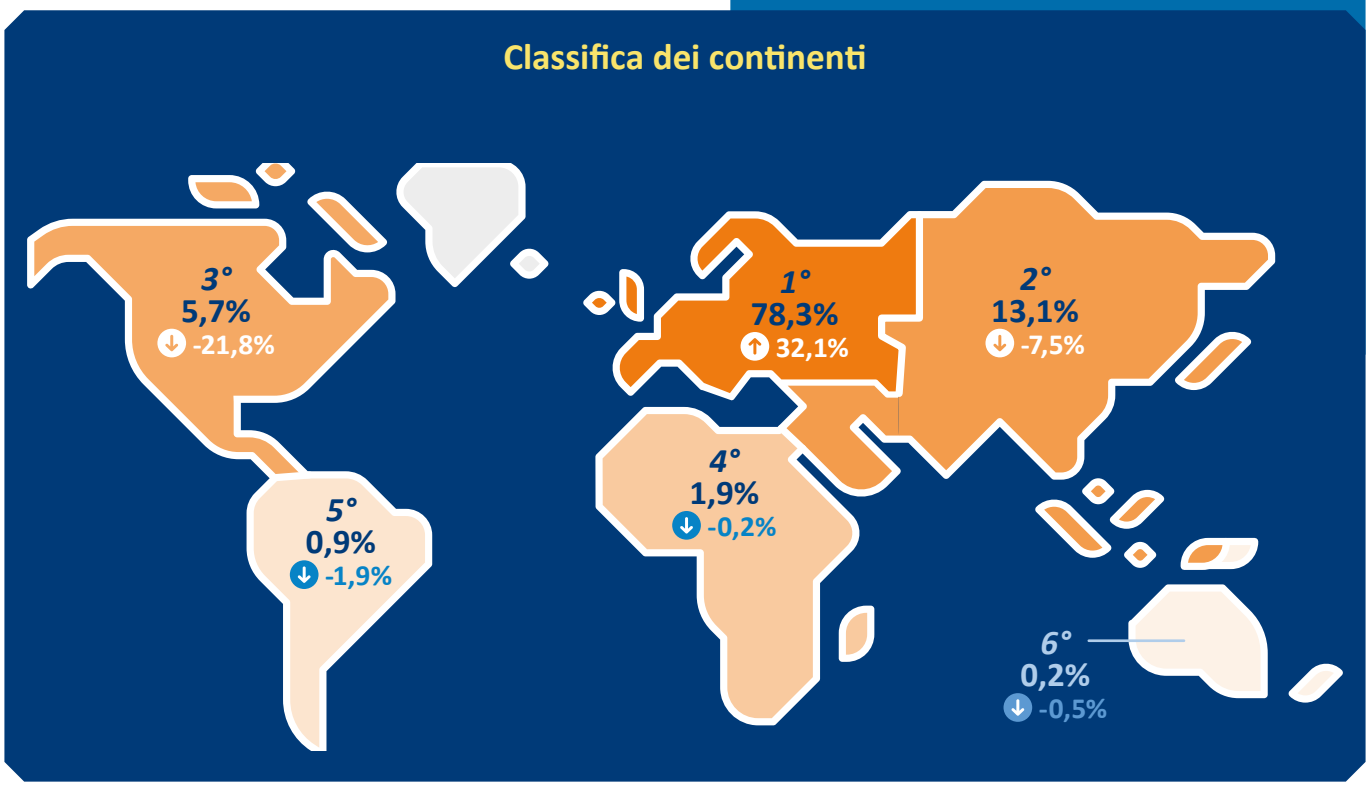
La classifica dei **Paesi più colpiti dallo scambio di dati delle carte di credito rubate continua a essere guidata dalla Russia**, seguita da India e Stati Uniti.

L'**Italia occupa il 23esimo posto** della classifica globale.

Paesi più soggetti a scambio di dati di carte di credito nel 2025

1	Russia	11	Germania
2	India	12	Brasile
3	Stati Uniti	13	Tanzania
4	Nigeria	14	Australia
5	Qatar	15	Giappone
6	Regno Unito	16	Tailandia
7	Messico	17	Cina
8	Canada	18	Filippine
9	Malesia	19	Singapore
10	Hong Kong	20	Francia

Classifica dei continenti



Fonti: Osservatorio Cyber CRIF

1.6. Focus: top 3 Paesi per continente

Di seguito le classifiche dei paesi più soggetti a scambio di dati di carte di credito per ciascun continente.

TOP 3 Europa 2025
1. Germania
2. Francia
3. Spagna

TOP 3 America 2025
1. Stati Uniti
2. Messico
3. Canada

TOP 3 Asia 2025
1. India
2. Qatar
3. Malesia

TOP 3 Africa 2025
1. Nigeria
2. Tanzania
3. Sud Africa

TOP 3 Oceania 2025
1. Australia
2. Nuova Zelanda
3. Papua Nuova Guinea

2. Focus Italia

2.1. Utenti che hanno ricevuto alert

Le attività degli hacker continuano ad avere una grande rilevanza anche nel 2025.

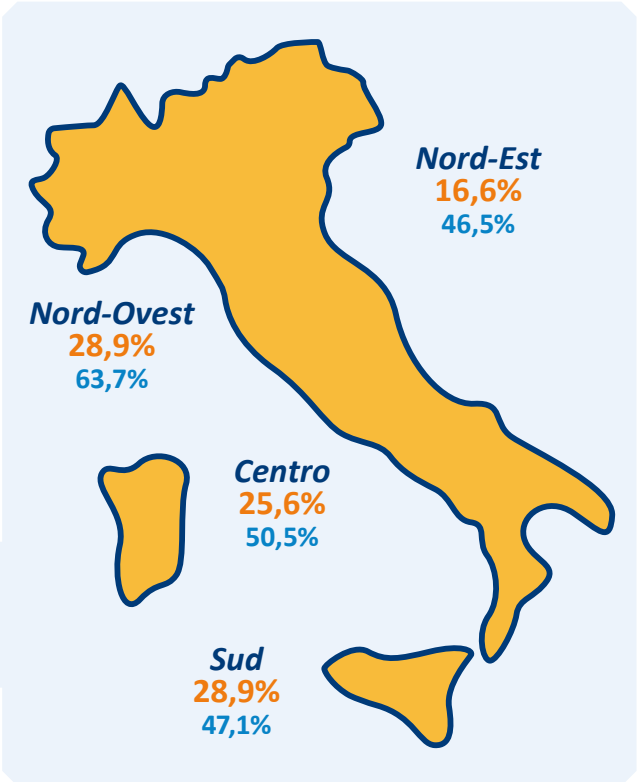
I dati dell'Osservatorio Cyber CRIF confermano un numero di consumatori allertati sul dark web, grazie ai servizi di CRIF, in crescita del +4,6% rispetto all'anno precedente.

Facendo un focus sull'Italia, dove **il 51,8% degli utenti ha ricevuto almeno un alert** nel 2025, si rileva in particolare un **aumento degli alert** inviati relativamente a furto di dati monitorati **sul dark web**. Gli **utenti allertati** per dati rilevati sul **dark web sono l'85,6%** mentre solo il **14,4%** degli utenti sono stati allertati per dati rilevati sul **web pubblico**.

Vediamo le **caratteristiche degli utenti privati italiani** che sono stati allertati dai nostri servizi di protezione dei dati personali sul web. Le fasce di età maggiormente coinvolte sono quelle dei 51-60 anni (26,8%) seguite dai 41-50 anni (25,3%) e dagli over 60 (25,2%). Gli uomini rappresentano la maggioranza degli utenti allertati (64,6%).

Le **regioni** in cui vengono allertate più persone sono Lazio (16,3%), Lombardia (15,2%), Sicilia (9,7%), Emilia-Romagna e Piemonte (entrambe 8,0%), ma in proporzione sono gli abitanti di Sardegna, Umbria, Lazio, Calabria e Friuli-Venezia Giulia che ricevono più alert.

Le **aree geografiche** in cui vengono allertate più persone sono il Sud (31,8%) e il Centro (26,2%), ma in proporzione sono gli abitanti del Nord Ovest e del Centro che ricevono più alert.



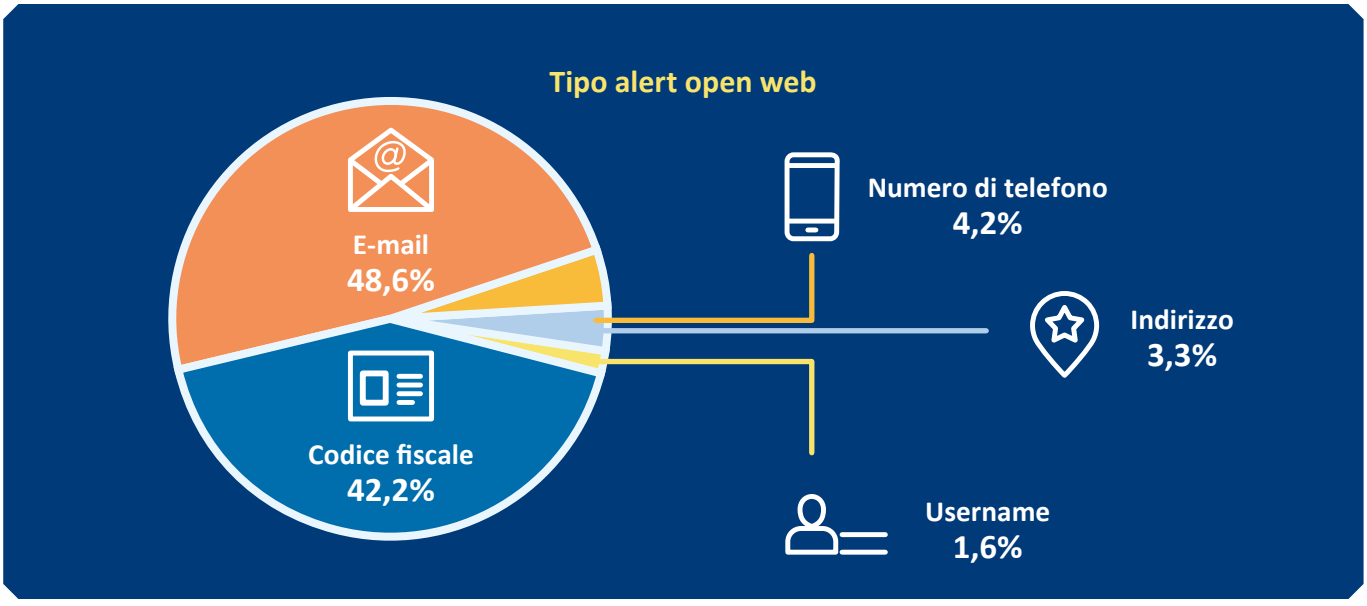
Area geografica
Distribuzione clienti allertati
Percentuale clienti allertati

Fonte: Osservatorio Cyber CRIF

2.2. Tipologia di dati rilevati di utenti italiani

Nel 2025, **i tipi di dati più frequentemente rilevati sull'open web**, quindi pubblicamente accessibili da chiunque sul web, sono stati l'**e-mail** (48,6% % dei dati rilevati) e il **codice fiscale** (42,2%), seguiti a distanza da **numero di telefono** (4,2%), **indirizzo** (3,3%) e **username** (1,6%).

Nel dark web sono state invece le credenziali e-mail ad essere più frequentemente rilevate nel 2025, in secondo luogo il **numero di telefono,** mentre al terzo posto si colloca il **codice fiscale**: questi preziosi dati potrebbero essere utilizzati per cercare di compiere truffe, ad esempio attraverso *phishing* o *smishing*.



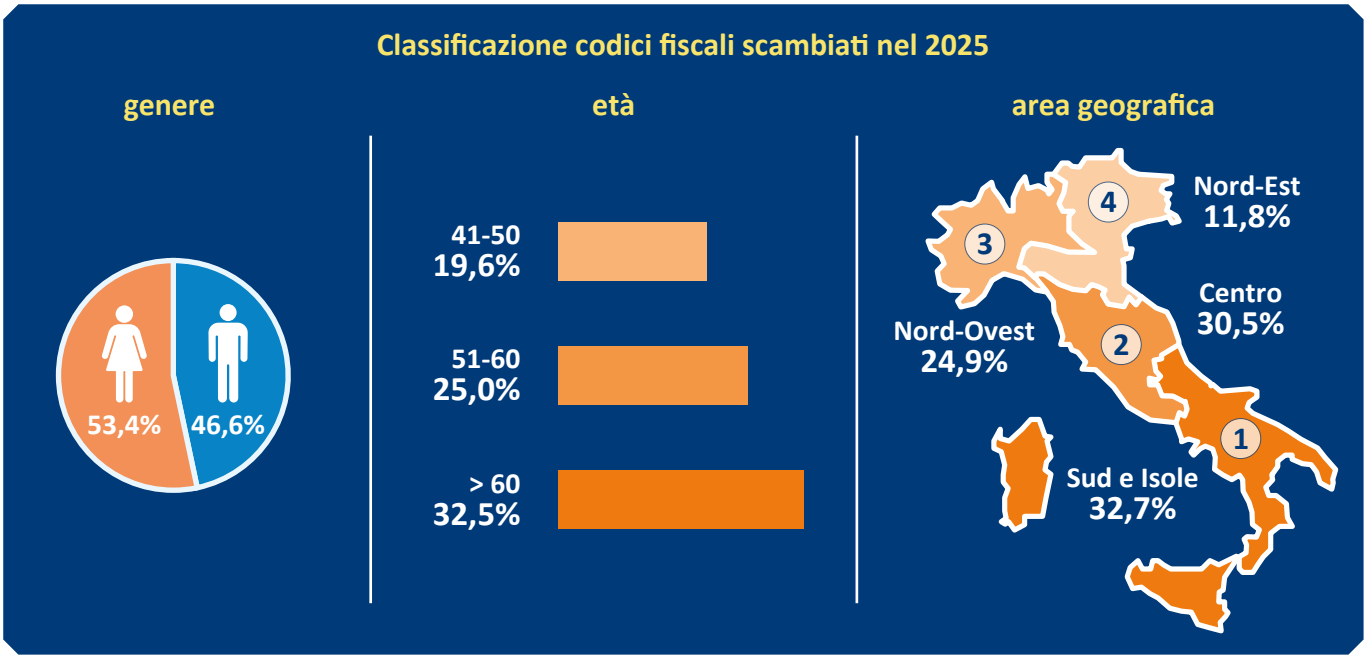
Fonti: Osservatorio Cyber CRIF

La presenza del **codice fiscale sul dark web** rappresenta un rischio concreto perché facilita furti d'identità e frodi con impatto economico. Nel 2025 abbiamo osservato numerosi **codici fiscali** scambiati in ambienti pericolosi, classificati per **età**, **genere** e **area geografica** di provenienza delle vittime.

Le fasce maggiormente coinvolte risultano gli **over 60**, pari al **32,5%** del totale (17,8% donne e 14,7% uomini), seguite dai **51-60 anni**, che rappresentano complessivamente il **25%** (14,3% donne e 10,7% uomini). A seguire troviamo la fascia **41-50**, che incide per **19,6%** (10,8% donne e 8,8% uomini). Le fasce più giovani **under 30** mantengono una presenza molto più contenuta, attorno al **6-7%**.

Dal punto di vista di genere si osserva una lieve prevalenza femminile: **53,4% donne** contro **46,6% uomini**. Sul piano territoriale, le quote maggiori provengono dal **Sud e Isole (32,7%)** e dal **Centro (30,5%)**, seguite dal **Nord Ovest (24,9%)**, mentre il **Nord Est (11,8%)** presenta un'incidenza inferiore ma comunque significativa.

Nel complesso emerge che la presenza del codice fiscale sul darkweb coinvolge principalmente **popolazione adulta e senior**, distribuita soprattutto nelle **regioni** più popolate del Paese (Lombardia, Lazio, Sicilia).



Fonti: Osservatorio Cyber CRIF

2.3. Come proteggersi da furti d'identità e truffe online

Sul dark web è presente una enorme mole di dati di ignari cittadini, che sono a rischio di subire furti d'identità e truffe online. Cosa devono fare le persone per proteggersi?

Ecco alcuni consigli per proteggere i dati personali dal rischio di subire furti d'identità e truffe online:

1. **Attivazione di aggiornamenti automatici per sistema operativo, applicazioni e browser:** il dispositivo sarà sempre protetto dalle ultime minacce e vulnerabilità che i criminali informatici potrebbero sfruttare.
2. **Backup regolari su cloud o dispositivi esterni e verifica periodica della loro integrità:** oltre a questo, fare una copia dei documenti più importanti o più utilizzati, in modo che siano sempre recuperabili via internet.
3. **Protezione dei dispositivi:** pin, password, riconoscimento facciale, ma anche autenticazione a due fattori per un livello di sicurezza aggiuntivo. Inoltre, attivazione del controllo remoto e la cancellazione dei dati in caso di smarrimento o furto, sono un'ulteriore tutela.
4. **Prestare attenzione a siti, mail e telefonate sospette**: è bene verificare sempre l'autenticità dei siti controllandone la URL e il certificato di sicurezza, evitando di cliccare su link sospetti presenti in sms, messaggi whatsapp ed e-mail. Evitare di fornire informazioni personali o finanziarie tramite messaggio o telefonata che li richieda.
5. **Per una sicurezza completa**, utilizzare **servizi per controllare la circolazione dei dati personali** e finanziari sul web e un antivirus ad ampia protezione sui dispositivi.

Considerando che le minacce del phishing e dello smishing sono in costante evoluzione, per proteggersi efficacemente è fondamentale adottare un approccio proattivo:

1. **Essere prudente**: diffidare di qualsiasi comunicazione, sia via e-mail, SMS, chiamata o messaggio che solleciti informazioni personali, password, telefono, codici di accesso, dati della carta di credito o informazioni finanziarie: nessuna banca chiederà mai di fornire queste informazioni per telefono o via mail.
2. **Verificare l'identità del mittente:** controllare attentamente l'indirizzo e-mail, il numero di telefono o l'URL del sito web, prestare attenzione a eventuali errori di ortografia, domini sospetti o indirizzi e-mail generici. Verificare sempre che l'URL inizi con "https://" e che sia presente il lucchetto nella barra degli indirizzi.
3. **Evitare di cliccare su link sospetti** ricevuti via e-mail o SMS, anche se sembrano provenire da un mittente conosciuto. Digitare manualmente l'indirizzo web del sito ufficiale per accedere ai servizi online, o usare l'app ufficiale.
4. **Non scaricare allegati**: è sconsigliato aprire allegati provenienti da mittenti sconosciuti o sospetti, poiché potrebbero contenere malware.
5. **Segnalare l'accaduto**: se si abbocca ad una mail di phishing, che sembra provenire da un e-commerce o una banca, si consiglia di contattare gli istituti tramite i canali ufficiali. Potranno mettere in atto tutte le misure di protezione nei confronti del cliente. Se opportuno, segnalare l'accaduto anche alla Polizia Postale.

Infine, dal momento oltre il 64% della popolazione mondiale utilizza quotidianamente **social media** come LinkedIn, Facebook, TikTok, Instagram e X, e che l'utente "tipico" vi trascorre più di due ore al giorno, **anche queste piattaforme stanno diventando un bersaglio crescente per il phishing**. È quindi fondamentale mantenere alta l'attenzione anche in questo caso.

Vademecum sulla sicurezza cyber

Profili falsi: attenzione ai falsi profili. Ad esempio, anche se il profilo usa logo, colori e caratteri simili a quello del brand ufficiale, assicurati che ci sia la "spunta blu" sul profilo dei brand che segui.

Condivisione delle informazioni personali: per la natura stessa dei social network, tendiamo a condividere tante informazioni personali. Anche su cosa condividiamo è sempre bene fermarsi un attimo a riflettere: è necessario? Con chi sto condividendo le mie foto e le mie informazioni?

Link abbreviati: diffidare dalle short URL e posizionare il mouse sul link per visualizzare l'indirizzo web completo.

Doppia autenticazione: abilitare l'autenticazione a due fattori (2FA) per gli account social, così che non sia sufficiente conoscere solo la password per accedere al profilo.

3. La value proposition di CRIF

3.1 La linea Mister Credit dedicata alla protezione dal furto di identità

CRIF è al fianco dei player finanziari per supportarli nella prevenzione delle frodi con soluzioni digitali innovative che ottimizzano i controlli e garantiscono customer journey frictionless e sicure.

La linea di servizi **Mister Credit** di CRIF si rivolge a privati e piccole medie imprese per prevenire le frodi creditizie e proteggere l'identità online e offline.

Oltre 500.000 consumatori utilizzano oggi in Italia i servizi Mister Credit per la protezione dal furto di identità.

IDENTIKIT è la **soluzione che consente di proteggere la propria identità**, avvisando quando viene richiesto un finanziamento a proprio nome, grazie a:

- **check up dei dati**, attingendo al Sistema di Informazioni Creditizie di CRIF e agli archivi pubblici, per avere un'analisi dettagliata dei propri dati creditizi e scoprire se si è vittima di un furto di identità;
- **monitoraggio costante e alert** che avvisano nel caso in cui venga richiesto credito o iscritto un protesto a proprio nome;
- **assistenza telefonica** per ripristinare la propria reputazione creditizia in caso di furto di identità.

SICURNET è la **soluzione che tiene sotto controllo la circolazione dei dati personali e finanziari sul web**, per impedire che possano essere utilizzati per scopi illeciti. In particolare, il servizio:

- **tutela i propri dati**, tenendo sotto controllo la circolazione di informazioni quali data di nascita, indirizzo, username, codice fiscale, numero dei documenti d'identità, indirizzi e-mail, numeri di telefono e cellulare;
- **monitora carte e IBAN** per una sicurezza a 360 gradi;
- **protegge dai rischi** grazie a un monitoraggio costante e inviando alert ogni volta che uno dei dati sotto monitoraggio risulta troppo esposto o viene intercettato in ambienti web rischiosi.

IDENTINET è la **soluzione che protegge a 360 gradi la reputazione creditizia e i dati dal furto di identità nel mondo reale e sul web**, avvisando quando viene richiesto un finanziamento a proprio nome o nel caso in cui i propri dati personali siano a rischio sul web pubblico o sul dark web. Disponibile anche tramite App.

SICURNET BUSINESS è la **soluzione innovativa che aiuta le aziende a gestire il cyber risk e a monitorare i propri dati** sul dark web, inviando alert tempestivi in caso di furto di dati.

Perché scegliere un partner come CRIF?

- **CRIF Information Core**: l'cosistema di dati unico in Italia, con oltre 40 fonti informative.
- **Advanced Analytics** e **Process Automation** nel settore finanziario: **oltre 35 anni di esperienza**.
- **Team globale di oltre 200 data scientist** impegnato da oltre 10 anni nello sviluppo e applicazione di modelli AI based.
- Piattaforme digitali avanzate in uso presso oltre **700 player nel mondo**.
- Profonda conoscenza di **processi e normative** del settore finanziario.
- **Network di partner tecnologici e fintech** per offrire soluzioni sempre all'avanguardia.

Autori

Beatrice Rubini
Executive Director
CRIF Personal Solutions & Cybersecurity

Maria Cristina Manfredini
Marketing
CRIF Personal Solutions & Cybersecurity

Francesco Marinucci
Product Manager
CRIF Personal Solutions & Cybersecurity

Claudia Silvagni
Product Marketing
CRIF Personal Solutions & Cybersecurity

CRIF | The end-to-end knowledge company

CRIF è un'azienda globale specializzata in sistemi di informazioni creditizie e di business information, analytics, servizi di outsourcing e processing, nonché in avanzate soluzioni in ambito digitale e open banking per lo sviluppo del business.
Nel 2025 ha avuto ricavi per 900 milioni di euro.

CRIF punta a creare valore per i consumatori, le imprese e le istituzioni finanziarie, fornendo informazioni e soluzioni che consentono decisioni più consapevoli, migliorano l'accesso al credito e accelerano l'innovazione digitale.

CRIF offre anche servizi per privati cittadini e PMI dedicati alla protezione da frodi e rischi cyber. Inoltre, CRIF Ratings, agenzia di rating del credito registrata presso ESMA e agenzia esterna di valutazione del merito creditizio (ECAI), fornisce rating del credito e valutazioni su imprese non finanziarie in Europa.

CRIF è inoltre AISP in tutti i paesi europei dove è applicabile la direttiva PSD2 per l'open banking, oltre che AISP in UK. Fondata a Bologna nel 1988, oggi l'azienda opera in 37 nazioni, in 4 continenti, con oltre 85 società e 6.600 professionisti. Ad utilizzare i suoi servizi oggi sono oltre 10.500 banche e società finanziarie, più di 450 assicurazioni, 90.000 imprese e 1.000.000 di consumatori.

A partire dal 2025, l'azienda ha ampliato i propri servizi creando CRIF Synesgy Ratings, società specializzata nelle valutazioni ESG a supporto delle decisioni strategiche e operative di banche e imprese.

Per maggiori informazioni

crif.it
mistercredit.it

CRIF Finance Italy

marketingfinanceitaly@crif.com

CRIF
LinkedIn - CRIF Finance Italy
marketingfinanceitaly@crif.com

crif.it

Together to the next level