Osservatorio Cyber

CRIF-Mister Credit

Analisi delle attività cyber nel 2024

CRIF
Together to the next level

Indice

Analisi delle attività cyber nel 2024

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.

Grazie all'analisi dell'Osservatorio emergono inoltre i rischi a cui vengono esposti quotidianamente individui e business, valutando i principali trend e offrendo alcuni spunti per fronteggiare le minacce cyber.

I dati sono il frutto di un'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**.

Cosa si intende per dark web e come funziona?

Il Dark Web è **un insieme di ambienti web che non appaiono attraverso le normali attività di navigazione** 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 2024, abbiamo rilevato **l'esposizione di nuovi dati** in circolazione sul dark web sempre più completi e da poter utilizzare per mettere a segno frodi di vario tipo.

> Nel 2024 si evidenziano oltre 2.080.000 segnalazioni inviate in merito all'esposizione dei dati sul dark web con un aumento del 15,4% degli alert rispetto al 2023.

Questi dati rivelano non solo la natura pervasiva dei cyberattacchi, ma anche la crescente difficoltà per le persone di proteggersi da schemi sempre più sofisticati. Tra questi, lo **smishing** - attacchi fraudolenti tramite SMS e app di messaggistica come WhatsApp - **è aumentato notevolmente** nell'ultimo anno. In Italia, ad esempio, una recente campagna di smishing simulava servizi di spedizione postale, inducendo gli utenti a rivelare

le credenziali bancarie tramite WhatsApp, o a ricevere finte notifiche di consegna di Amazon tramite SMS.

Oltre a queste, il **phishing** tradizionale, il **vishing** e lo **spear phishing** rimangono minacce significative. Tuttavia, l'emergere di **attacchi guidati dall'intelligenza artificiale** è diventato una nuova e pericolosissima **minaccia**: solo per citarne alcune, le false truffe di Elon Musk, in cui video e audio **deepfake** sono stati utilizzati per promuovere schemi di investimento fraudolenti. Oppure le **truffe CEO WhatsApp deepfake**, che hanno preso di mira molte aziende in tutto il mondo, inducendo i dipendenti a trasferire fondi sulla base di istruzioni apparentemente legittime dei loro superiori.

Inoltre, la continua proliferazione 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.

Il numero di alert inviati in relazione all'esposizione dei dati sul web pubblico è stato di 59.000 nel 2024, in calo del 27% rispetto al 2023. Tra i dati più frequentemente rilevati 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 concorsi di ammissione enti pubblici.

In questo contesto, dove si colloca l'Italia?

L'Italia non è certo immune da questa minaccia. Nel 2024, il paese si è classificato al **quinto posto a livello globale in termini di indirizzi e-mail compromessi** che circolano sul dark web.

Per quanto riguarda i dati delle **carte di credito** in circolazione, l'Italia si colloca al **18° posto** a livello mondiale, una posizione comunque significativa.

Infine, è al 52° posto per il rilevamento dei **numeri telefonici** nella classifica mondiale e al 12° posto nell'Unione europea.

È evidente che bisogna prestare attenzione ai dati che vengono condivisi e proteggerli con strumenti adeguati, ma è anche essenziale essere consapevoli delle nuove tecniche di attacco e delle vulnerabilità dei sistemi e dei dispositivi che utilizziamo quotidianamente.

La rapida evoluzione dell'Intelligenza Artificiale avanzata, pur offrendo vantaggi come i chatbot conversazionali, ha aumentato in modo significativo le minacce di ingegneria sociale.

Man mano che aumentano i contenuti online generati dall'Intelligenza Artificiale sorgono nuove sfide per molti utenti, che non sono consapevoli della potenza e della facilità con cui queste tecnologie possono essere utilizzate dai truffatori.

Inoltre, le tensioni geopolitiche globali, combinate con l'evoluzione delle tecniche criminali informatiche grazie all'IA, rendono ancora più necessarie misure di protezione preventiva e reazioni proattive contro potenziali attacchi mirati ad aziende, infrastrutture critiche e istituzioni governative.

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.
CEO WhatsApp deepfake: truffa informatica in cui i criminali utilizzano l'intelligenza artificiale per imitare la voce di un CEO e ingannare i dipendenti tramite messaggi vocali o chiamate su WhatsApp.
Stealer-as-a-Service: malware per rubare informazioni, come credenziali e dati finanziari.

Osservatorio Cyber
CRIF-Mister Credit

Analisi delle attività cyber nel 2024

Italia al 5° posto
per furto di e-mail e password online

2,1 MILIONI
gli alert cyber di CRIF

utenti allertati per dati sul **dark web**

e

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

+13,5% 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**.

I DATI PIÙ VULNERABILI SUL WEB

PASSWORD
le più utilizzate:
123456
123456789
12345678

E-mail personali e aziendali

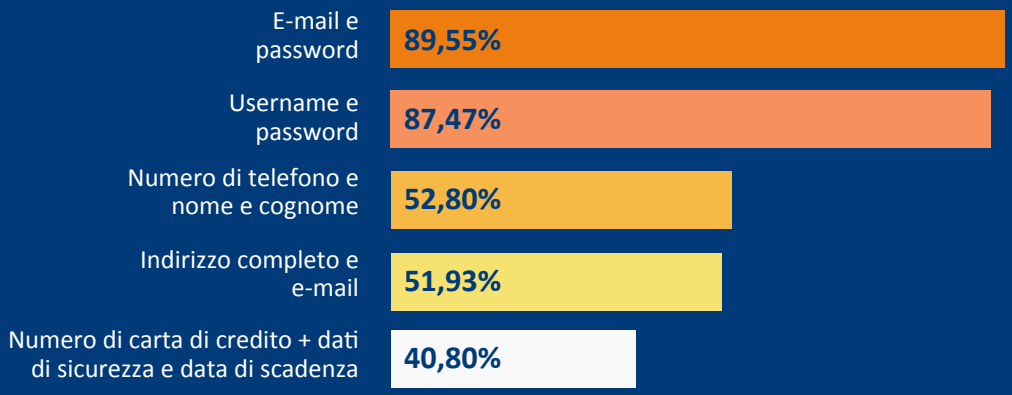
Username

Numero di telefono

Nome e cognome

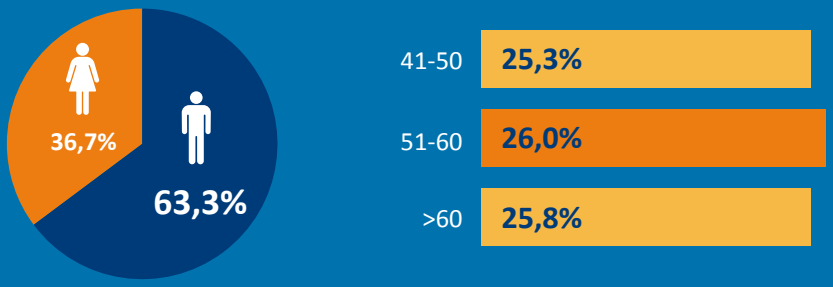
Password ed e-mail si confermano i dati più vulnerabili insieme alla **username**, seguiti da numero di telefono e da nome e cognome.

LE COMBINAZIONI DI DATI PIÙ ESPOSTE



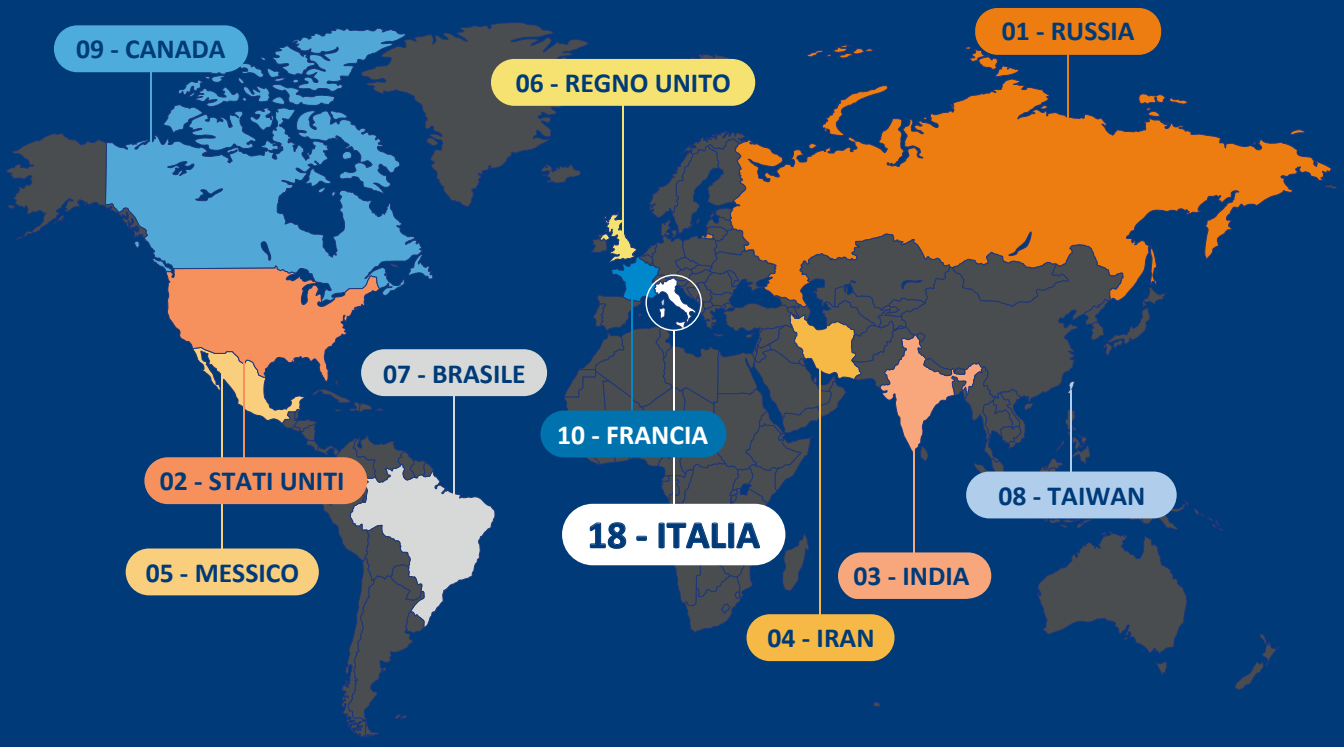
Preoccupante la combinazione di **numeri di carta di credito**, **dati di sicurezza** e **date di scadenza**, riscontrata nel **40,80%** dei casi.
Benché in sensibile calo rispetto al 2023 e alle altre combinazioni di dati, rimane altamente **allarmante a causa del grave rischio di frode finanziaria**.

IL PROFILO DEGLI UTENTI PIÙ COLPITI



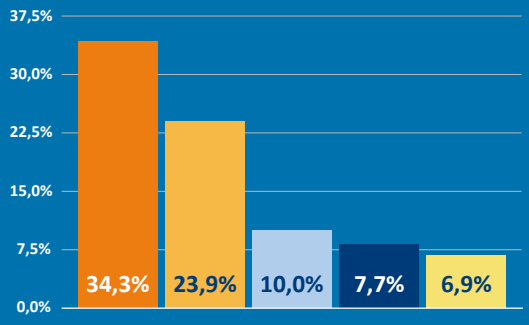
La fascia di età degli utenti maggiormente a rischio è quella dei **51-60**, seguita dagli **over 60** quasi a pari merito con i **41-50**.

DOVE VENGONO RUBATI I DATI DELLE CARTE DI CREDITO



01 — 10

GLI ACCOUNT PIÙ RUBATI OLTRE ALLE E-MAIL



- **Servizi di VPN**
- **Social network**
- **Siti internet**
- **E-commerce**
- **Enti pubblici / istituzioni**

Escludendo i servizi di posta elettronica, tra le altre tipologie abbiamo al primo posto i **servizi di VPN**, al secondo posto account relativi ai più diffusi **social network**, seguono **siti internet e di e-commerce**. Si sottolinea l'**ingresso al quinto posto del furto di account relativi a enti pubblici e istituzioni**; i **servizi finanziari** (come piattaforme di pagamento) scendono invece al settimo posto.

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. Dati vulnerabili e combinazioni di dati

Rispetto al fenomeno cyber, le categorie di dati bersaglio di attacchi sono molteplici.

Dalle analisi emerge che **indirizzi e-mail, password, nomi utente, numeri di telefono, nomi e cognomi** sono i dati più diffusi sul dark web e quindi più vulnerabili. Sono comuni anche quelli relativi agli **indirizzi di residenza, ai documenti d'identità e codici identificativi personali.**

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

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

Si consideri che, con un solo numero di telefono, possono essere effettuati vari tipi di phishing e truffe, come la truffa "**Account takeover**" che appare come una notifica di accesso insolito a un account, ad esempio un conto bancario online, da un altro dispositivo. L'utente è invitato a fare clic su un link per ripristinare l'accesso fornendo determinate informazioni. L'obiettivo di questo attacco è quello di ottenere credenziali e altri dati personali per commettere frodi.

Ricordiamo che una banca non richiederà mai informazioni personali tramite messaggi, quindi è importante non rispondere.

Le combinazioni di dati più esposte

L'analisi delle **combinazioni principali di dati ritrovati** nel 2024 rivela un quadro chiaro delle informazioni più vulnerabili agli attacchi informatici.

> La combinazione di e-mail e password è la più comune, con la password che appare accanto alla e-mail nel 89,55% dei casi, e nel 87,47% dei casi è anche associata alla username.

La combinazione di **username e password** è principalmente legata agli account aziendali, evidenziando possibili 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.).

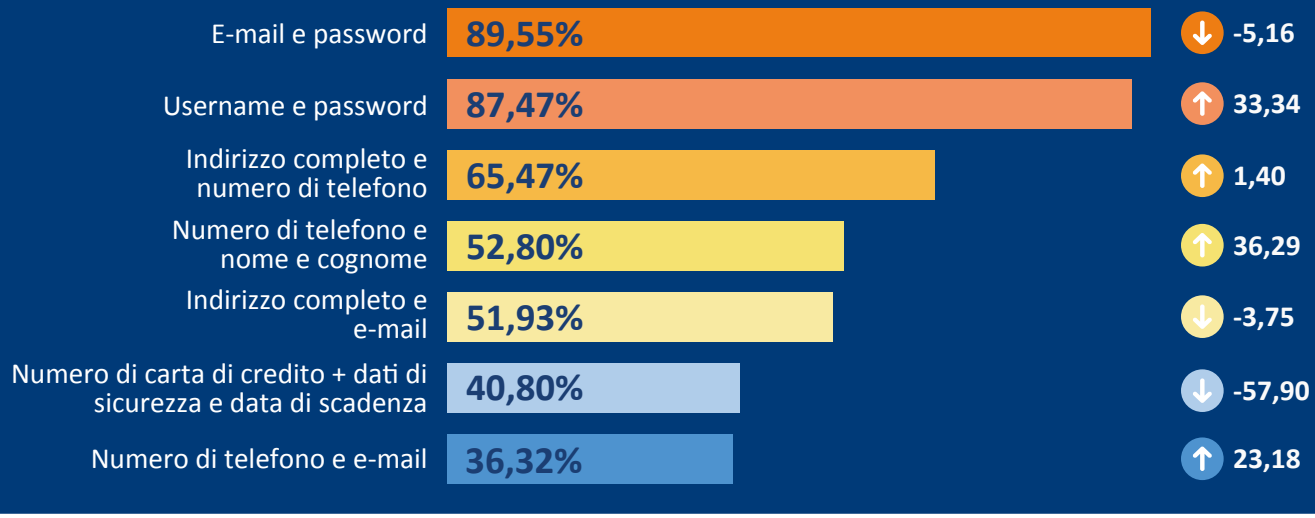
Un'altra preziosa informazione per i criminali informatici è **l'indirizzo residenziale completo,** che è associato **all'e-mail** nel 51,93% dei casi e al **numero di telefono** nel 65,47% dei casi. L'elevata percentuale di **numeri telefonici** con nomi e cognomi può essere collegata al fenomeno dello smishing.

Preoccupante, inoltre, la combinazione di numeri di carta di credito, dati di sicurezza e date di scadenza, trovata nel 40,80% dei casi.
Anche se l'incidenza è inferiore rispetto ad altre combinazioni di dati, rimane altamente allarmante a causa del grave rischio di frode finanziaria.

TOP 10 dei dati più vulnerabili nel 2024

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

Combinazioni principali dei dati



Fonti: Osservatorio Cyber CRIF

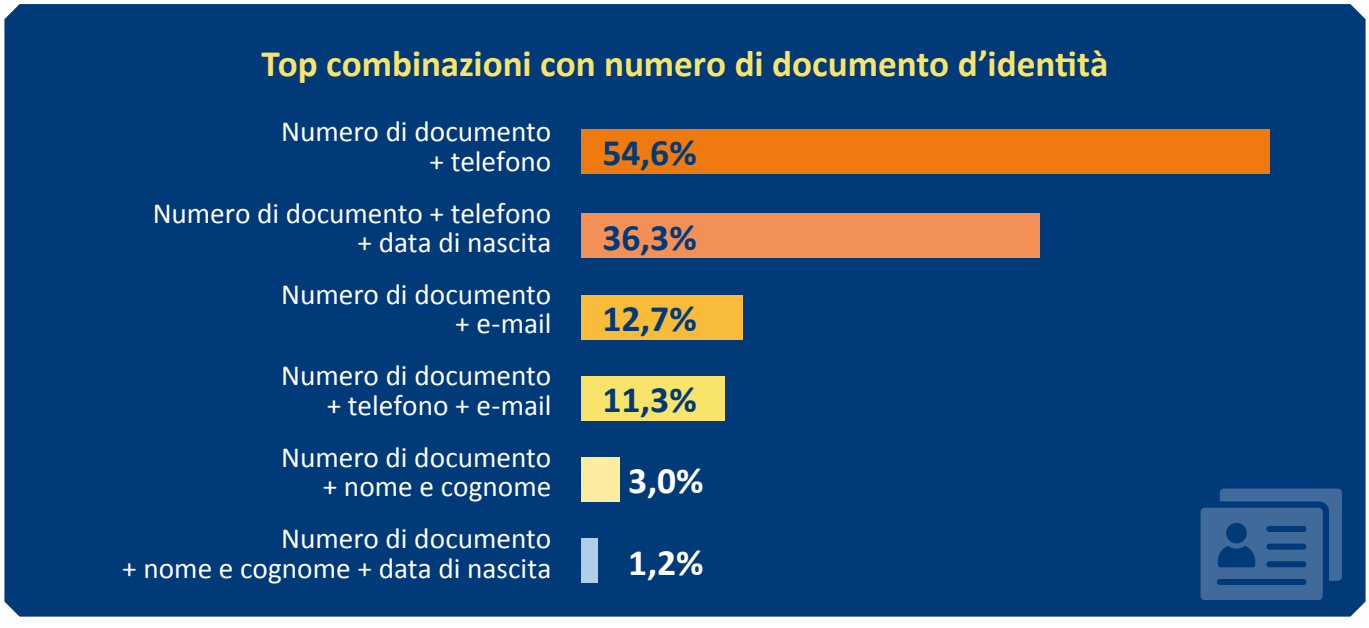
Documenti d'identità

Esaminando le combinazioni di dati che includono un **numero di documento d'identità**, possiamo osservare come questi, associati ad altri dati personali, diventino preziosi e vulnerabili agli attacchi.

Queste informazioni possono essere sfruttate per ricreare un profilo completo della vittima, consentendo ai truffatori di richiedere prestiti, carte di credito, o di effettuare acquisti utilizzando l'identità della vittima.

La combinazione più frequente è quella di numero di documento associato al numero di telefono nel 54,6% dei casi, seguita dal numero di documento rilevato assieme a numero di telefono e data di nascita nel 36,3% dei casi.

Infine, la combinazione di numero di documento con telefono ed e-mail è meno comune, con un'incidenza dell'11,3%. Benché meno frequente, questa combinazione rimane rilevante poiché può essere utilizzata per phishing e altre forme di attacco.



Fonte: Osservatorio Cyber CRIF

Numero identificativo personale

Altre combinazioni interessanti sono quelle relative ai **numeri identificativi personali**, come **codice fiscale** o **numero di previdenza sociale**, che nel 46,4% dei casi vengono ritrovati assieme a **numero di telefono**, nel 23,4% assieme **all'e-mail**, inoltre il numero identificativo personale è rilevato con **telefono** ed **e-mail** nel 22,7% dei casi.

Per quanto riguarda la combinazione relativa al numero identificativo personale con **indirizzo completo ed e-mail** è rilevata nel 21,4% dei casi.

Infine, la combinazione con **nome e cognome e data di nascita** è rilevata nel 12,5% dei casi.

Queste percentuali mostrano che spesso il numero identificativo personale viene carpito assieme a diversi altri dati personali, che dobbiamo imparare a proteggere e monitorare in modo efficace.

Fonte: Osservatorio Cyber CRIF

1.2. Tipologia di account più rilevati

Al primo posto i servizi di VPN, al secondo posto account relativi ai più diffusi social network, seguono siti internet e di e-commerce

L'analisi qualitativa dei contesti in cui i dati circolano permette di comprendere le tipologie di servizi a cui sono associati gli account rintracciati sul dark web.

Escludendo i servizi di posta elettronica, tra le altre tipologie abbiamo al **primo posto** i **servizi di VPN,** al **secondo posto** account relativi ai più diffusi **social network**, seguono siti **internet** e di **e-commerce**, mentre si sottolinea l'ingresso al **quinto posto** del furto di account relativi a **enti pubblici e istituzioni**; i **servizi finanziari** (come piattaforme di pagamento) scendono invece al **settimo** posto.

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

Anche per questa tipologia di furto di dati possiamo affermare che "il fattore umano" ha un grande peso: la disattenzione dell'utente è una delle cause più comuni, così come password deboli o utilizzate per più account.

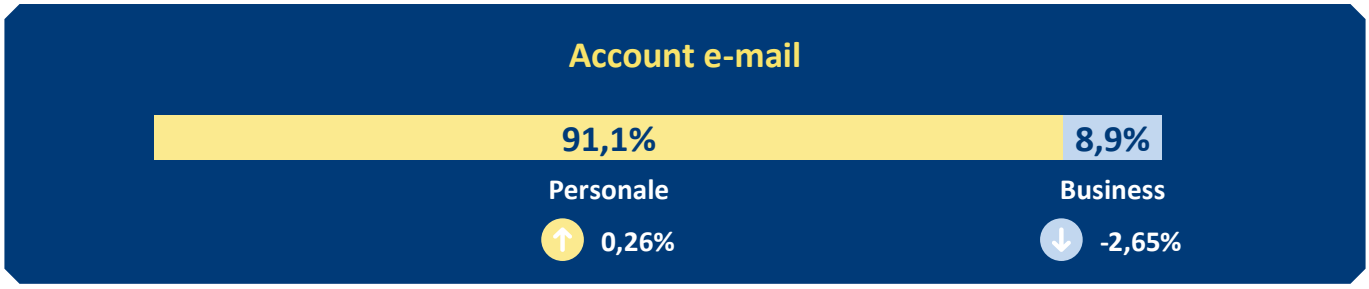
Un altro punto in comune tra alcuni tipi di account (come i social network, le piattaforme di streaming e di gioco) è la **volontà degli utenti di fornire le proprie credenziali a servizi apparentemente innocenti che offrono omaggi** come elementi di gioco, classifiche di musica in streaming e così via – quando in realtà spesso si tratta di un semplice strumento di raccolta di credenziali.

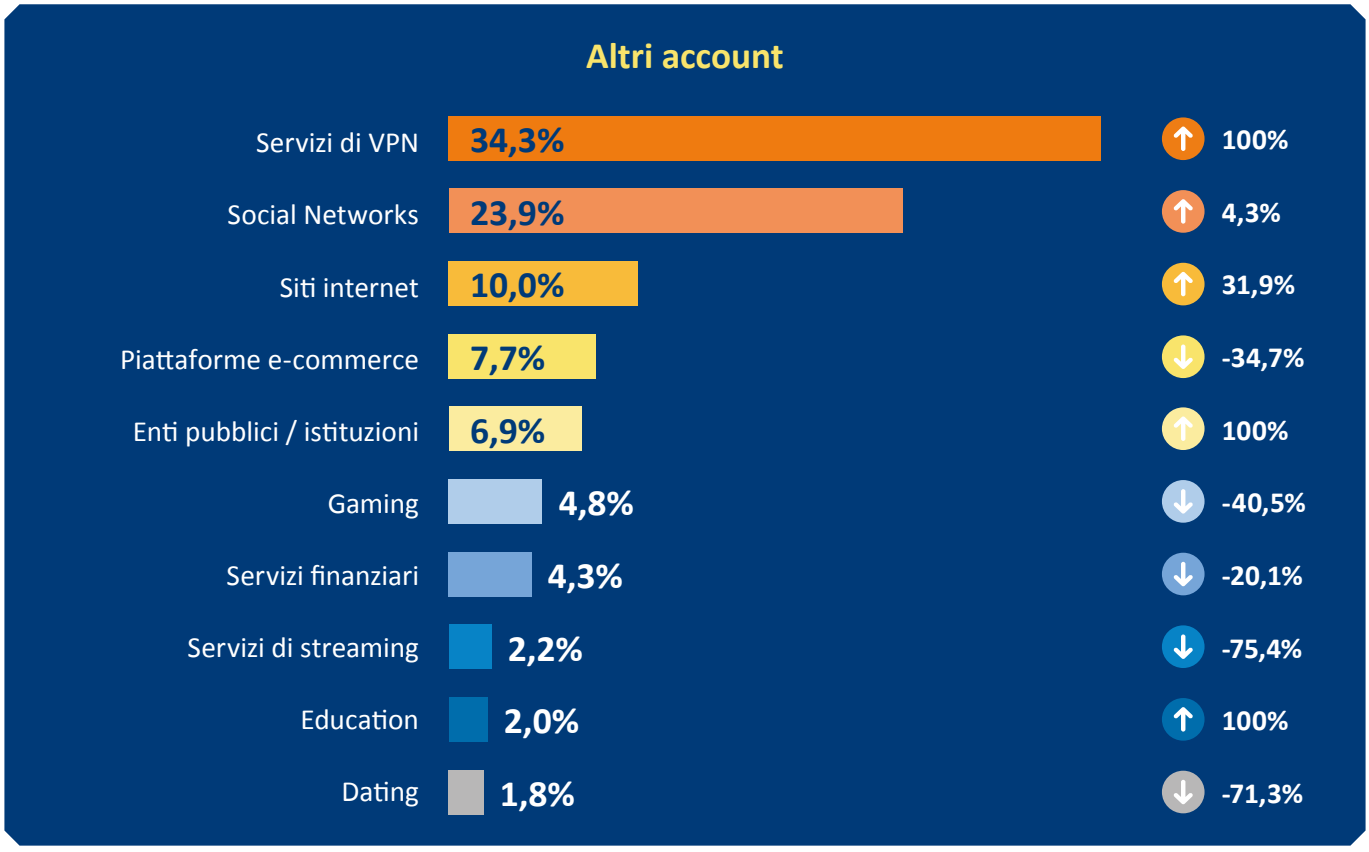
Attraverso una **analisi qualitativa dei domini degli account e-mail esposti sul dark web**, abbiamo rilevato se si riferiscono ad account personali o di business: **nel 91,3%** dei casi sono account e-mail **personali** mentre nel restante **8,7%** dei casi sono **account business**, ed è una tendenza che rimane stabile nel tempo.

Si conferma così che, da un lato, gli utenti privati prestano ancora un'attenzione limitata alla sicurezza online, continuando ad essere un bersaglio primario per gli hacker, dall'altro lato ci suggerisce che le aziende cercano di adottare misure di sicurezza per limitare la vulnerabilità dei propri dipendenti agli attacchi.

Inoltre, i privati non hanno alle spalle il supporto di un team IT dedicato e, in quanto tali, sono un facile bersaglio per i malintenzionati.

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 comuni sul dark web

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

La top 10 delle password in circolazione nel 2024 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 "111111", che possono essere hackerate letteralmente 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 è circoscritto a un singolo Paese. Anche in Italia, le password più comuni trovate sul dark web riferibili a utenti italiani includono combinazioni numeriche di base come "123456" o "123456789", nomi propri come "alessandro", "andrea" e "francesca", e riferimenti allo sport come "juventus" e "napoli", o a termini semplici come "ciaociao", "cambiami" e "amoremio". Questo dimostra che la scarsa attenzione alla sicurezza informatica è un problema diffuso a livello globale.

È fondamentale aiutare gli utenti a comprendere che una password debole rappresenta una porta aperta per gli hacker.

Per proteggere i propri dati, è necessario adottare comportamenti più responsabili, come creare **password complesse e uniche** per ogni account, utilizzare un **gestore di password,** attivare **l'autenticazione a due fattori** quando disponibile oppure un **monitoraggio dei propri dati** così da poter agire in modo mirato e rapido in caso di rilevamento, **riducendo il rischio di danni economici e reputazionali**.

Top 10 Password
in circolazione sul dark web nel 2024

1	123456
2	123456789
3	12345678
4	12345
5	111111
6	1234567
7	querty
8	1234567890
9	Password
10	qwertyuiop

Fonte: Osservatorio Cyber CRIF

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

Come evidenziato in precedenza, gran parte dei dati analizzati 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, Germania e Francia**. Segue **l'Italia**, che occupa la quinta posizione, seguita dal **Regno Unito**.

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

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 **crescita del 93,9%,** significativa rispetto al periodo precedente, seguita dal **Nord America benchè in calo del 49,4% rispetto al 2023.** Al terzo posto **l'Asia in crescita del 62,1%.**

Le posizioni di Sud America, Africa e Oceania restano invariate.

La classifica dei Paesi più colpiti dallo scambio di dati delle carte di credito rubate è guidata dalla Russia, che rispetto al 2023 sale dal 5° al 1° posto, seguita dagli Stati Uniti, che erano in testa alla classifica nel 2023.

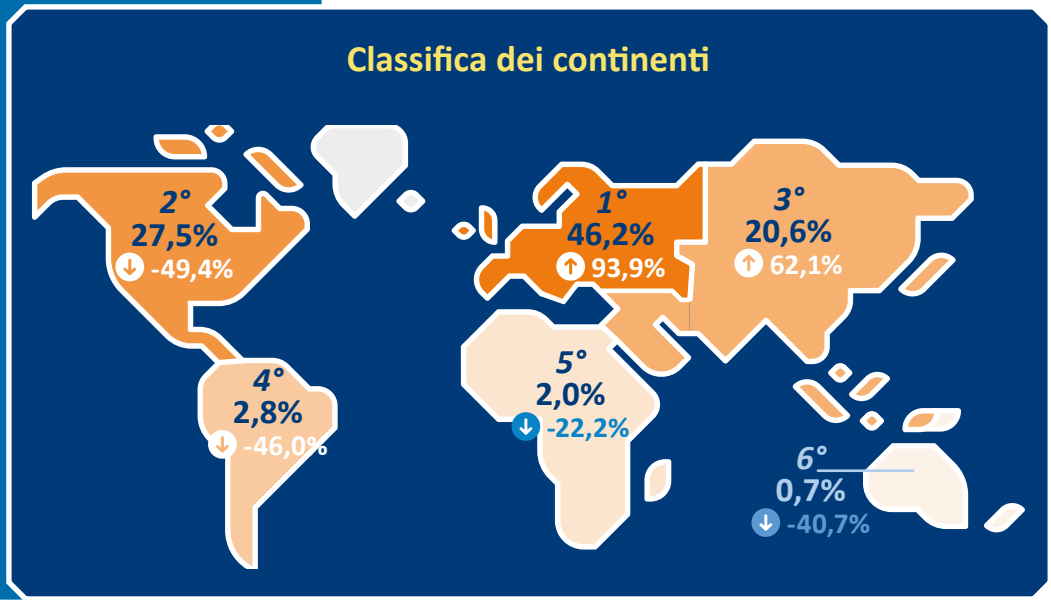
L'India segue, passando dall'ottavo al terzo posto, mentre al quarto posto troviamo **l'Iran**, non presente nella top 20 dello scorso anno, e al quinto il **Messico**, che passa dal terzo al quinto posto.

L'Italia occupa il 18esimo posto della classifica globale dei Paesi più soggetti a scambio di dati delle carte di credito.

Top 20 Paesi maggiormente colpiti nel 2024

1. Russia
2. Stati Uniti
3. India
4. Iran
5. Messico
6. Regno Unito
7. Brasile
8. Taiwan
9. Canada
10. Francia
11. Spagna
12. Cina
13. Giappone
14. Nigeria
15. Australia
16. Germania
17. Ucraina
18. Italia
19. Corea
20. Argentina

Classifica dei continenti



Fonti: Osservatorio Cyber CRIF

1.6. Focus: top 3 Paesi per continente

Di seguito le classifiche dei Paesi maggiormente soggetti a scambio di dati di carte di credito per ciascun continente; in particolare, in riferimento all'Europa, una specifica relativa ai Paesi che fanno parte dell'Unione europea.

TOP 3 Europa 2024

1. Russia
2. Regno Unito
3. Francia

TOP 3 EU 2024

1. Francia
2. Spagna
3. Germania

TOP 3 America 2024

1. Stati Uniti
2. Messico
3. Brasile

TOP 3 Asia 2024

1. India
2. Iran
3. Taiwan

TOP 3 Africa 2024

1. Nigeria
2. Sud Africa
3. Egitto

TOP 3 Oceania 2024

1. Australia
2. Nuova Zelanda
3. Guam

2. Focus Italia

2.1. Utenti che hanno ricevuto alert

Le attività degli hacker continuano ad avere una grande rilevanza anche nel 2024.

I dati dell'Osservatorio Cyber CRIF confermano un numero di consumatori allertati sul dark web, grazie ai servizi di CRIF, in crescita del +13,5% rispetto all'anno precedente.

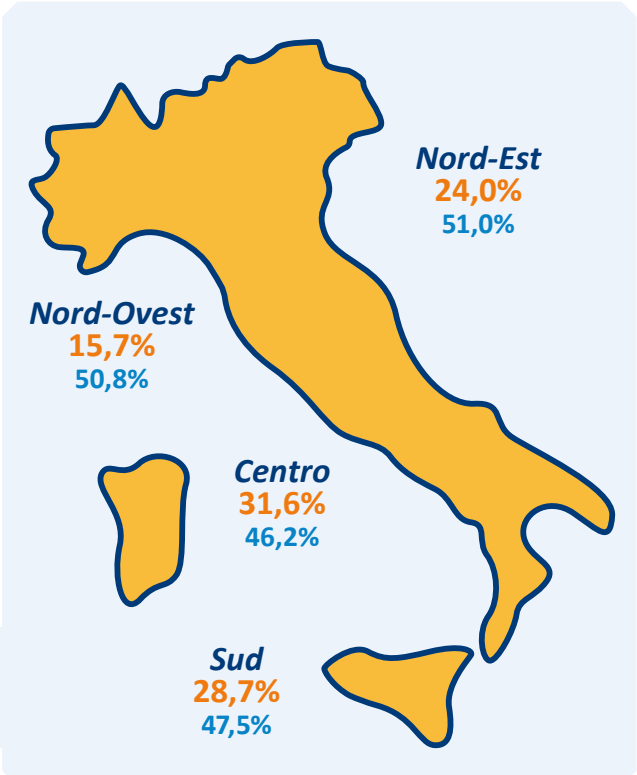
Facendo un focus sull'Italia, dove **il 48,4% degli utenti ha ricevuto almeno un alert** nel 2024, si rileva in particolare un **aumento degli alert** inviati relativamente a furto di dati monitorati **sul dark web**. Gli utenti allertati per dati rilevati sul **dark web sono l'88%** mentre solo il **12%** degli utenti sono stati allertati per dati rilevati sul **web pubblico**.

Vediamo di seguito 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 (26,0%) seguite dagli over 60 (25,8%), e dai 41-50 anni (25,3%). Gli uomini rappresentano la maggioranza degli utenti allertati (63,3%).

Le **regioni** in cui vengono allertate più persone sono Lazio (18,1%), Lombardia (14,0%), Sicilia (8,6%) e Campania (8,5%), ma in proporzione sono gli abitanti di Molise, Umbria, Emilia-Romagna, Piemonte e Valle d'Aosta che ricevono più alert.

Le **aree geografiche** in cui vengono allertate più persone sono il Centro (31,6%) e il Sud (28,7%), ma in proporzione sono gli abitanti del Nord-Ovest e del Nord-Est che ricevono più alert.



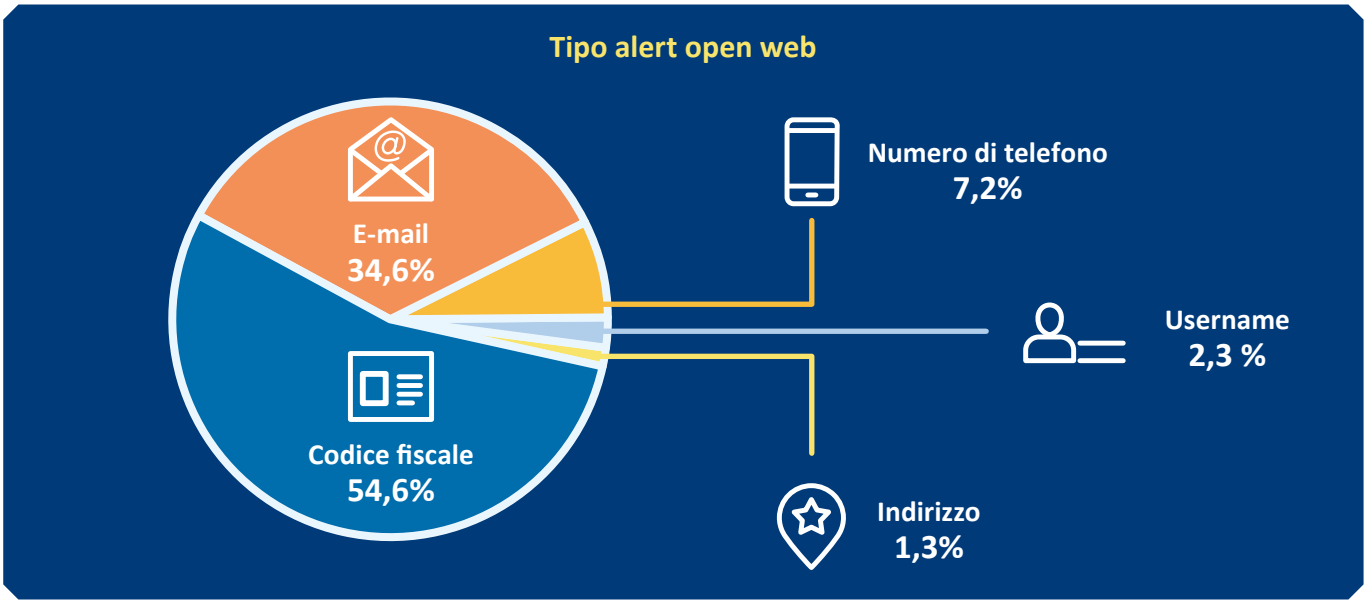
Area geografica
Distribuzione clienti allertati
Percentuale clienti allertati

Fonte: Osservatorio Cyber CRIF

2.2. Tipologia di dati rilevati di utenti italiani

Nel 2024, **i tipi di dati più frequentemente rilevati sull'open web**, quindi pubblicamente accessibili da chiunque sul web, sono stati il **codice fiscale** (54,6% dei dati rilevati) e l'**e-mail** (34,6%), seguiti a distanza da **numero di telefono** (7,2%), **username** (2,3%) e **indirizzo** (1,3%).

Nel dark web sono state invece le credenziali e-mail ad essere più frequentemente rilevate nel 2024, 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

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.

I consigli per protergersi dai furti d’identità online.

1. **Attivazione di aggiornamenti automatici per sistema operativo, applicazioni e browser:** in questo modo 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. 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 indirizzo e certificato di sicurezza, evitando di cliccare su link sospetti presenti in sms, messaggi whatsapp e e-mail. Evitare di fornire informazioni personali o finanziarie tramite messaggio o telefonata diretta.
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.

I consigli per proteggersi da phishing e smishing.

1. **Essere prudenti:** 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 in modo sospetto via e-mail o SMS, anche se sembrano provenire da un mittente conosciuto. Per accedere ai servizi online, digitare manualmente l'indirizzo web del sito ufficiale, o utilizzare l'app, sempre 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 a 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 che più del 63% della popolazione mondiale è presente su **social media** quali LinkedIn, Facebook, TikTok, Instagram e X, e che l'utente "tipico" vi trascorre più di 2 ore al giorno, **anche il phishing su queste piattaforme è in aumento** e quindi è bene non abbassare la guardia 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, è bene assicurarsi che ci sia la "spunta blu" sul profilo del brand che si segue.

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.

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 autorizzata da ESMA e riconosciuta come ECAI, fornisce 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 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.

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