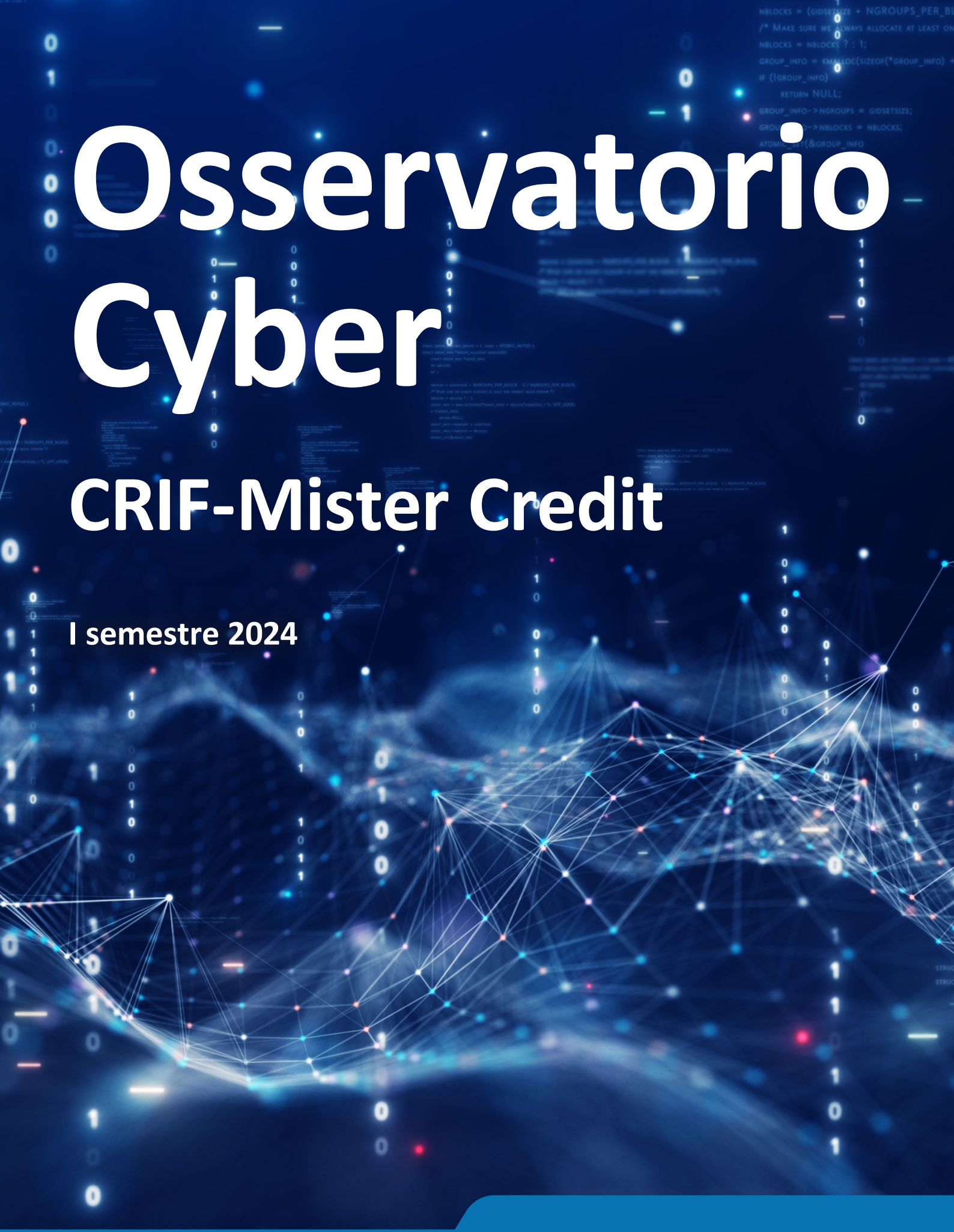
Osservatorio Cyber

CRIF-Mister Credit

I semestre 2024



CRIF
Together to the next level

Indice

Executive Summary

L'Osservatorio Cyber si propone di analizzare le vulnerabilità di individui e organizzazioni agli attacchi cyber, e interpretare i trend emergenti 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.
Attraverso un'analisi degli ambienti web in cui avviene l'esposizione e lo scambio dei dati personali, lo studio mostra le rischiosità a cui vengono esposti quotidianamente persone e aziende, e valuta i principali trend, fornendo indicazioni per mitigare il rischio cyber.

Il perimetro di analisi dell'Osservatorio Cyber include non solo il web pubblico, ma anche siti web, gruppi, forum e comunità specializzate del cosiddetto "Dark Web". Ma cosa intendiamo per dark web e come funziona? Il Dark Web è la parte nascosta di internet, accessibile solo tramite browser specifici o 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 primo semestre 2024, abbiamo rilevato l'esposizione di nuovi dati in circolazione sul dark web sempre più completi relativamente alle vittime e da poter utilizzare per mettere a segno frodi di vario tipo.

Di conseguenza, aumenta del 10% anche il numero degli **alert inviati relativi all'esposizione di dati sul dark web che è stato di 978.957 nel primo semestre 2024 rispetto al semestre precedente.** Questo dato ci mostra quanto sia diffuso il fenomeno e la difficoltà per gli utenti di difendersi da attacchi quali *phishing, smishing, vishing, spear phishing*, e anche l'emergente utilizzo di *exploit zero-click*, che permette di eseguire codice malevolo con un semplice SMS, senza che l'utente debba interagire in alcun modo con il messaggio.

Il numero degli **alert inviati relativi all'esposizione di dati sul web pubblico è stato di 23.500 nel primo semestre 2024,** ed è sceso del 34% rispetto al secondo semestre del 2023.
In totale, **nel primo semestre 2024, sono stati inviati oltre 1.002.457 alert**, in prevalenza relativi a dati trovati sul dark web.

La diminuzione della presenza di dati personali sul web pubblico è ormai un trend, determinato anche dal quadro normativo sulla privacy che ha imposto una maggiore regolamentazione mirata a fornire un maggiore controllo da parte dell'utente sull'esposizione dei propri dati personali.
Questo non deve portarci, tuttavia a un falso senso di sicurezza: la migrazione delle minacce verso il dark web richiede comunque una grande attenzione alla protezione dei dati.

In questo contesto, come si colloca l'Italia?

L'Italia non è certo immune da questa minaccia. Nel primo semestre del 2024, **il nostro Paese si è posizionato al 5° posto nella classifica mondiale per quanto riguarda il numero di indirizzi e-mail compromessi e messi in circolazione sul dark web.** Per quanto riguarda i dati delle carte di credito in circolazione, l'Italia si colloca al 18° posto nella classifica globale, un dato anche questo significativo. Infine, si posiziona al 41° posto per rilevamento di numeri di telefono che, come vedremo più diffusamente nello studio, giocano un ruolo importante in diverse tipologie di truffe online come lo smishing, che sempre più viene veicolato anche attraverso le app di messaggistica istantanea. Menzioniamo ad esempio la truffa legata ad allettanti proposte di lavoro, in cui le vittime vengono indotte a investire denaro o a fornire dati personali o bancari. Oppure la truffa denominata "mamma ho cambiato numero" con la quale i cybercriminali mirano sempre a ottenere un vantaggio economico, a discapito della vittima.

In conclusione, i dati raccolti 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 un contesto di questo tipo l'educazione relativa alle opportunità e ai rischi dei servizi digitali è fondamentale per aiutare i cittadini a difendersi. Da diversi anni CRIF porta avanti progetti per sensibilizzare e coinvolgere le persone su tematiche legate ai rischi cyber.

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

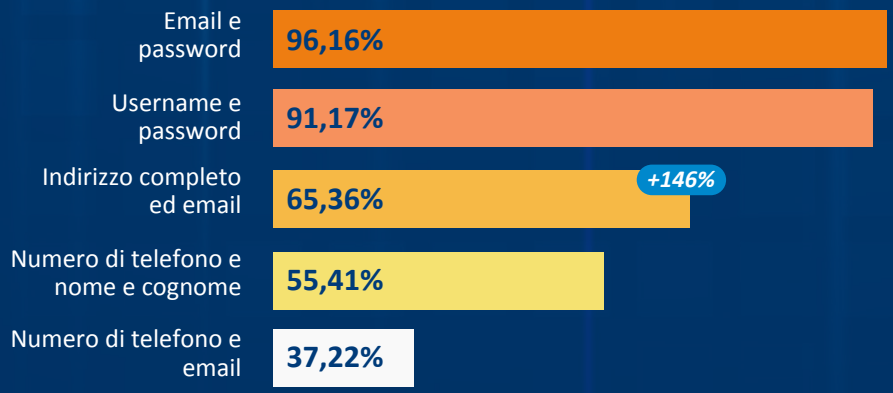
le più utilizzate:

123456
123456789
12345678

- Email personali e aziendali
- Nome e cognome
- Numero di telefono
- Username

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

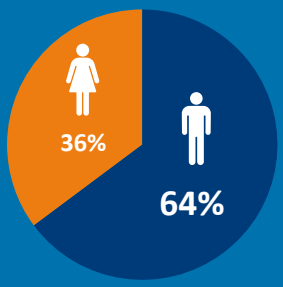
LE COMBINAZIONI DI DATI PIÙ ESPOSTE

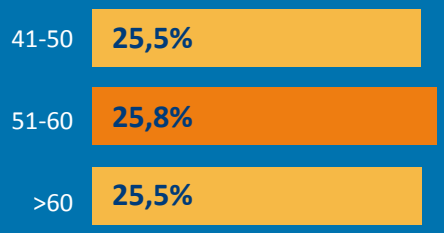


Preoccupa l'incremento registrato rispetto allo scorso semestre, +146%, relativo alla combinazione di **indirizzo completo più email**. Questo tipo di combinazione aumenta la vulnerabilità della vittima.

*Variazione I semestre 2024 vs II semestre 2023

IL PROFILO DEGLI UTENTI PIÙ COLPITI

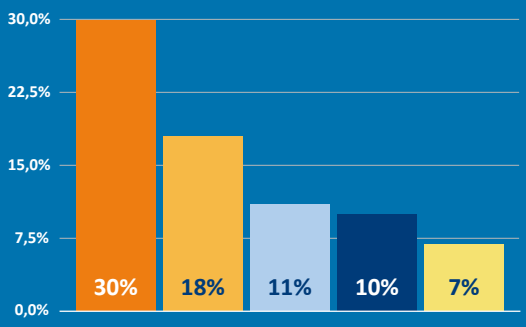




La fascia di età degli utenti maggiormente a rischio è quella dei **51-60**, seguita dai **41-50** a pari merito con gli **over 60**.

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.

Quali sono i dati più vulnerabili?

Il fenomeno cyber e le combinazioni di dati

Diverse sono le categorie dei dati che sono oggetto di attacco; abbiamo tuttavia osservato che sono l'indirizzo e-mail, la password, la username, il numero di telefono e il nome e cognome quelli che prevalentemente circolano sul dark web e pertanto sono più vulnerabili. Vengono trovati anche dati relativi all'indirizzo di residenza, documenti d'identità e identificativi personali.

TOP 10 DATI PIÙ VULNERABILI – I semestre 2024	
1	Password
2	E-mail
3	Username
4	Numero di telefono
5	Nome e Cognome
6	Indirizzo di residenza
7	Codici identificativi personali
8	Documento d'identità
9	Carta di credito
10	Passaporto

Fonte: Osservatorio Cyber CRIF

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.
Più informazioni si hanno sul soggetto, più l'attacco può essere mirato e credibile, e quindi i frodatori hanno più probabilità di successo.

Basti pensare che solamente con il numero di telefono si possono perpetrare diverse tipologie di phishing e truffe, ad esempio la truffa dell'"Accesso Eseguito", che si presenta come una notifica di accesso anomalo al proprio account – ad esempio quello dell'online banking – da un altro dispositivo. L'utente viene invitato a cliccare sul link per ripristinare l'accesso fornendo alcuni dati; l'obiettivo di questo attacco è ottenere le credenziali e altri dati personali per mettere a segno una frode. Ricordiamo che una banca non richiederebbe mai dati personali tramite messaggi, pertanto è opportuno non rispondere.

Le combinazioni di dati più esposte

Analizzando le combinazioni di dati più frequentemente esposte nel primo semestre del 2024, emerge un quadro chiaro delle informazioni più vulnerabili agli attacchi informatici.

La combinazione di e-mail e password risulta la più frequente, dove la password compare assieme alla mail nel 96,16% dei casi, mentre nel 91,17% dei casi è associata allo username.

Questi dati confermano come il **furto dell'account** continui a essere un obiettivo primario per gli hacker, sottolineando la necessità di adottare corrette pratiche di gestione password (es: una password diversa per ogni account, modifica frequente, password manager ecc.).

Un altro dato appetibile per i cyber criminali risulta essere l'**indirizzo di residenza completo**, associato alla **e-mail** nel 65,36% dei casi, e al **numero di telefono** nel 62,26% dei casi.

Le informazioni personali, combinate fra loro, vengono sfruttate per identificare gli individui e migliorare la precisione degli attacchi di ingegneria sociale, permettendoci di comprendere meglio le tipologie di frodi attuabili: i dati di contatto possono essere utilizzati, infatti, per perpetrare frodi mirate come lo spear phishing, una tipologia di phishing indirizzato a un bersaglio preciso, e proprio per questo più difficile da rilevare. Ricordiamo ad esempio gli attacchi BEC (Business e-mail compromise), o la truffa del CEO, in cui, con l'obiettivo di sottrarre denaro o dati sensibili, i cybercriminali inviano e-mail mirate ai dipendenti, spacciandosi per entità di fiducia come il CEO della propria azienda. Queste e-mail possono provocare gravi perdite finanziarie e compromettere la reputazione dell'azienda.

Infine, **particolarmente rilevante è la combinazione di numero di carta di credito, rilevata nel 41,79% dei casi, con i dati di sicurezza e la data di scadenza**. Sebbene questa casistica sia più bassa rispetto ad altre combinazioni, rimane estremamente preoccupante per il rischio di frodi finanziarie.

TOP COMBINAZIONI DI DATI	I SEMESTRE 2024	VARIAZIONE VS II SEM 2023
E-mail + password	96,16%	-1%
Username + password	91,17%	31%
Numero di telefono + nome-cognome	55,41%	59%
Numero di telefono + e-mail	37,22%	142%
Indirizzo completo + e-mail	65,36%	146%
Indirizzo completo + Numero di telefono	62,26%	-31%
Numero di carta di credito credito + dati di sicurezza e data di scadenza	41,79%	-58%

Fonte: Osservatorio Cyber CRIF

È interessante osservare come anche gli estremi dei documenti d'identità e di altri codici identificativi personali (es. il codice fiscale o Social security number) siano oggetto di attacco e di esposizione assieme ad altri dati, la cui conoscenza è necessaria per acquistare o richiedere servizi.

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.

La combinazione più frequente è quella di numero di documento associato al **numero di telefono** nell'81,17% dei casi, seguita dal numero di documento rilevato assieme a **nome e cognome** nel 74,68% dei casi.

Altre combinazioni significative includono il numero di documento ritrovato assieme a **telefono e data di nascita** nel 76,71% dei casi, e numero di documento rilevato con **nome e cognome**, e **data di nascita** nel 78,87%.

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.

Infine, la combinazione di numero di documento con **telefono ed e-mail** è meno comune, con un'incidenza del 14%. Benché meno frequente, questa combinazione rimane rilevante poiché può essere utilizzata per phishing e altre forme di attacco.

TOP COMBINAZIONI CON NUMERO DI DOCUMENTO D'IDENTITÀ	PERCENTUALE
Numero di documento + telefono	81,17%
Numero di documento + nome + cognome	74,68%
Numero di documento + telefono + data di nascita	76,71%
Numero di documento + nome e cognome + data di nascita	78,87%
Numero di documento + telefono + e-mail	14%

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 94,99% dei casi vengono ritrovati assieme a nome e cognome, nel 78,89% al telefono, nel 39,30% assieme a nome, cognome e data di nascita.

Invece, la combinazione personale (nome, cognome e indirizzo completo) è presente nel 35,11% dei casi.

Il numero identificativo personale è rilevato con **telefono ed e-mail nel 39,66% dei casi**, infine, la combinazione con indirizzo completo ed email è rilevata nel 57% dei casi.

Queste percentuali relative 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.

COMBINAZIONI CON NUMERO IDENTIFICATIVO PERSONALE	PERCENTUALE
Numero identificativo Personale + nome e cognome	94,99%
Numero identificativo Personale + telefono	78,89%
Numero identificativo Personale + nome e cognome + data di nascita	39,30%
Numero identificativo Personale + nome e cognome + passaporto	36,15%
Numero identificativo Personale + nome e cognome + indirizzo completo	35,11%
Numero identificativo Personale + telefono + e-mail	39,66%
Numero identificativo Personale + telefono + data di nascita	37%
Numero identificativo Personale + indirizzo completo + e-mail	57%

Fonte: Osservatorio Cyber CRIF

Account più frequentemente in circolazione sul Dark Web

Attraverso un'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, tra le altre tipologie di servizi abbiamo **al primo posto servizi di VPN** (Virtual Private Network), sistemi sempre più utilizzati globalmente anche da account privati che permettono di creare una connessione sicura e privata a Internet, anche quando si naviga su una rete pubblica o poco sicura. **Al secondo posto, account relativi ai più diffusi social network, mentre al quarto e quinto posto, si sottolinea il furto di account relativi a servizi finanziari** (come piattaforme di pagamento) **e account di siti di e-commerce.**

TIPOLOGIA DI ACCOUNT PIÙ RILEVATI	I SEMESTRE 2024
Servizi di VPN	30%
Social Network	18%
Siti internet	11%
Servizi finanziari	10%
Piattaforme e-commerce	7%
Education	6%
Gaming	5%
Dating	5%
Governmental	4%
Forum	1%

Fonte: Osservatorio Cyber CRIF

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 dire che un grande peso ha “il fattore umano”: la disattenzione dell’utente è una delle cause più comuni, così come password deboli o utilizzate per più account.

Account personali e aziendali

Attraverso un'analisi qualitativa dei domini degli account email esposti sul dark web, abbiamo rilevato se si riferiscono ad account personali o di business: nel 91,6% dei casi si tratta di account email personali, mentre nel restante 8,4% dei casi si tratta di account business, tendenza che rimane stabile nel tempo e che sembra confermare che, da un lato, gli utenti privati prestano ancora un’attenzione limitata alla sicurezza online, continuando così a essere un bersaglio primario per gli hacker, dall’altro lato, la stabilità in questo trend ci suggerisce che le aziende cercano di adottare misure di sicurezza per limitare la vulnerabilità dei propri dipendenti agli attacchi.

È essenziale non abbassare la guardia rispetto alle minacce informatiche al fine di proteggere i propri account.

Account email	I semestre 2024	II semestre 2023	Variazione percentuale
Personale	91,57%	91,53%	+0,05%
Business	8,43%	8,47%	-0,55%

Fonte: Osservatorio Cyber CRIF

1.1 Classifica delle password più trovate sul dark web

L'analisi delle password rilevate ci fa riflettere sulla vulnerabilità degli account a cui le stesse sono associate. Nella top 10 delle password in circolazione nel primo semestre 2024 troviamo quanto segue:

10 PASSWORD PIÙ UTILIZZATE SUL DARK WEB - I SEMESTRE 2024	
1	123456
2	123456789
3	12345678
4	password
5	12345
6	qwerty
7	1234567
8	111111
9	1234567890
10	qwertyuiop

Fonte: Osservatorio Cyber CRIF

L'analisi delle password più diffuse sul dark web nel primo semestre del 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. In cima alla classifica troviamo password come "123456", "password" e "qwerty", 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.

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", "123456789,", nomi propri come "francesco", "alessandro" e "giuseppe", e riferimenti allo sport come "juventus, e termini semplici come "cambiami", "amoremio "e "ciaociao".

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, ma anche attivare 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.

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

Come già analizzato, 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'email, a 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 Brasile, Giappone, Polonia e Canada.

Anche il dominio .edu, molto diffuso tra scuole, college e università, circola diffusamente sul dark web; questo significa che numerosi indirizzi e-mail di studenti e professori sono esposti al rischio cyber.

La tabella a seguire mostra la classifica dei domini più rilevati e i paesi maggiormente colpiti.

TOP 10 paesi più colpiti – I semestre 2024	
1	.COM .NET global and USA
2	.RU Russia
3	DE Germania
4	.FR Francia
5	.IT Italia
6	.UK Regno Unito
7	.BR Brasile
8	.JP Giappone
9	.PL Polonia
10	.CA Canada

Fonte: Osservatorio Cyber CRIF

1.3 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 (+107%) seguita dal Nord America. Al terzo posto troviamo l'Asia, in crescita del +61%.

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

CONTINENTE	I SEMESTRE 2024
Europa	44,2%
Nord America	27,3%
Asia	22,7%
Sud America	2,9%
Africa	2,1%
Oceania	0,7%

Data Source Provider: Cyber CRIF Observatory

La classifica dei paesi più soggetti a scambio di dati di carte di credito vede in testa la Federazione Russa, gli Stati Uniti, l'India, l'Iran e il Regno Unito.

L'Italia occupa il 18° posto della classifica globale; a seguire la Top 20.

Paesi più soggetti a scambio di dati di carte di credito – I semestre 2024			
1	RUSSIA	11	NIGERIA
2	STATI UNITI	12	CINA
3	INDIA	13	GIAPPONE
4	IRAN	14	AUSTRALIA
5	REGNO UNITO	15	GERMANIA
6	TAIWAN	16	MESSICO
7	BRASILE	17	UCRAINA
8	CANADA	18	ITALIA
9	FRANCIA	19	REPUBBLICA DI COREA
10	SPAGNA	20	ARGENTINA

Fonte: Osservatorio Cyber CRIF

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

TOP 3 AFRICA I SEMESTRE 2024	
1	Nigeria
2	Sud Africa
3	Egitto

TOP 3 AMERICA I SEMESTRE 2024	
1	USA
2	Canada
3	Messico

TOP 3 ASIA I SEMESTRE 2024	
1	India
2	Iran
3	Taiwan

TOP 3 OCEANIA I SEMESTRE 2024	
1	Australia
2	Nuova Zelanda
3	Guam

TOP 3 EUROPA I SEMESTRE 2024	
1	Regno Unito
2	Francia
3	Spagna

Fonte: Osservatorio Cyber CRIF

Focus Italia

Facendo un focus sull'Italia, dove il **36,8% degli utenti ha ricevuto almeno un alert nel primo semestre 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 il 90,7% mentre solo il 9,3% 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 (25,8%), seguite dai 41-50 anni (25,5%), a parimerito con gli over 60 (25,5%). Gli uomini rappresentano la maggioranza degli utenti allertati (64,0%).

Le regioni in cui vengono allertate più persone sono Lazio (18,7%), Lombardia (13,8%), Sicilia e Campania (entrambe 8,5%), ma in proporzione sono gli abitanti di Molise, Sicilia, Lombardia, Umbria e Valle d'Aosta che ricevono più alert.

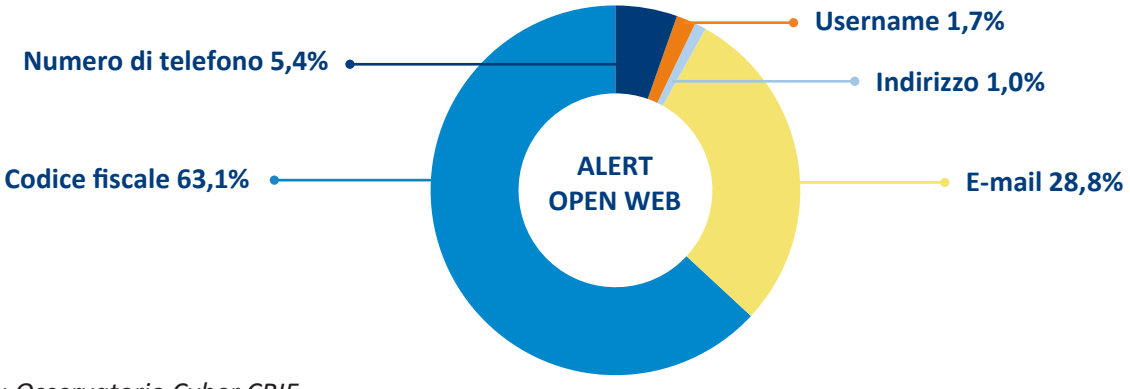
Le aree geografiche in cui vengono allertate più persone sono il Centro (32,4%) e il Nord (38,9% nel complesso), ma in proporzione sono gli abitanti del Nord-Ovest e del Nord-Est che ricevono più alert.

Area Geo	Distribuzione utenti allertati	Distribuzione utenti	Percentuale allertati su totale
Nord-Ovest	23,3%	22,1%	38,5%
Nord-Est	15,6%	15,0%	38,0%
Centro	32,4%	34,6%	34,3%
Sud	28,8%	28,3%	37,2%

Fonte: Osservatorio Cyber CRIF

2.1 Tipologia di dati rilevati di utenti italiani

Nel primo semestre 2024, i tipi di dati più frequentemente rilevati sull'open web, quindi pubblicamente accessibili da chiunque sul web, sono stati il codice fiscale (63,1% dei dati rilevati) e l'e-mail (28,8%), seguiti a distanza da numero di telefono (5,4%), username (1,7%) e indirizzo (1%).



Fonte: Osservatorio Cyber CRIF

Nel dark web sono state invece le credenziali e-mail a essere più frequentemente rilevate nel primo semestre 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*.

2.2 Come proteggersi da furti d'identità e truffe online?

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

1. **Attiva gli aggiornamenti automatici per sistema operativo, applicazioni e browser:** il tuo dispositivo sarà sempre protetto dalle ultime minacce e vulnerabilità che i criminali informatici potrebbero sfruttare.
2. **Effettua backup regolari su cloud o dispositivi esterni** e verifica periodicamente la loro integrità. In aggiunta, fai una copia dei tuoi documenti, almeno di quelli più importanti o più utilizzati, in modo che siano sempre recuperabili via internet.
3. **Proteggi i tuoi dispositivi:** pin, password, riconoscimento facciale, ma anche autenticazione a due fattori per un livello di sicurezza aggiuntivo. Inoltre, attiva il controllo remoto e la cancellazione dei dati in caso di smarrimento o furto.
4. **Fai attenzione a siti, mail e telefonate sospette:** verifica sempre l'autenticità dei siti controllandone la url e il certificato di sicurezza. Non cliccare su link sospetti presenti in sms, messaggi WhatsApp ed e-mail. Non fornire mai informazioni personali o finanziarie tramite messaggio o telefonata che te li richieda.
5. **Per una sicurezza completa**, utilizza servizi per controllare la circolazione dei tuoi dati personali e finanziari sul web e utilizza un antivirus ad ampia protezione sui tuoi dispositivi.

Considerando che la minaccia del phishing e dello smishing è in costante evoluzione, per proteggerti efficacemente, è fondamentale adottare un approccio proattivo:

- **Sii prudente:** diffida di qualsiasi comunicazione che via e-mail, SMS, chiamata o messaggio ti solleciti informazioni personali, password, telefono, codici di accesso, dati della carta di credito o informazioni finanziarie. Nessuna banca ti chiederà di fornire queste informazioni per telefono o via mail.
- **Verifica l'identità del mittente:** controlla attentamente l'indirizzo e-mail, il numero di telefono o l'URL del sito web. Cerca eventuali errori di ortografia, domini sospetti o indirizzi e-mail generici. Verifica sempre che l'URL inizi con "https://" e che sia presente il lucchetto nella barra degli indirizzi.
- **Non cliccare su link sospetti:** evita di cliccare su eventuali link che trovi su e-mail o SMS sospetti, anche se sembrano provenire da un mittente conosciuto. Digita manualmente l'indirizzo web del sito ufficiale per accedere ai tuoi servizi online, o usa l'app ufficiale.
- **Non scaricare allegati:** non aprire allegati provenienti da mittenti sconosciuti o sospetti, poiché potrebbero contenere malware.
- **Segnala l'accaduto:** se pensi di aver abboccato a una mail di phishing, e la mail sembrava provenire da un e-commerce o una banca, contattali tramite i loro canali ufficiali per segnalare l'accaduto così che possano mettere in atto misure di protezione nei tuoi confronti. Se opportuno, puoi segnalare il fatto anche alla Polizia Postale.

Infine, dal momento che più del 62% della popolazione mondiale è presente su social media, quali LinkedIn, Facebook, TikTok, Instagram e X, e che l'utente tipo vi trascorre più di 2 ore al giorno, anche su queste piattaforme è bene non abbassare la guardia (il phishing sui social network è purtroppo in aumento).

Vademecum sulla sicurezza cyber

- **Profili falsi:** attenzione agli impostori. 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:** diffida dalle short URL. Posiziona il mouse sul link per visualizzare l'indirizzo web completo.
- **Doppia autenticazione:** abilita l'autenticazione a due fattori (2FA) per i tuoi account social, così che non sia sufficiente avere la tua password per accedere al tuo profilo.

La value proposition di CRIF

Protezione dalle frodi e gestione del cyber risk

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. Inoltre, grazie alla **linea di servizi Mister Credit** dedicata a privati e piccole medie imprese, CRIF è partner di primarie banche e finanziarie per lo sviluppo dell'offerta di servizi a valore aggiunto per tutelare i clienti dalle frodi creditizie e proteggere l'identità online e offline.

Oltre 500.000 consumatori utilizzano oggi in Italia i servizi Mister Credit di CRIF per la protezione dal furto di identità. In particolare, **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 (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.

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?

- Ecosistema di dati unico in Italia, **CRIF Information Core**, con oltre 40 fonti informative.
- **35+ anni di esperienza** in Advanced Analytics e Process Automation nel settore finanziario.
- **Team globale di oltre 30 esperti AI**, impegnato da oltre 10 anni nello sviluppo di soluzioni basate sull'intelligenza artificiale.
- Piattaforme digitali avanzate in uso presso oltre **700 player nel mondo.**
- Profonda conoscenza dei **processi e normative** del settore finanziario.
- **Network di partner tecnologici e fintech** per offrire soluzioni sempre all'avanguardia.

CRIF
LinkedIn - CRIF Finance Italy
marketingfinanceitaly@crif.com

crif.it
mistercredit.it

Together to the next level