punto impresa digitale

CAMERA DI COMMERCIO
MONTE ROSA LAGHI
ALTO PIEMONTE

Eccellenze in Digitale

UNIONCAMERE

con il supporto di Google.org

mercoledì 20 marzo 2024

CYBERSECURITY IN PRATICA

strumenti e tecniche per riconoscere le minacce informatiche

PROGRAMMA DELL'INCONTRO

- Cybercrime S.p.A.: quando il crimine diventa business
- L'hacking cognitivo: come fregare l'essere umano
- Phishing e ransomware: i veicoli di attacco
- Le password: la chiave sotto lo zerbino
- Strumenti di lavoro e best practice generali
- Il Checkup Sicurezza IT del PID: casi reali della CCIAA

CYBERCRIME S.P.A.: QUANDO IL CRIME DIVENTA BUSINESS

Eccellenze in Digitale
UNIONCAMERE

punto impresa digitale

CAMERA DI COMMERCIO
MONTE ROSA LAGHI
ALTO PIEMONTE

pid@pno.camcom.it www.pno.camcom.it/digitale/pid/eccellenze-digitale

PERICOLI AZIENDALI

In un panorama digitale in continua evoluzione, la cybersecurity va oltre il semplice aspetto informatico.

Il fattore umano emerge come componente critica nella difesa dalle minacce digitali.
La cybersecurity non è solo una questione di codici e algoritmi, ma anche di comportamenti e decisioni quotidiane.

IL CYBERCRIME OGGI

💰 Più redditizio del traffico di droga

💸 Si stimano: 6 trilioni di $ nel 2021, 8 trilioni nel 2023, più di 10 nel 2025

🏭 Possiedono aree aziendali: marketing, finanza, ricerca e sviluppo, ICT, etc.

🕵️ Difficile individuazione, potendo attaccare da ogni parte del mondo

IL CYBERCRIME IN ITALIA E NEL MONDO

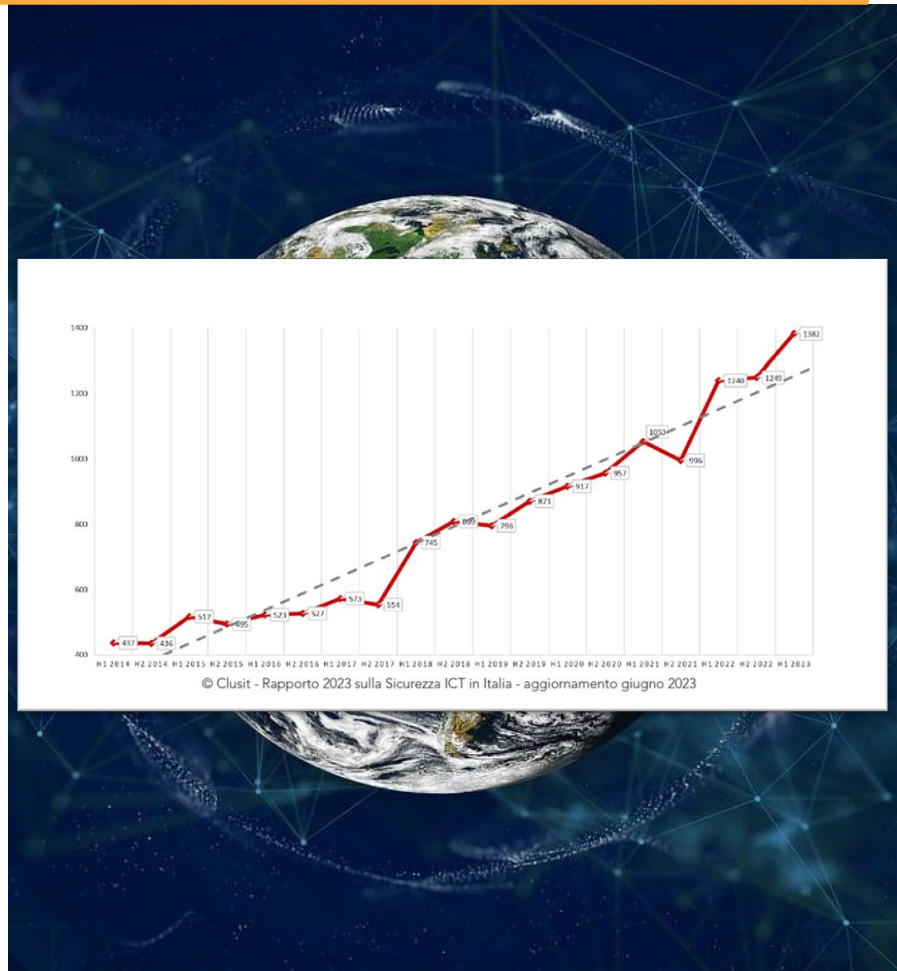
⚠️ 79% degli attacchi ICT nel 2023 è stato classificato “a impatto elevato” (il rimanente a medio impatto: sparisce l’impatto basso)

🥇 Italia 3° al mondo (1° in UE) come vittima di malware e superiore alla media mondiale (14% vs 9%) come vittima di phishing

👎 26° posto (terz’ultima) in EU per competenze digitali almeno di base

📉 Nel 2020, 4 italiani su 10 ha pagato il riscatto (dati ritornati nel 50%, ripristinati nel 50%)

📈 Attacchi hacker in Italia nel 2023 cresciuti del +40% rispetto al 2022 (4 volte superiore rispetto al resto del Mondo)

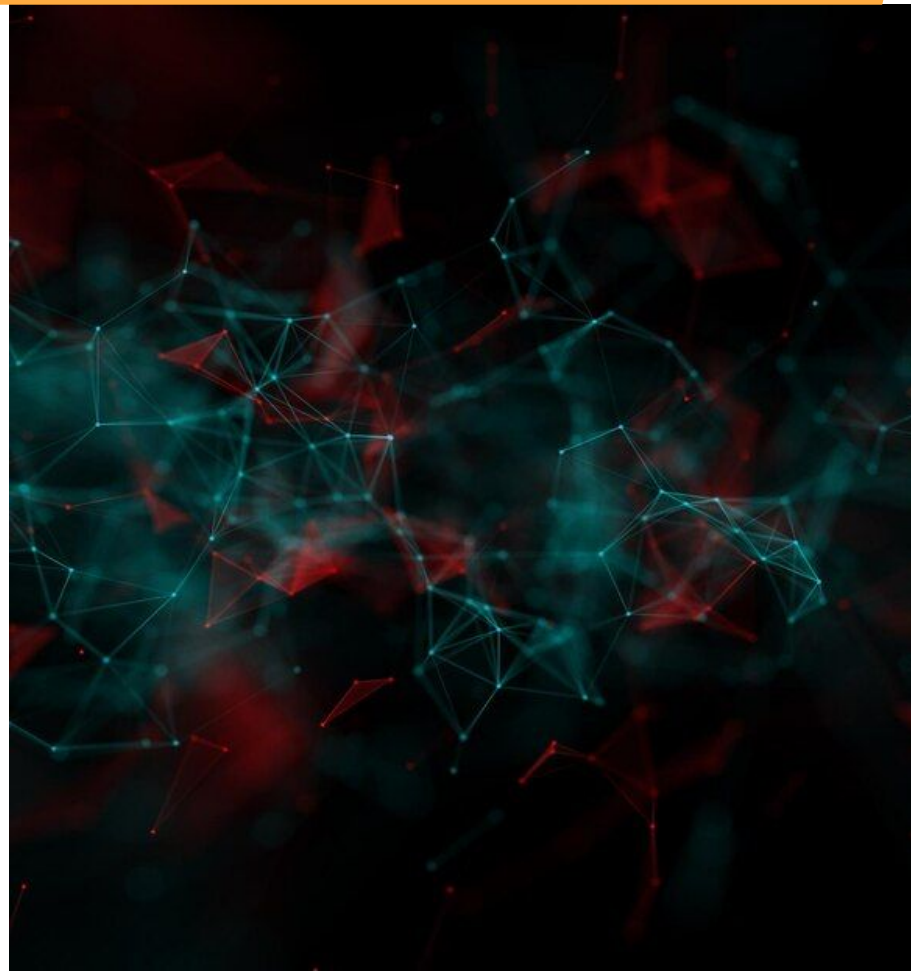


DOVE FINISCONO I DATI RUBATI?

Usati per ricattare!
Tuttavia, non c’è mai garanzia di restituzione, oltre alla possibilità di subire un doppio ricatto, soprattutto se percepiti come “utenti paganti”.

DOVE FINISCONO I DATI RUBATI?

Messi in vendita nel Dark Web, sicché altri attaccanti possano comprarli e usarli contro di voi.



L’HACKING COGNITIVO: COME FREGARE L’ESSERE UMANO

L'INGEGNERIA SOCIALE

Ingegneria sociale (o "hacking cognitivo"):
insieme di strategie di attacco
che sfruttano la manipolazione delle persone
per rivelare informazioni sensibili
(o, in altre parole, "fregare il prossimo con la psicologia").

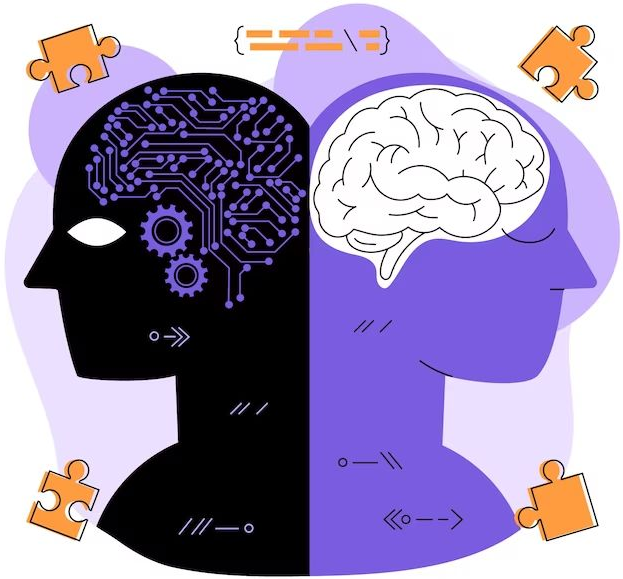
MA QUALI ASPETTI VENGONO SFRUTTATI?

LE EMOZIONI UMANE

Rabbia, sensi di colpa, paura, panico, eccitazione, etc.

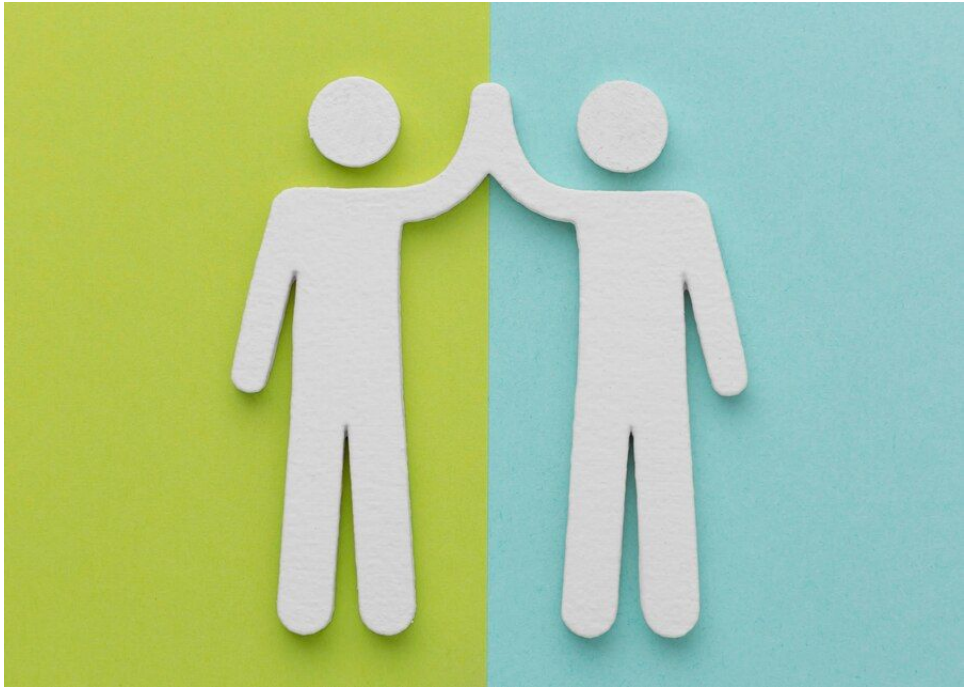
I BIAS COGNITIVI

Avversione alla perdita, urgenza, autorità, etc.



I RAPPORTI PERSONALI

Persuasione, reciprocità, dovere sociale, fiducia verso il prossimo, etc.

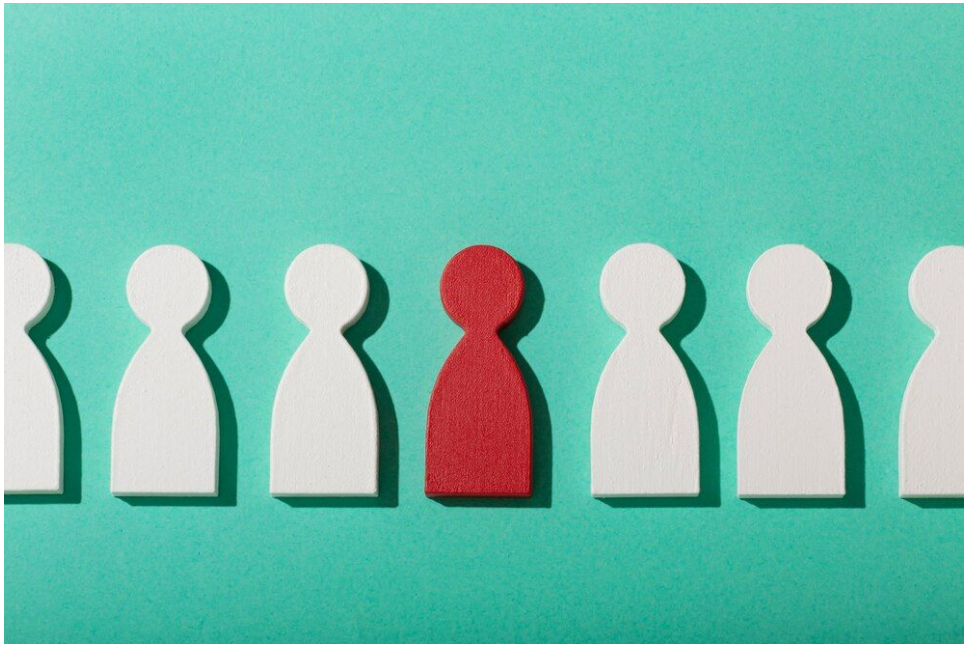


ATTEGGIAMENTI ERRATI

Mancato rispetto delle policy, abitudini, etc.

CARATTERISTICHE E ATTEGGIAMENTI INDIVIDUALI

Curiosità, conformità al gruppo, effetto spettatore, etc.



COMPETENZE

Funzionamenti, linguaggio tecnico, etc.

BORNOUT

Routine, decisionale, da autenticazione, dell’operatore, da allerta, etc.

FALSE CREDENZE DELLE IMPRESE

«Mica vengono a colpire me! Siamo una piccola impresa!»

«Non ho nulla di importante o interessante per loro!»

«Mica è mai successo niente fino ad ora!»

E LE TRUFFE? LE POSSIAMO EVITARE?

www.NewsBIELLA.it
QUOTIDIANO ONLINE GRATUITO di BIELLA e del biellese
BIELLA CITTÀ CREATIVA UNESCO

CRONACA | 26 gennaio 2024, 11:20

"Il figlio è in difficoltà, deve fare bonifico di 3mila euro": ma è una truffa. A sventarla l'impiegata di banca

La dipendente della banca, moglie di un Carabiniere e ben informata delle diverse modalità di truffe che avvengono ogni giorno, ha chiesto ulteriori informazioni e, dopo aver verificato che il conto corrente (su cui doveva avvenire il versamento) era straniero, ha consigliato alla pensionata di mettersi in contatto con il figlio telefonicamente per capire se il messaggio fosse autentico.

Alla fine, il figlio ha risposto tranquillamente alla chiamata del genitore e ha confermato che non ci fosse alcun tipo di problema. Era, purtroppo, una truffa, raccolta dai Carabinieri al momento della presentazione della denuncia. Si consiglia, sempre, di fare massima attenzione.

il Biellese

Fa un bonifico di 3mila euro per il figlio. Era una truffa

I carabinieri invitano alla massima attenzione. Solo la scorsa settimana un altro caso era stato sventato grazie all'intervento di un'impiegata di banca

Sulla nota chat di messaggistica, il 75enne, aveva ricevuto un messaggio da un uno sconosciuto. Chi scriveva diceva di essere il figlio e che aveva avuto un problema. Gli si era guastato il telefono e quindi si era fatto prestare un apparecchio da un conoscente. Ma se fosse stato solo quello il problema... Ahimè, si trovava molto in imbarazzo, ma doveva saldare un debito d 3 mila euro, e anche in fretta.

Il pensionato, abile nella gestione dei suo affari attraverso i servizi bancari online, non ci ha pensato due volte e ha subito disposto il versamento della cifra richiesta facendola accreditare sul conto corrente indicato da chi si spacciava per essere suo figlio.

Solo dopo, a versamento fatto, si è interrogato se chi gli aveva scritto fosse realmente chi diceva di essere. Provando a mettersi in contatto con il figlio, sul suo tradizionale numero, ha così scoperto che era stato beffato. Il passo successiva è stato quello di contattare i carabinieri e sporgere denuncia.

PHISHING E RANSOMWARE: I VEICOLI DI ATTACCO

IL PHISHING

Richiama il termine «fishing», «pesca», perché si tende a gettare l'amo nel mucchio

IL PHISHING

Richiama il termine «fishing», «pesca», perché si tende a gettare l'amo nel mucchio

1% minimo "abbocca"

IL PHISHING

Si esplica:

📧 Nelle e-mail (Phishing)

✉️ Negli SMS (Smishing)

📞 Nei chiamate (Vishing)

📱 Nei QR Code (Qrishing)

🛜 Nei Wi-Fi (Wiphishing)

Possono essere combinate tra loro!

CRONACHE

A- A+

Sabato, 10 febbraio 2024

"Il suo conto corrente è sotto attacco", 80enne perde 240 mila euro con un sms

Dopo aver ricevuto il messaggio, la vittima è stata contattata da un individuo che si è spacciato per un operatore del servizio antifrode della sua banca

Di Redazione Cronache

IL PHISHING

Si esplica nei click sui link o download di allegati (non nella sola apertura dell'e-mail o dell'SMS).

LO SPOOFING

Significa assumere l’identità di qualcun altro.

IL NAME-DROPPING

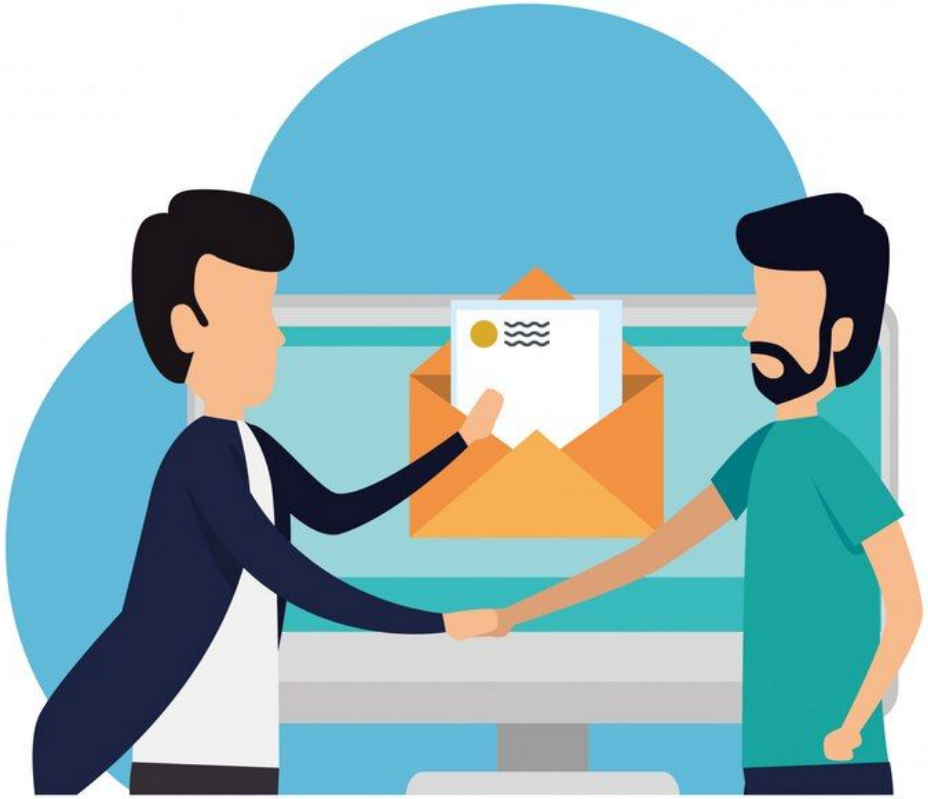
Citare un nome noto per acquisire credibilità:

👥 Noto “a tutti”.

👤 Noto “alla persona”.

LA BUSINESS E-MAIL COMPROMISE (BEC)

Sofisticata forma di attacco in cui gli aggressori manipolano le comunicazioni aziendali per ottenere benefici finanziari o accedere a informazioni sensibili, spesso impersonando figure di autorità o partner commerciali.



BEC: THE MAN IN THE MIDDLE

Vengono intercettate delle conversazioni via e-mail, per dirottare pagamenti o indurre in altre azioni.

ESEMPIO DI “THE MAN IN THE MIDDLE”

Un dirigente di Confindustria si è fatto truffare da una email falsa

Gianfranco Dell'Alba ha versato su un conto sconosciuto circa 500mila euro credendo di seguire le indicazioni di una collega

Oggi su *Repubblica* c’è un articolo su una inusuale truffa subita da Confindustria: un suo dirigente ha versato circa 500mila euro che appartenevano all’associazione degli industriali su un conto sconosciuto, seguendo le indicazioni di una email falsa. Il dirigente, Gianfranco Dell’Alba, credeva che l’email fosse stata scritta dalla direttrice generale di Confindustria Marcella Panucci, perché era dal suo indirizzo che gli era arrivata. Dell’Alba, che era il capo della delegazione di Confindustria a Bruxelles, è stato poi licenziato dall’associazione.

BEC: CEO FRAUD

Avviene grazie alla violazione della casella di un alto dirigente, con la cui identità viene richiesto ai dipendenti di compiere determinate azioni, come effettuare pagamenti anche molto cospicui.

ESEMPIO DI “CEO FRAUD”

Storia di un furto telematico da tre milioni di dollari

Colpo grosso via Internet ai danni della Mattel: l’anno scorso tre milioni di dollari hanno preso il volo per via di una singola mail truffaldina.

La mail interna aziendale proveniva dal nuovo direttore generale della Mattel e ordinava il pagamento di questa cifra a un nuovo fornitore in Cina. L’ordine arrivava poco dopo un ricambio del personale a vari livelli, per cui la manager finanziaria che l’ha ricevuto era ansiosa di dimostrare la propria solerzia e diligenza. Così ha verificato la conformità dell’ordine ai protocolli di sicurezza, che esigevano che i trasferimenti di denaro avessero l’approvazione di due manager di alto livello. Lei aveva questa qualifica, e l'aveva anche il direttore generale, per cui il bonifico da tre milioni di dollari è partito subito alla volta di un conto presso la Bank of Wenzhou, in Cina.

Qualche ora dopo la manager ha accennato al pagamento durante una conversazione con il direttore generale, che però ha negato di aver dato un ordine del genere. Panico: è partita subito una serie di chiamate alla banca che doveva inviare il bonifico, alla polizia e all’FBI. Ma la risposta è stata inesorabile: troppo tardi, i soldi sono già in Cina.

BEC: BUSINESS CONTACTS THROUGH COMPROMISED EMAIL

Simile alla CEO Fraud, con la differenza che la casella violata è quella di un dipendente e la richiesta viene inoltrata a più fornitori.

BEC: DATA THEFT

Simile alla CEO Fraud e alla Business Contacts Through Compromised e-Mail, qui la richiesta avviene da un finto dirigente verso dipendenti in possesso di dati importanti.

BEC: BUSINESS EXECUTIVE AND ATTORNEY IMPERSONATION

I truffatori si fingono legali o avvocati che devono trattare questioni urgenti.

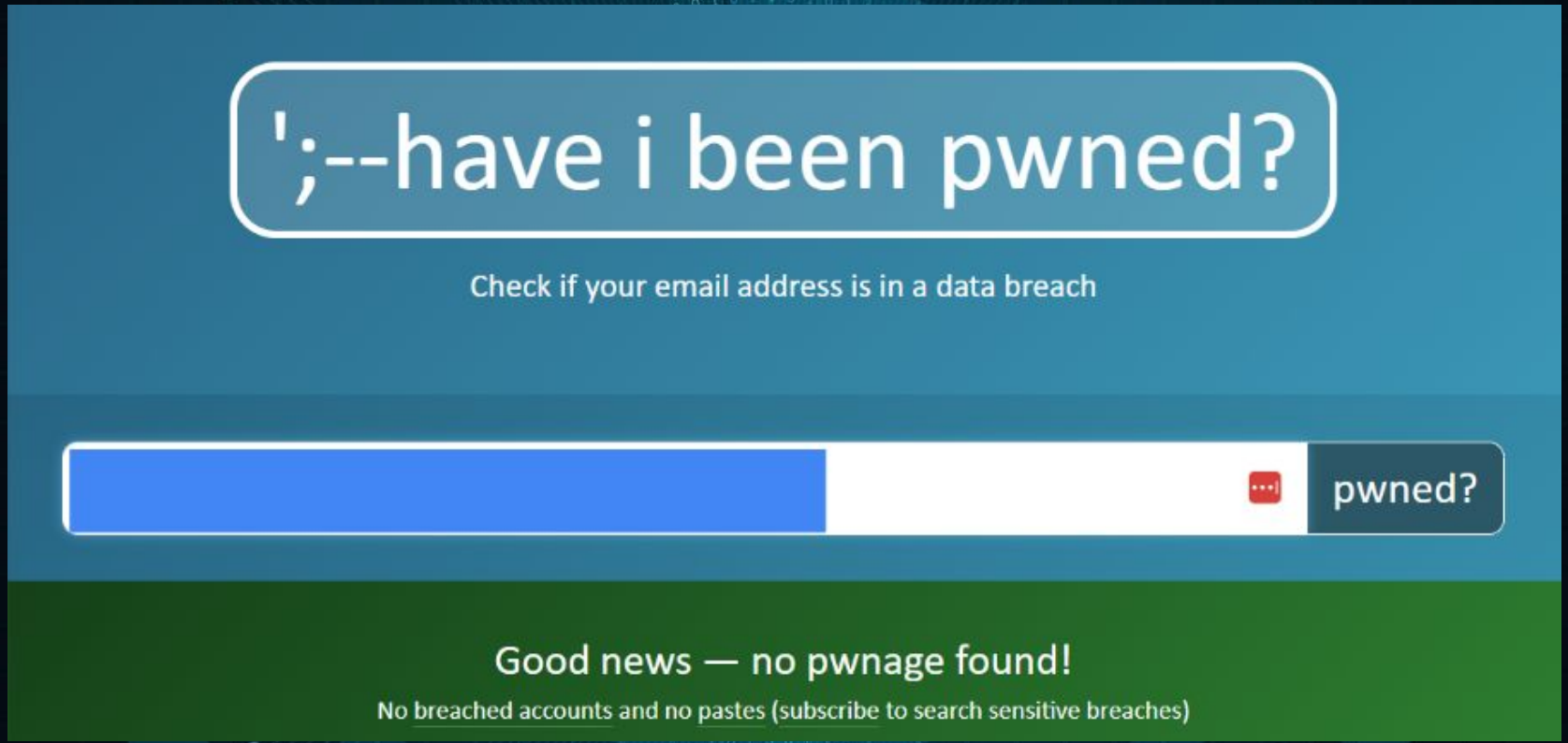
TOCCA A VOI!

ANDATE SUL SITO

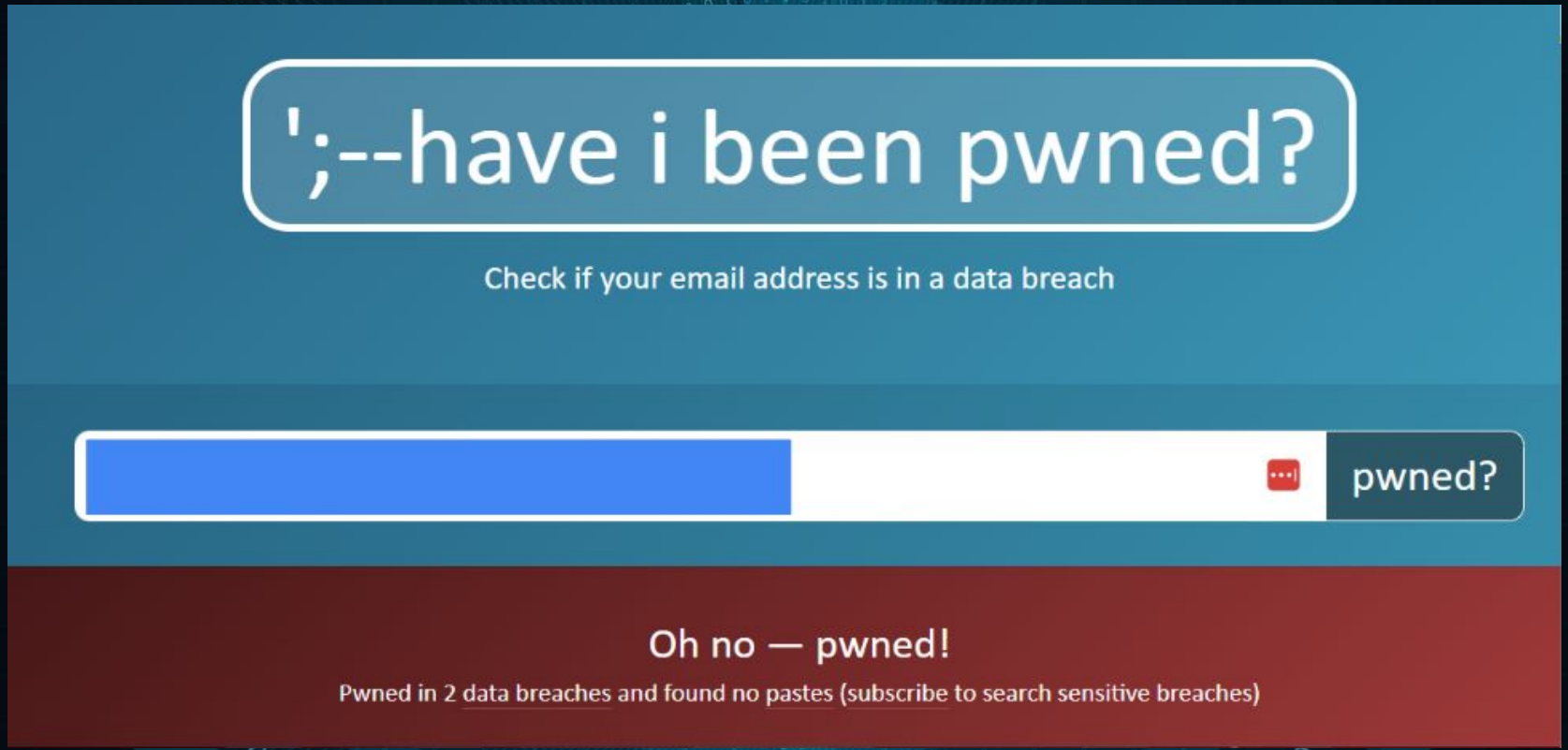
https://haveibeenpwned.com/

O SCANSIONATE IL QR CODE E INSERITE LA VOSTRA E-MAIL PERSONALE O DI LAVORO (OPPURE PRIMA UNA E POI L'ALTRA)

TOCCA A VOI!


';--have i been pwned?
Check if your email address is in a data breach
pwned?
Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)

TOCCA A VOI!


';--have i been pwned?
Check if your email address is in a data breach
pwned?
Oh no — pwned!
Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

TOCCA A VOI!

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

houzz

Houzz: In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames

TOCCA A VOI!

Houzz : A metà del 2018, il sito web di progettazione abitativa Houzz ha subito una violazione dei dati . L'azienda venne a conoscenza dell'incidente più tardi quell'anno e lo rivelò ai membri interessati nel febbraio 2019. Quasi 49 milioni di indirizzi e-mail univoci erano coinvolti nella violazione insieme a nomi, indirizzi IP, posizioni geografiche e hash salati di password o collegamenti ai profili di social media utilizzati per autenticarsi al servizio. I dati sono stati forniti a HIBP da dehashed.com .

Dati compromessi: indirizzi e-mail, posizioni geografiche, indirizzi IP, nomi, password, profili di social media, nomi utente

MyFitnessPal : nel febbraio 2018, il servizio di dieta ed esercizio fisico MyFitnessPal ha subito una violazione dei dati . L'incidente ha messo in luce 144 milioni di indirizzi e-mail univoci insieme a nomi utente, indirizzi IP e password archiviati come hash SHA-1 e bcrypt (i primi per gli account precedenti, le seconde per gli account più recenti). Nel 2019, i dati sono apparsi in vendita su un mercato del dark web (insieme a numerose altre grandi violazioni) e successivamente hanno iniziato a circolare in modo più ampio. I dati sono stati forniti all'HIBP da una fonte che ha richiesto che venissero attribuiti a "BenjaminBlue@exploit.im".

Dati compromessi: indirizzi email, indirizzi IP, password, nomi utente

COSA FARE SE È ROSSA?

1) Cambiare la password sui siti compromessi

COSA FARE SE È ROSSA?

1) Cambiare la password sui siti compromessi
2) Cambiare la password della e-mail

COSA FARE SE È ROSSA?

1) Cambiare la password sui siti compromessi
2) Cambiare la password della e-mail
3) Se la password utilizzata è usata (uguale o simile) su altri siti, bisogna cambiarla su ogni sito in cui è usata

USARE LA STESSA PASSWORD

TECHCOMPANY360

Zuckerberg hackerato su Twitter e l'importanza dell'autenticazione a due fattori

Home > Tech Lab

Il re dei social network utilizzava "dadada" come password per accedere a LinkedIn, rete hackerata nel 2012

Paolo Longo

Pubblicato il 08 Giu 2016

TROVATE TUTTI GLI ELEMENTI CHE POTREBBERO FAR SOSPETTARE CHE L'E-MAIL SIA UNA TRUFFA

TOCCA A VOI!

Mittente: comunicazione@studiorossi.it

Oggetto: Verifica Dati Account Urgente

Ciao Utente,

Siamo spiacenti per l'inconveniente, ma il nostro sistema ha rilevato un'attività sospetta sul suo account aziendale. Per garantire la sicurezza delle sue informazioni, è necessario verificare i suoi dati aziendali al più presto possibile.

Faccia clic sul seguente link per accedere alla nostra pagina di verifica e aggiornare le informazioni richieste:

https://bit.ly/3UMotMg

Grazie per la collaborazione. Cordiali saluti,

Assistenza Clienti

TOCCA A VOI!

Mittente: assistenza@studiorossi.it

Oggetto: Verifica Dati Account Urgente

Ciao Utente,

Siamo spiacenti per l'inconveniente, ma il nostro sistema ha rilevato un'attività sospetta sul suo account aziendale. Per garantire la sicurezza delle sue informazioni, è necessario verificare i suoi dati aziendali al più presto possibile.

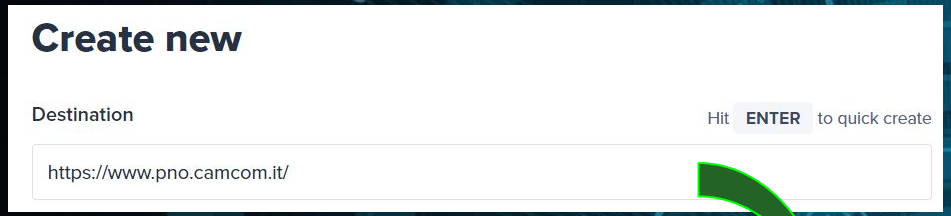
Faccia clic sul seguente link per accedere alla nostra pagina di verifica e aggiornare le informazioni richieste:

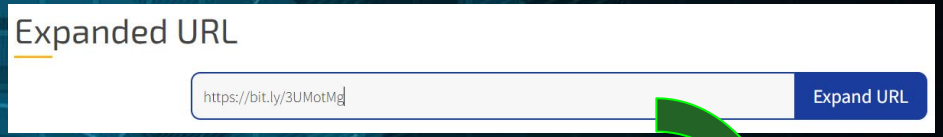
https://bit.ly/3UMotMg

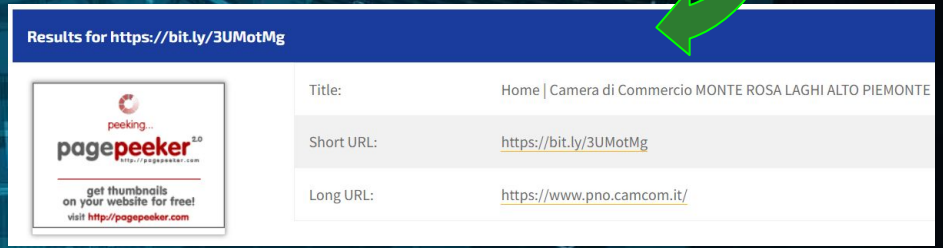
Grazie per la collaborazione. Cordiali saluti,

Assistenza Clienti

ACCORCIARE LINK E FARLI ESPLODERE







TOCCA A VOI!

Mittente: assistenza@studiorossi.lt

Oggetto: Conferma Dati Fatturazione

Gentile Marco,

Siamo spiacenti per l'inconveniente, ma abbiamo riscontrato un problema con i tuoi dati di fatturazione. Per evitare interruzioni nei servizi, la preghiamo di confermare immediatamente i dettagli del tuo account utilizzando il link qui sotto:

www.conferma-fatturazione.com

Grazie per la collaborazione. Cordiali saluti,

Team Amministrativo

TOCCA A VOI!

Mittente: assistenza@studiorossi.lt

Oggetto: Conferma Dati Fatturazione

Gentile Marco,

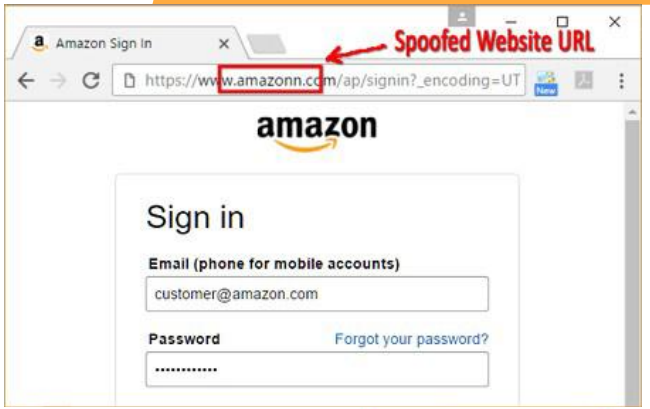
Siamo spiacenti per l'inconveniente, ma abbiamo riscontrato un problema con i tuoi dati di fatturazione. Per evitare interruzioni nei servizi, la preghiamo di confermare immediatamente i dettagli del tuo account utilizzando il link qui sotto:

www.conferma-fatturazione.com

Grazie per la collaborazione. Cordiali saluti,

Team Amministrativo

ESEMPI DI PHISHING



Da: ADMIN-ICT-Sapienza Università di Roma <tammykee0147@gmail.com>
Date: mer 9 set 2020, 19:18
Subject: Webmail@uniroma1.it
To:

Hai superato il numero massimo di contenuti della tua casella di posta

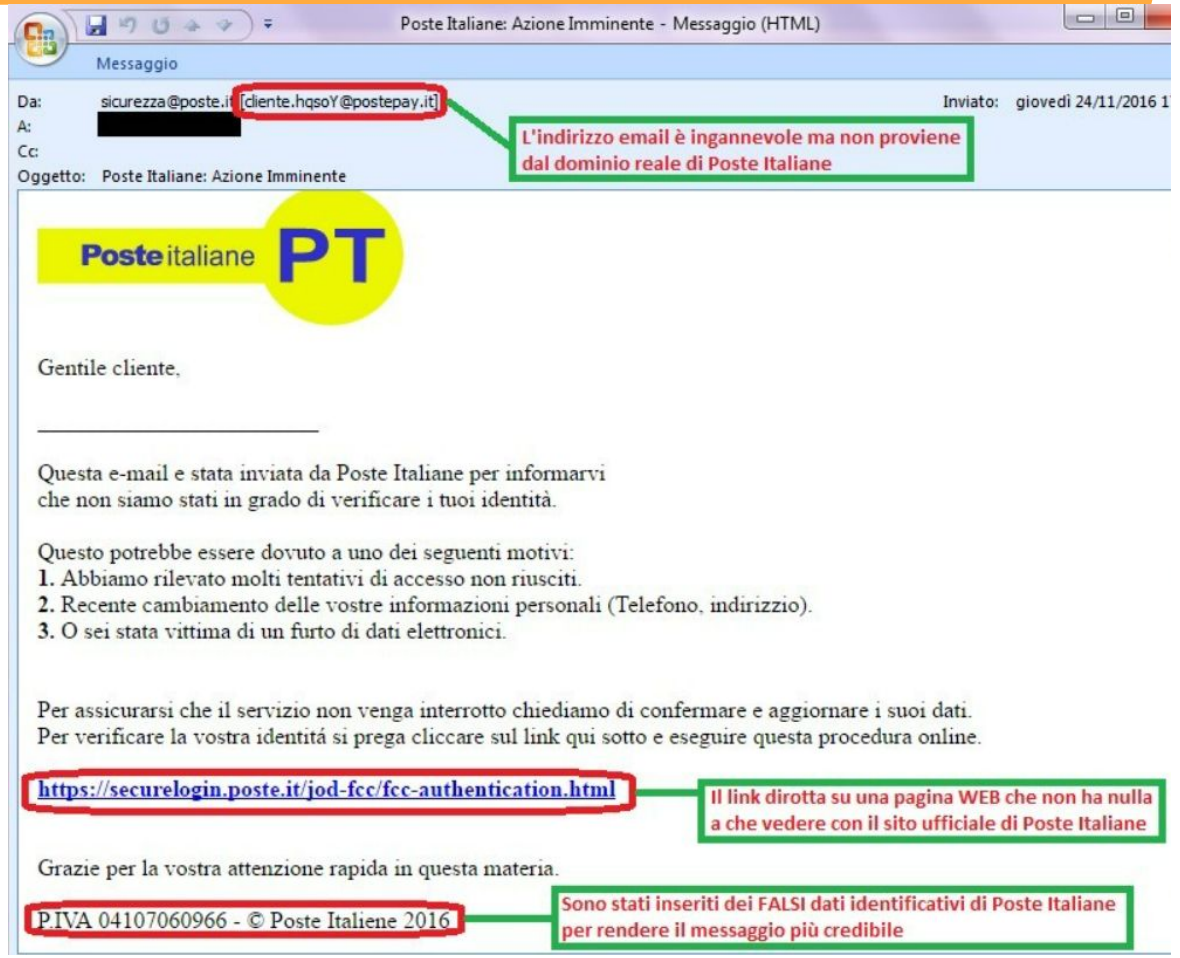
Trasferiremo tutti gli account di posta elettronica a Outlook Web

2020 e come tale deve essere confermato da tutti i titolari di conto attivi e accedi affinché gli aggiornamenti e i trasferimenti abbiano effetto immediato.

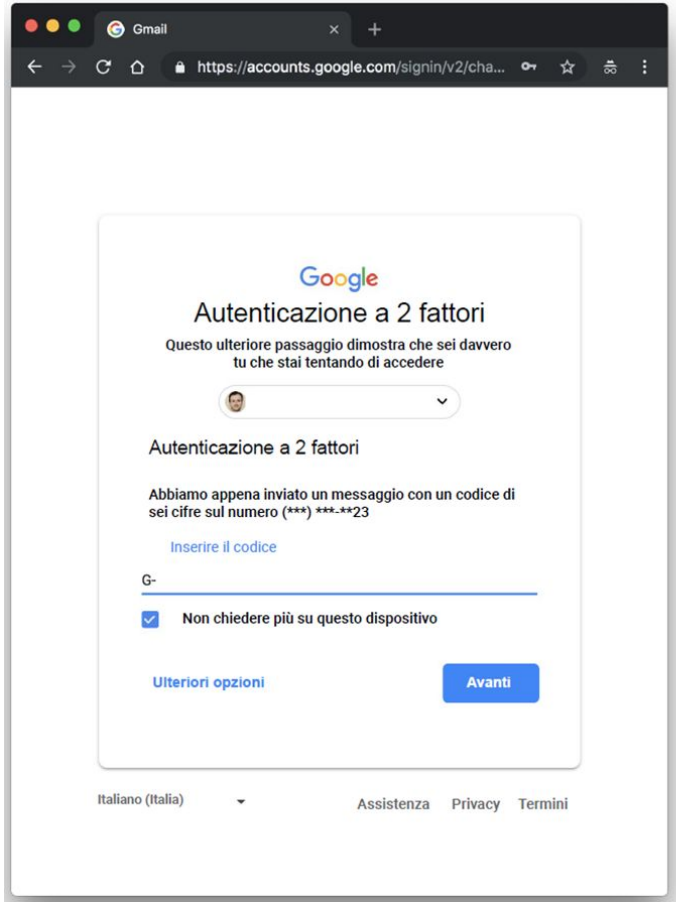
Questo viene fatto al fine di aumentare la sicurezza e l'efficienza grazie a recenti eventi mondiali covid-19 e ti consigliamo agire e aiutarci ad aggiornare il nostro server. Servire Immettere i dettagli di seguito:

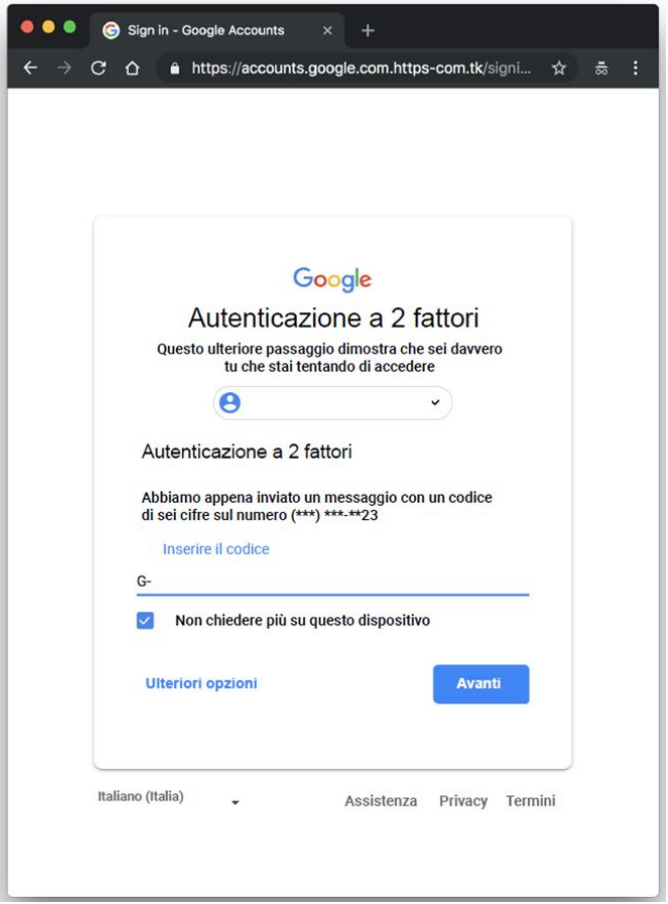
Nome e cognome:
E-mail identificativo utente:
Password email:
Data di nascita:

Attenzione: se non lo fai, il tuo account verrà disattivato entro 72 ore.

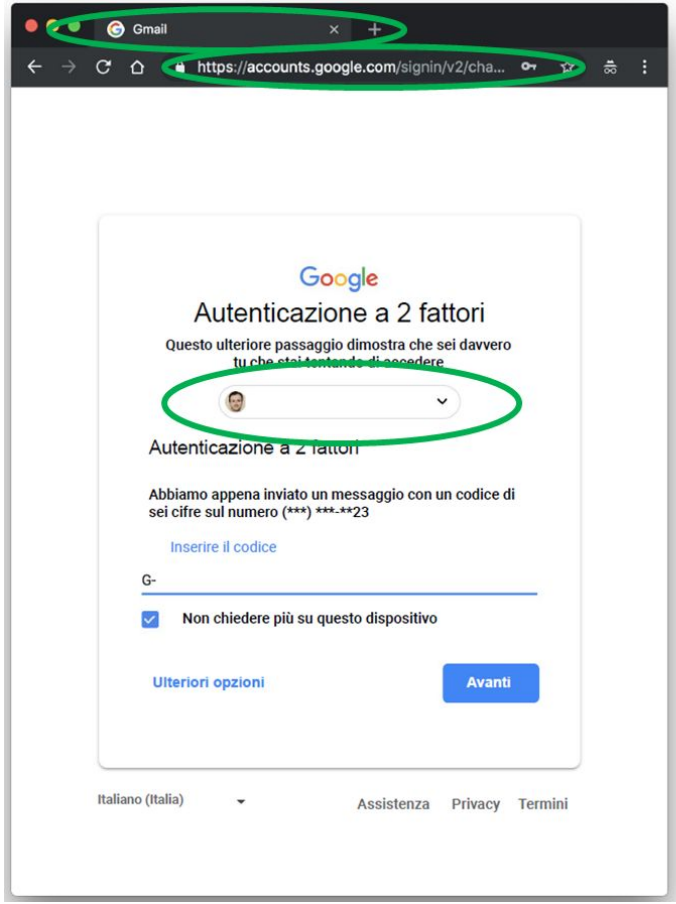


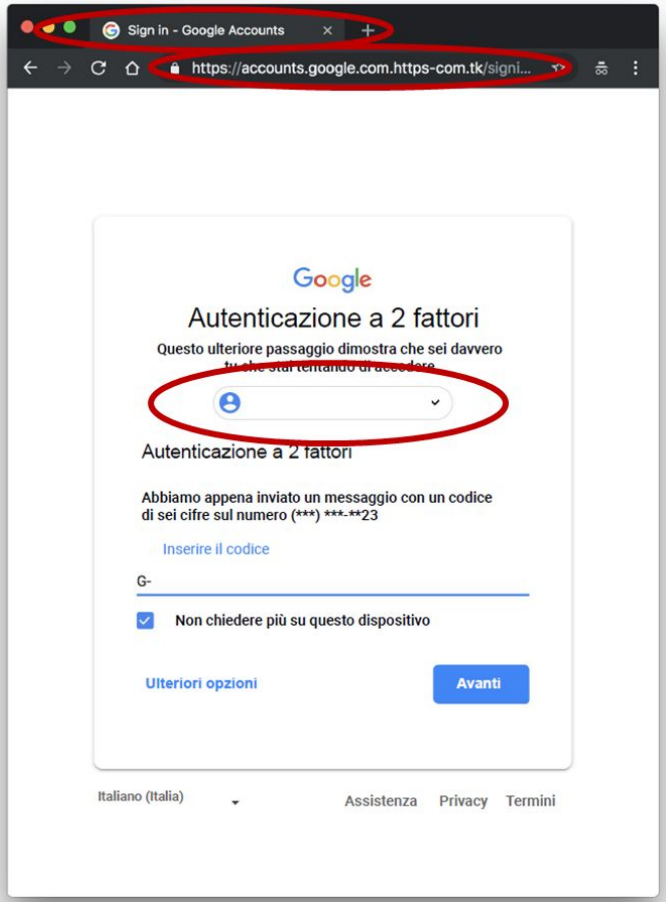
ESEMPI DI PHISHING





ESEMPI DI PHISHING





PHISHING: CASO STUDIO DALLA CAMERA DI COMMERCIO

si segnala che in questi giorni è stata rilevata una campagna malevola che propone un **falso aggiornamento del software Dike** al fine di installare un software di controllo remoto.
L'e-mail, scritta in italiano corretto, presenta un PDF allegato e riporta come oggetto"**Aggiornamento critico Dike**" e mittente **INFOCERT S.p.A.** comunicazioni@infocert.it.

All'interno del PDF un link rimanda al download di un file di installazione che, se avviato, installa un software di controllo remoto dando agli attaccanti l'accesso alla macchina della vittima.

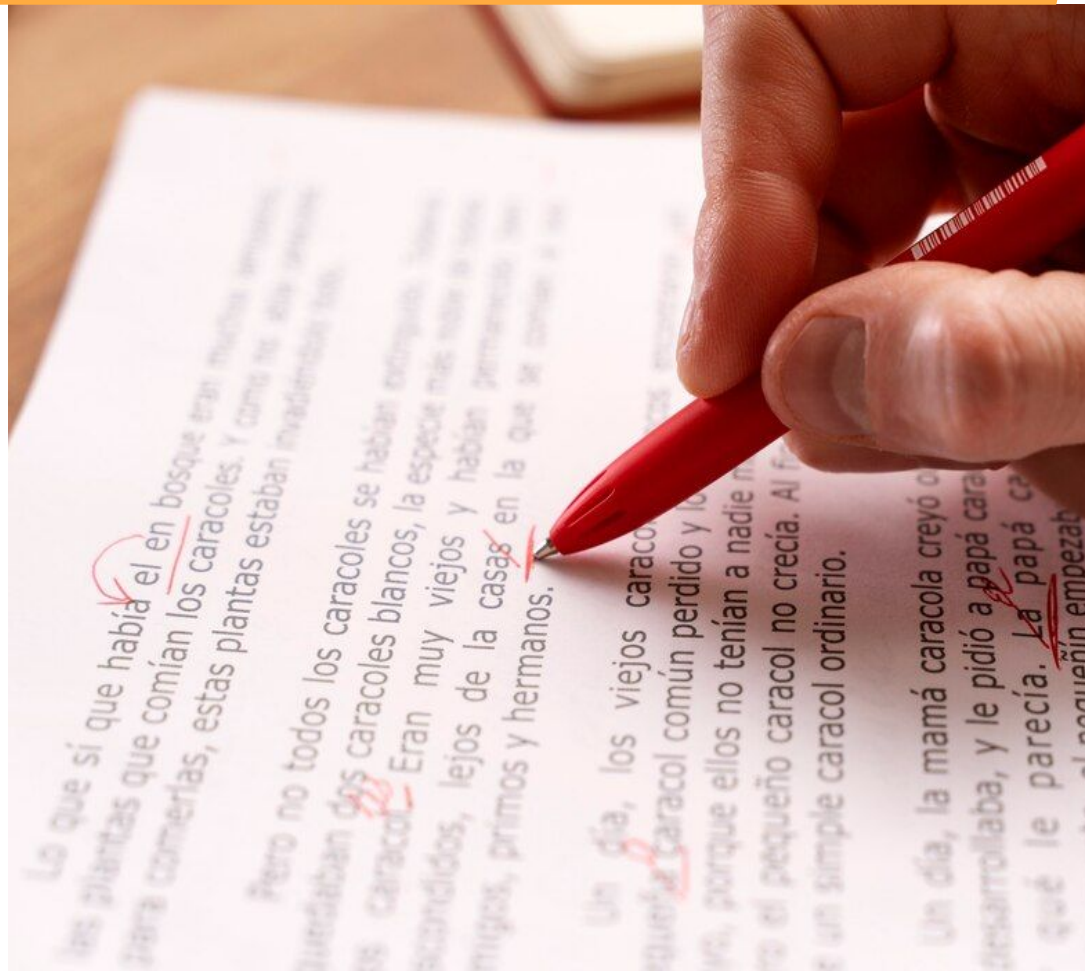
Si precisa inoltre che l'aggiornamento del software dike viene proposto direttamente dall'applicazione e non attraverso invio di mail; su piattaforma

LA REGOLA DEI 5 SECONDI

La fretta spesso non è una alleata:
non “pressiamo” dipendenti e collaboratori
a fare sempre più di fretta
(a volte, alcuni secondi in più,
anziché uno spreco di tempo,
sono un salvavita).

PHISHING: COME DIFENDERSI?

La grammatica.



PHISHING: COME DIFENDERSI?

Il tono.

PHISHING: COME DIFENDERSI?

La richiesta.

PHISHING: COME DIFENDERSI?

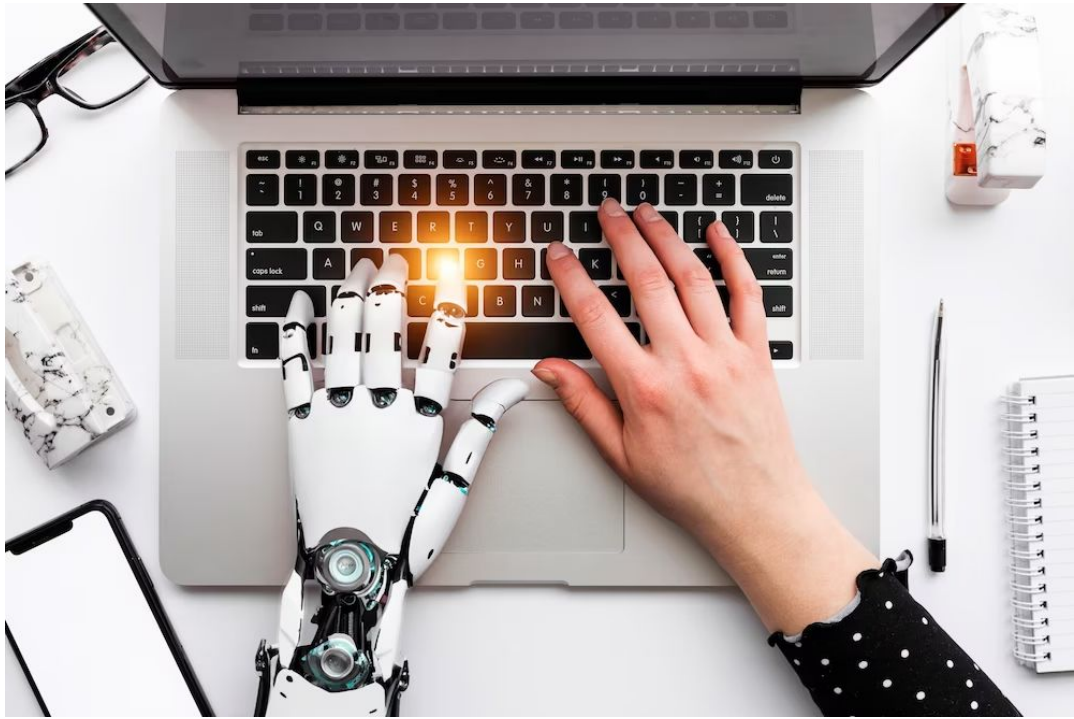
I link (soprattutto se abbreviati).

PHISHING: COME DIFENDERSI?

L’indirizzo di posta elettronica.

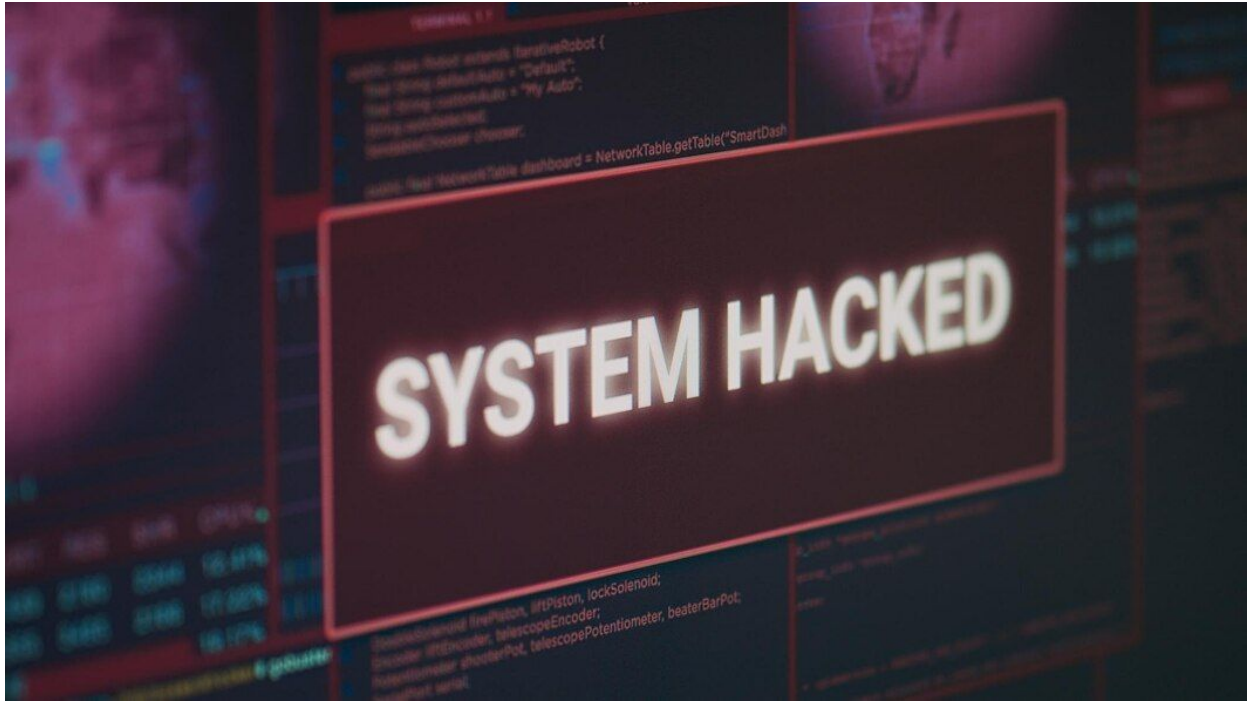
PHISHING: ATTENZIONE ALL'INTELLIGENZA ARTIFICIALE

NB: L'AI renderà i messaggi di phishing sempre più precisi e raffinati; occorrerà dunque alzare maggiormente la guardia.



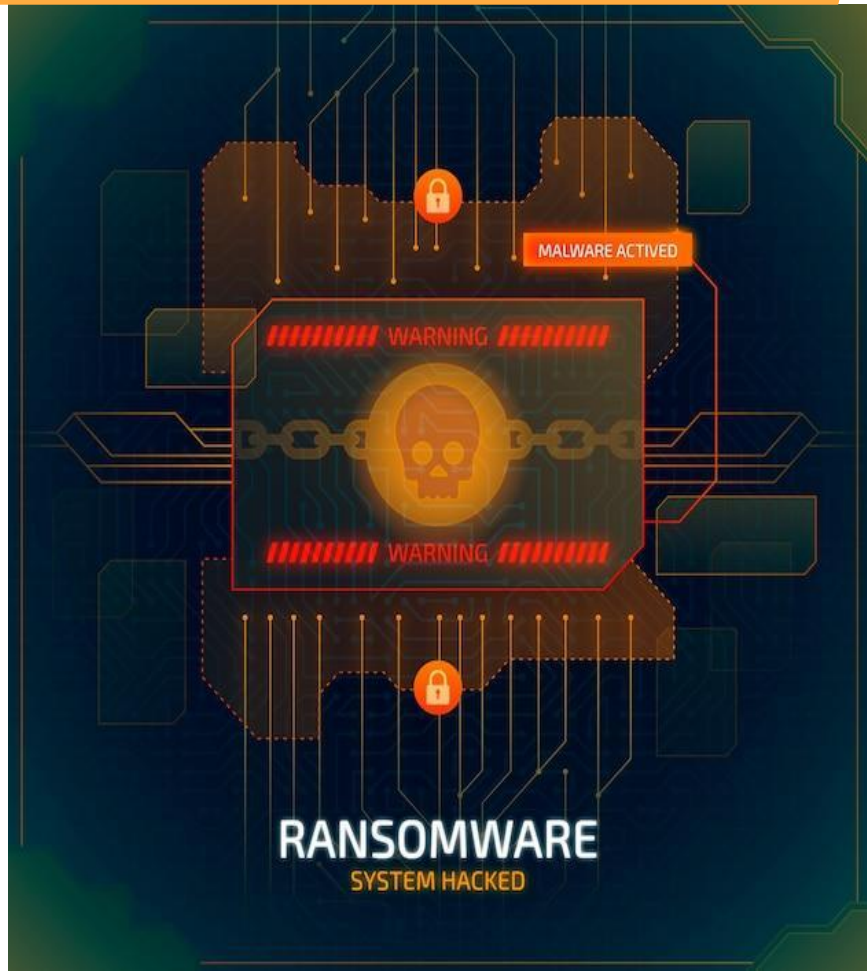
I MALWARE

Applicazioni con la finalità di creare un danno.



I RANSOMWARE

Malware che criptano i dati rendendoli inutilizzabili dal proprietario.



I RANSOMWARE

Le e-mail di phishing veicolano circa il 75% dei ransomware: lo scopo solitamente è il ricatto.

LA REGOLA DEI 5 SECONDI

La fretta spesso non è una alleata:
non “pressiamo” dipendenti e collaboratori
a fare sempre più di fretta
(a volte, qualche secondo in più,
anziché uno spreco di tempo,
è un salvavita).

MALWARE E RANSOMWARE: COME DIFENDERSI?

Prima di scaricare un file, valutare chi, cosa, perché.

MALWARE E RANSOMWARE: COME DIFENDERSI?

“In sola lettura” / “Visualizzazione protetta.”

VISUALIZZAZIONE PROTETTA Attenzione. I file provenienti da Internet possono contenere virus. A meno che non sia necessario modificare il file, è consigliabile restare in Visualizzazione protetta. Abilita modifica

I download automatici.

MALWARE E RANSOMWARE: COME DIFENDERSI?

I filtri antispam.

MALWARE E RANSOMWARE: COME DIFENDERSI?

Antivirus / Antimalware.

GLI ATTACCHI DDoS

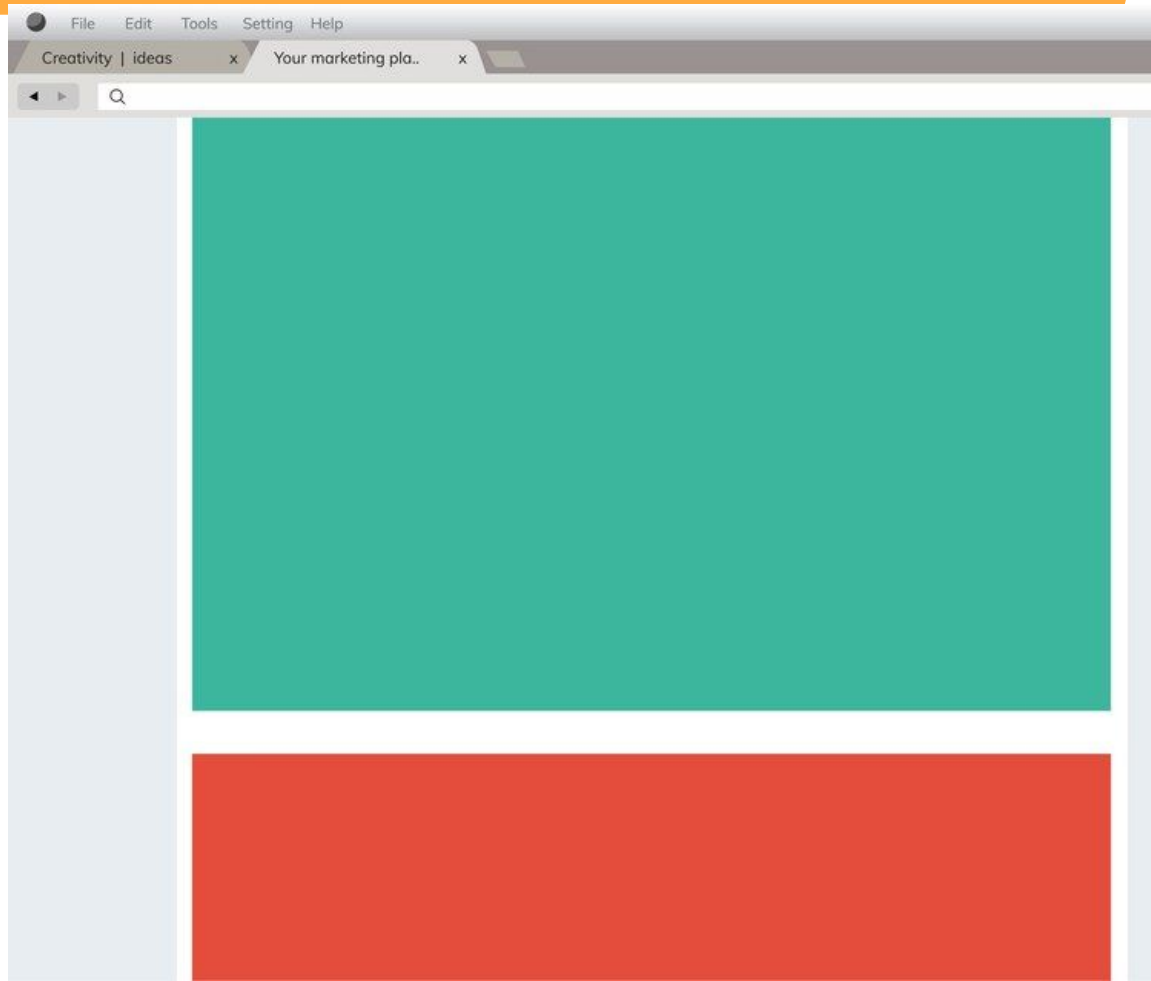
Sono tentativi malevoli di sovraccaricare un servizio online con un flusso massivo di richieste, rendendolo inaccessibile agli utenti legittimi. Sfruttando una rete distribuita di dispositivi, gli aggressori cercano di sopraffare le risorse del sistema, causando interruzioni di servizio.

- Sistemi di mitigazione DDoS
- Firewall e filtraggio del traffico
- Limitazione dei protocolli e delle porte
- Monitoraggio del traffico

IL TAP - NABBING

È l’apertura automatica di più schede nel browser, affinché l’utente non si ricordi di averle aperte e cada nelle trappole contenute in tali schede.

- Blocco di pop-up e reindirizzamenti
- Utilizzo di browser sicuri
- Aggiornamenti
- Consapevolezza



LE PASSWORD: LA CHIAVE SOTTO LO ZERBINO

Eccellenze in Digitale

UNIONCAMERE

TOP 10 PASSWORD PIÙ COMUNI IN ITALIA (2023)

CLASSIFICA	PASSWORD
1	admin
2	123456
3	password
4	Password
5	12345678
6	123456789
7	password99
8	qwerty
9	UNKNOWN
10	12345

Eccellenze in Digitale

UNIONCAMERE

TOP 10 PASSWORD PIÙ COMUNI IN ITALIA (2023)

CLASSIFICA	PASSWORD	CONTEGGIO
1	admin	38.369
2	123456	14.335
3	password	12.476
4	Password	10.281
5	12345678	5.831
6	123456789	4.049
7	password99	3.847
8	qwerty	2.688
9	UNKNOWN	2.539
10	12345	2.464

Eccellenze in Digitale

UNIONCAMERE

TOP 10 PASSWORD PIÙ COMUNI IN ITALIA (2023)

CLASSIFICA	PASSWORD	CONTEGGIO	TEMPO NECESSARIO PER DECIFRARLA
1	admin	38.369	< 1 Secondo
2	123456	14.335	< 1 Secondo
3	password	12.476	< 1 Secondo
4	Password	10.281	< 1 Secondo
5	12345678	5.831	< 1 Secondo
6	123456789	4.049	< 1 Secondo
7	password99	3.847	< 1 Secondo
8	qwerty	2.688	< 1 Secondo
9	UNKNOWN	2.539	17 Minuti
10	12345	2.464	< 1 Secondo

Eccellenze in Digitale

UNIONCAMERE

TOP 10 PASSWORD PIÙ COMUNI NEL MONDO (2023)

CLASSIFICA	PASSWORD	CONTEGGIO	TEMPO NECESSARIO PER DECIFRARLA
1	123456	4.524.867	< 1 Secondo
2	admin	4.008.850	< 1 Secondo
3	12345678	1.371.152	< 1 Secondo
4	123456789	1.213.047	< 1 Secondo
5	1234	969.811	< 1 Secondo
6	12345	728.414	< 1 Secondo
7	password	710.321	< 1 Secondo
8	123	528.086	< 1 Secondo
9	Aa123456	319.725	< 1 Secondo
10	1234567890	302.709	< 1 Secondo

TOP 200 PASSWORD PIÙ COMUNI (2023)

HTTPS://NORDPASS.COM/IT/MOST-COMMON-PASSWORDS-LIST/

PASSWORD: QUALI ASPETTI ATTENZIONARE?

Avere molte credenziali di accesso ci porta a sbagliare.

PASSWORD: QUALI ASPETTI ATTENZIONARE?

Avere molte credenziali di accesso ci porta a sbagliare.

Spesso si creano password deboli e/o uguali.

PASSWORD: QUALI ASPETTI ATTENZIONARE?

Avere molte credenziali di accesso ci porta a sbagliare.

Spesso si creano password deboli e/o uguali.

Pensiamo di doverle ricordare: **non è così!**

PASSWORD: QUALI ASPETTI ATTENZIONARE?

Avere molte credenziali di accesso ci porta a sbagliare.

Spesso si creano password deboli e/o uguali.

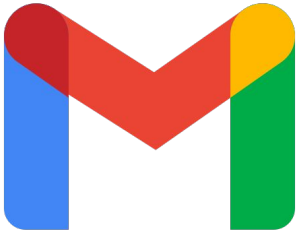
Pensiamo di doverle ricordare: **non è così**!

Lo scopo è l'**infiltrazione**.

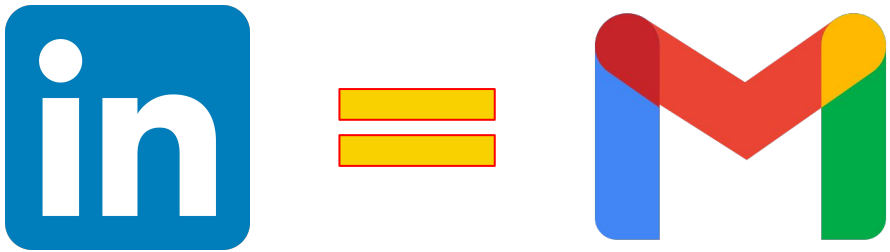
ESEMPIO CONCRETO: SI PARTE DALLA PASSWORD…

ESEMPIO CONCRETO: SI PARTE DALLA PASSWORD…

=

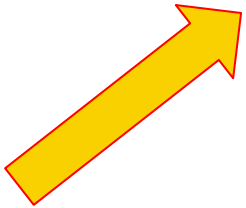


ESEMPIO CONCRETO: SI PARTE DALLA PASSWORD…



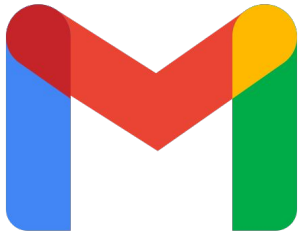
ESEMPIO CONCRETO: SI PARTE DALLA PASSWORD…

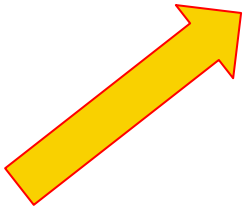
=



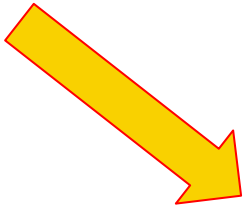
ESEMPIO CONCRETO: SI PARTE DALLA PASSWORD...

=





INTESA SANPAOLO

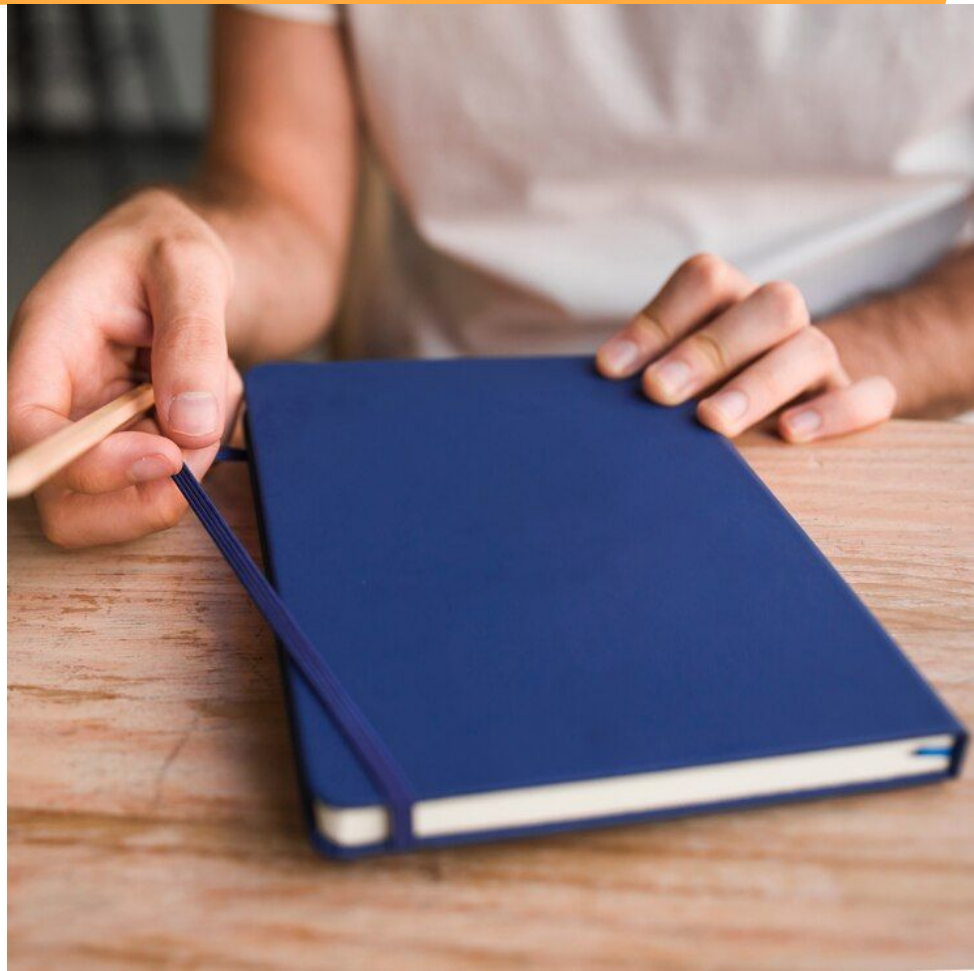


COME VIENE RUBATA UNA PASSWORD?

Spiata.

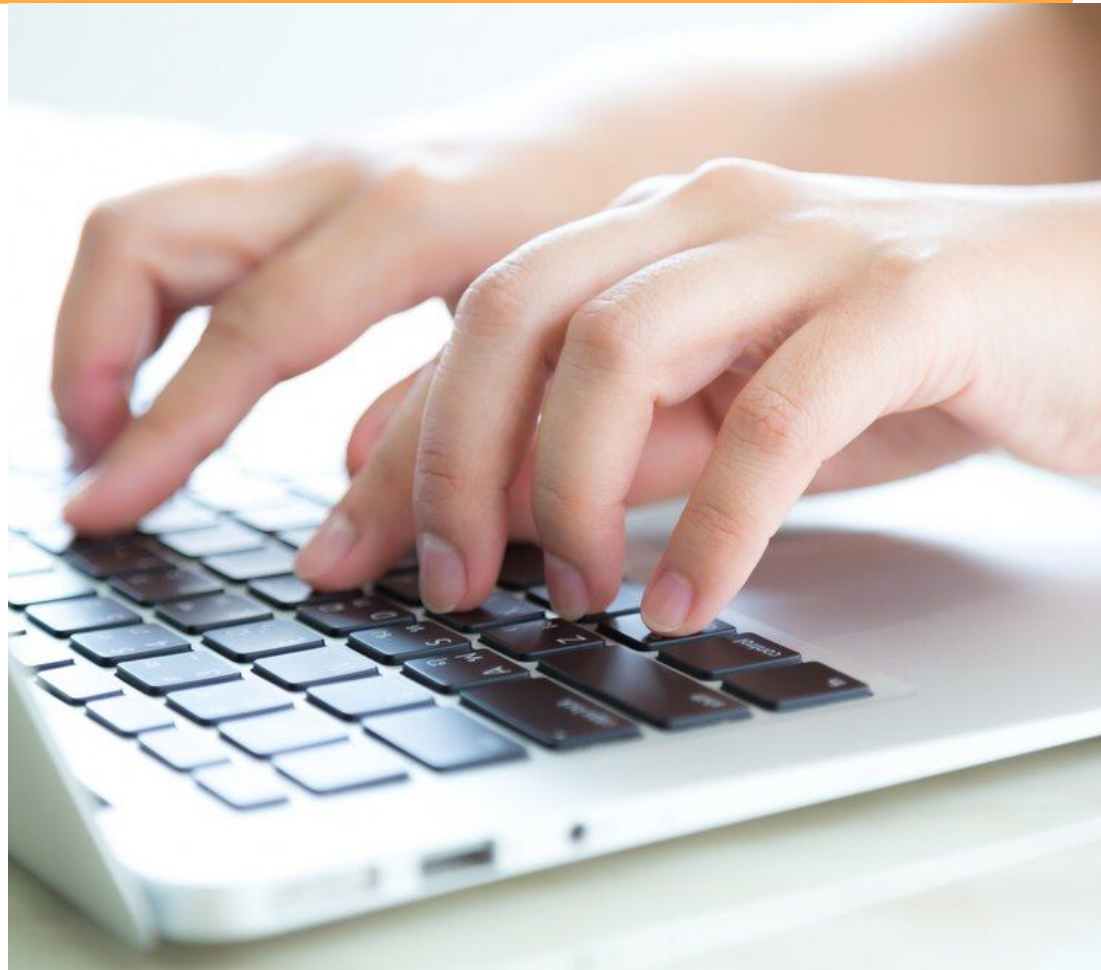
COME VIENE RUBATA UNA PASSWORD?

Rubata.



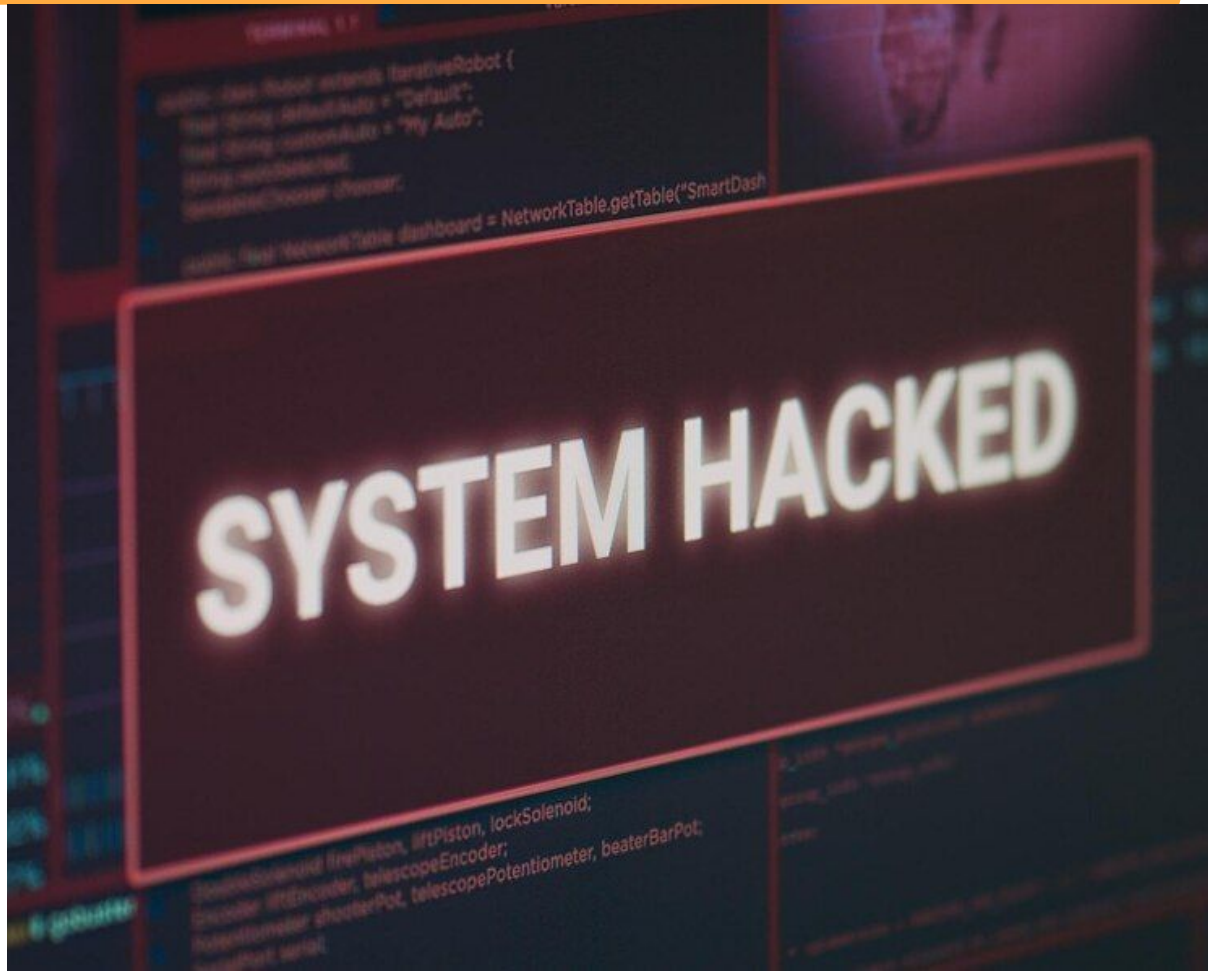
COME VIENE RUBATA UNA PASSWORD?

Fornita da noi (finto link o malware)



COME VIENE RUBATA UNA PASSWORD?

Data Breach.



COME VIENE RUBATA UNA PASSWORD?

Attacchi “Brute Force”

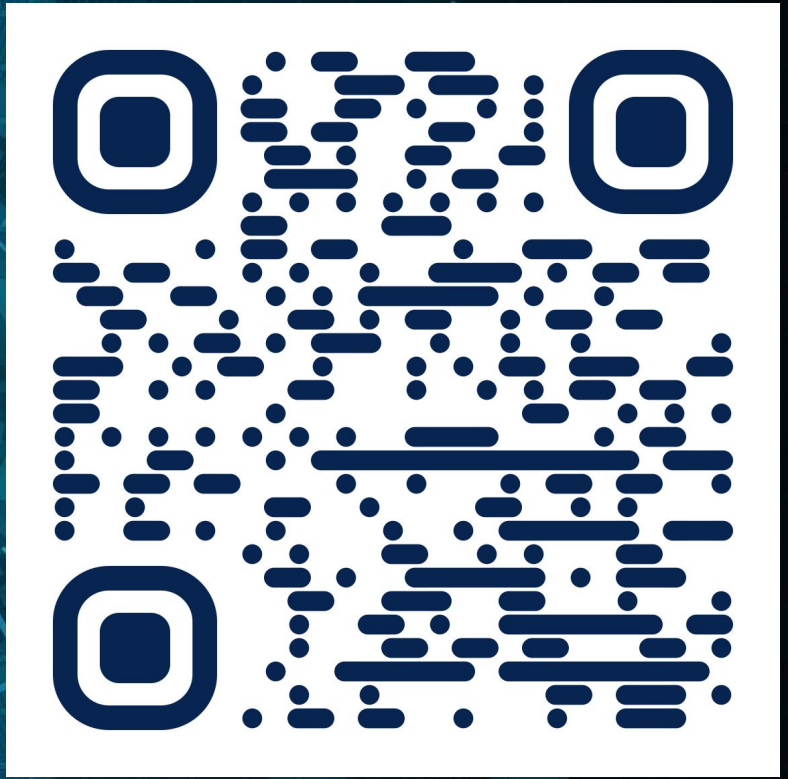
TOCCA A VOI!

ANDATE SUL SITO

https://password.kaspersky.com/it/

E INSERITE UNA PASSWORD CHE

UTILIZZATE: COSA ESCE?



TOCCA A VOI!

Avresti dovuto cambiare questa password già molto tempo fa!

- Cattive notizie
  ⚠ Ripetizione di sequenze di caratteri
- Questa password è apparsa 42542807 volte in un database di password esposte.

La tua password può essere craccata ancor prima che tu possa dire "Ops!"

Vuoi imparare a creare password super forti? Clicca qui!

TOCCA A VOI!

Ottima password!

- La password è a prova di hacker.
- La tua password non appare in alcun database di password rese note.

La tua password sarà craccata con un comune home computer in circa...

10000+ secoli

Farai in tempo a trovare “la risposta alla domanda fondamentale sulla vita, l'universo e tutto quanto”. Perciò, non ti preoccupare per la tua password.

Vuoi imparare a creare password super forti? Clicca qui!

PASSWORD: COME DIFENDERSI?

- Lunghezza di almeno 12 caratteri
- Maiuscole + Minuscole + Numeri + Caratteri speciali

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

PASSWORD: COME DIFENDERSI?

- No riferimenti personali (Spear Phishing)
- No parole o frasi di senso compiuto (dizionari/vocabolari)

PASSWORD: COME DIFENDERSI?

- Non utilizzare i sistemi di salvataggio automatico delle password
- Utilizzare i Password Manager (famosi)

FOCUS: I PASSWORD MANAGER - LASTPASS

LastPass | Perché LastPass | Prezzi | Personale | Business | Partner | Supporto | Accedi | Contatta l'ufficio vendite | Ottieni LastPass Free

Meno password, meno pensieri

Preparati a un futuro senza password, liberandotene subito per una protezione pervasiva.

Personale | Aziendale

Inizia una prova gratuita di qualsiasi piano. Non è necessaria una carta di credito.

Più di 33 milioni
Le persone che proteggono le proprie

4.4★
Valutazione di Chrome Web Store e App Store

G2 4.4★
Leader nella gestione delle password

Top 50 Security Products 2023
Best Software Awards per il miglior prodotto per la

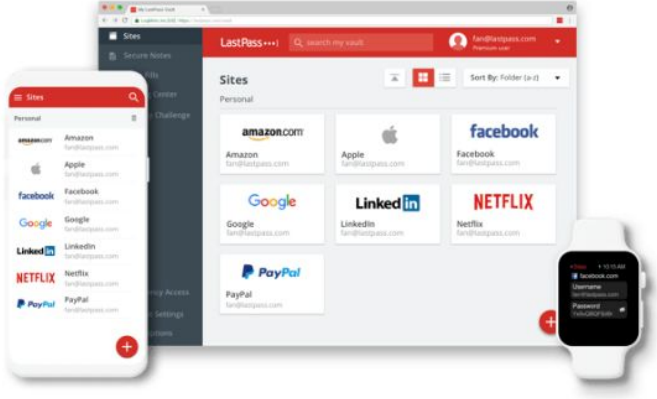
Le aziende che scelgono LastPass

Ehilà 👋, che ne diresti di un mondo digitale più sicuro?

LASTPASS: REGISTRAZIONE

Una password.
Zero stress.

A tutto il resto ci pensa LastPass.



Caratteristiche di Free

- Cassaforte sicura per le password

Crea un account

o accedi

Email

Password principale

Forza

Conferma password principale

Promemoria (opzionale)

Registrati gratis

Compilando questo modulo, accetto le Condizioni per l'utilizzo e l'Informativa sulla privacy. Desidero ricevere email promozionali, finché non lo rifiuterò esplicitamente.

LASTPASS: FREE VS PREMIUM

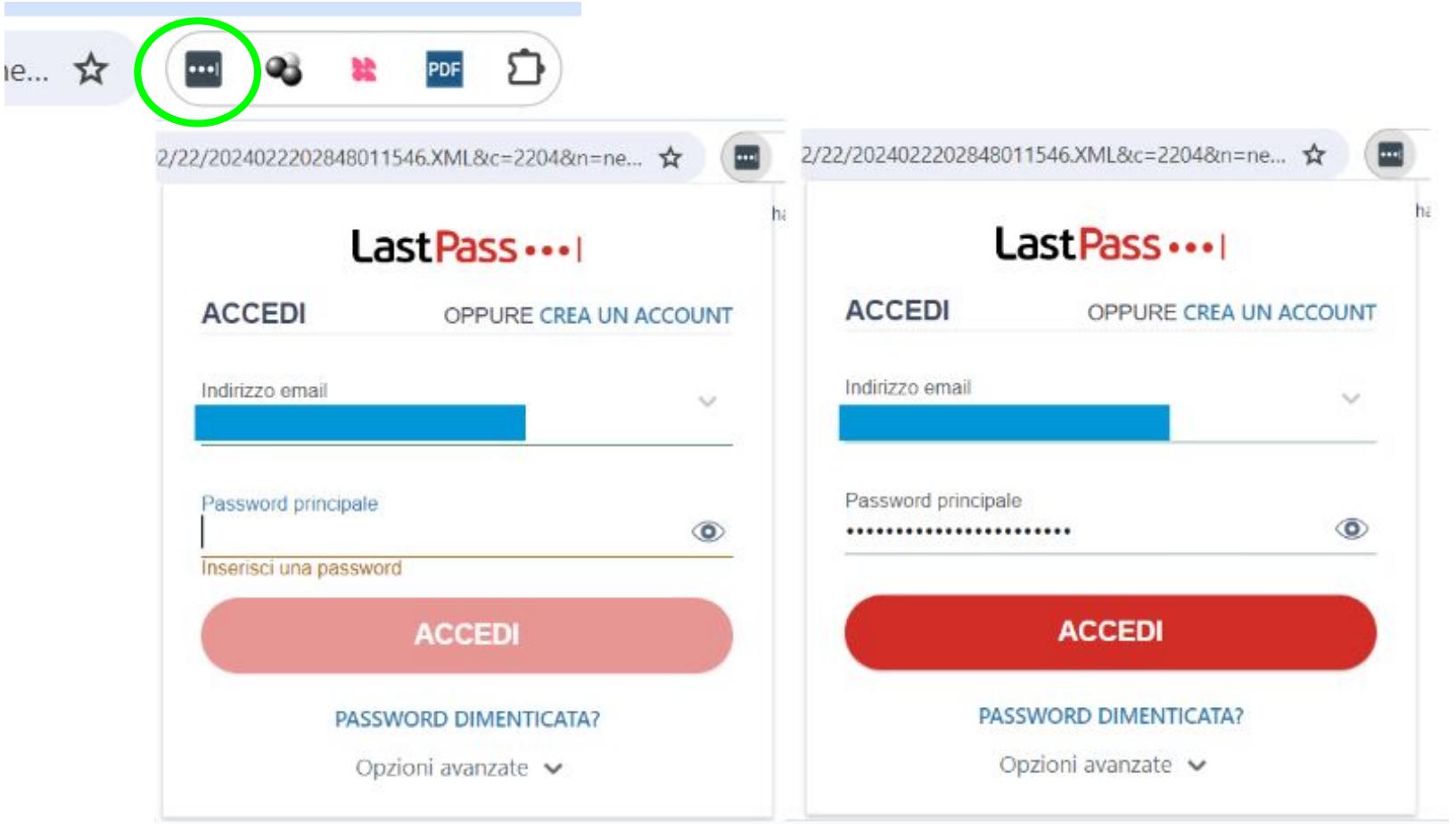
Caratteristiche di Free

- Cassaforte sicura per le password
- Accedi da un tipo di dispositivo
- Condivisione uno a uno
- Salvataggio e inserimento delle password
- Generatore di password
- Note sicure
- Dashboard sicurezza e punteggio di sicurezza
- Monitoraggio del dark web
- Supporto di base
- Autenticazione a più fattori
- LastPass Authenticator

Caratteristiche di Premium

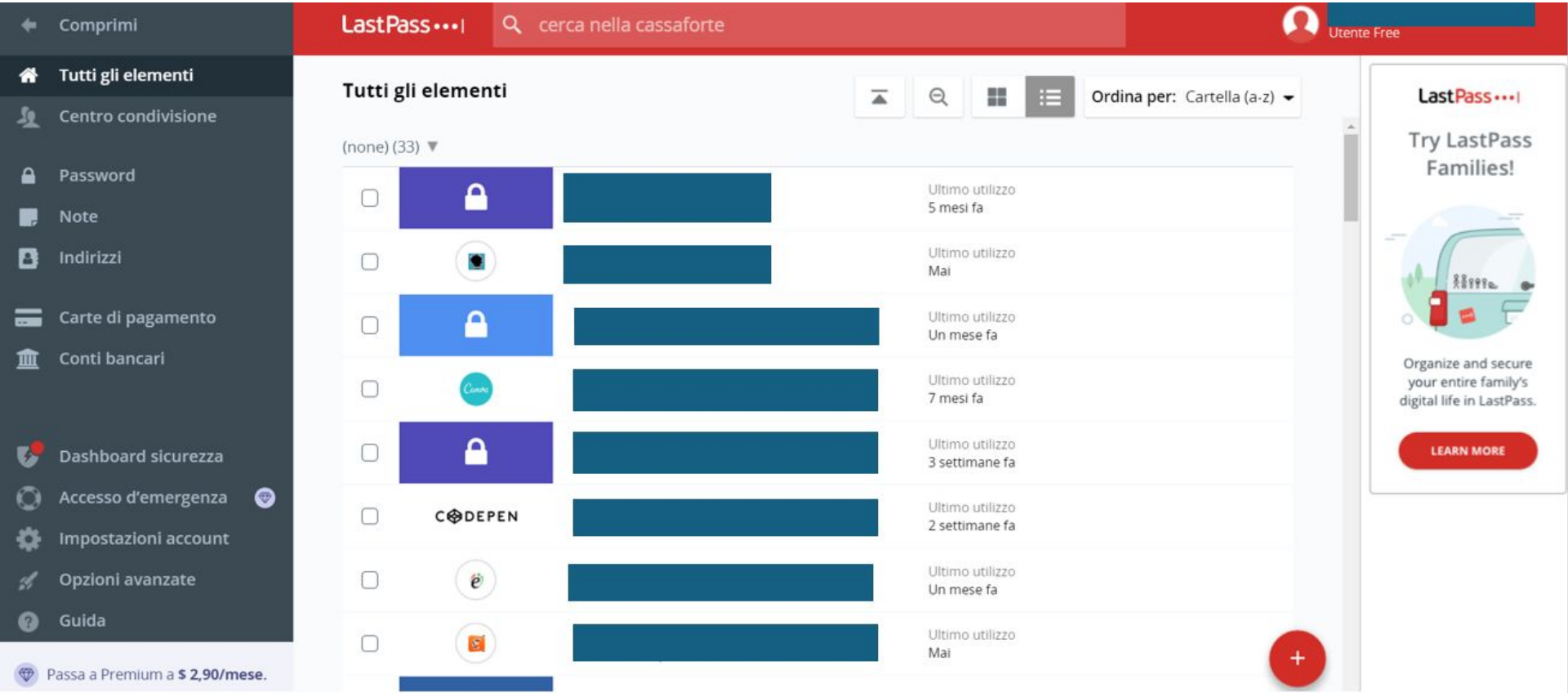
- Condivisione uno a molti
- Accesso di emergenza
- Opzioni multifattoriali avanzate
- Supporto tecnico prioritario
- LastPass per applicazioni
- 1 GB di spazio di archiviazione file crittografato
- Supporto personale

LASTPASS: ESTENSIONE ED ACCESSO RAPIDO

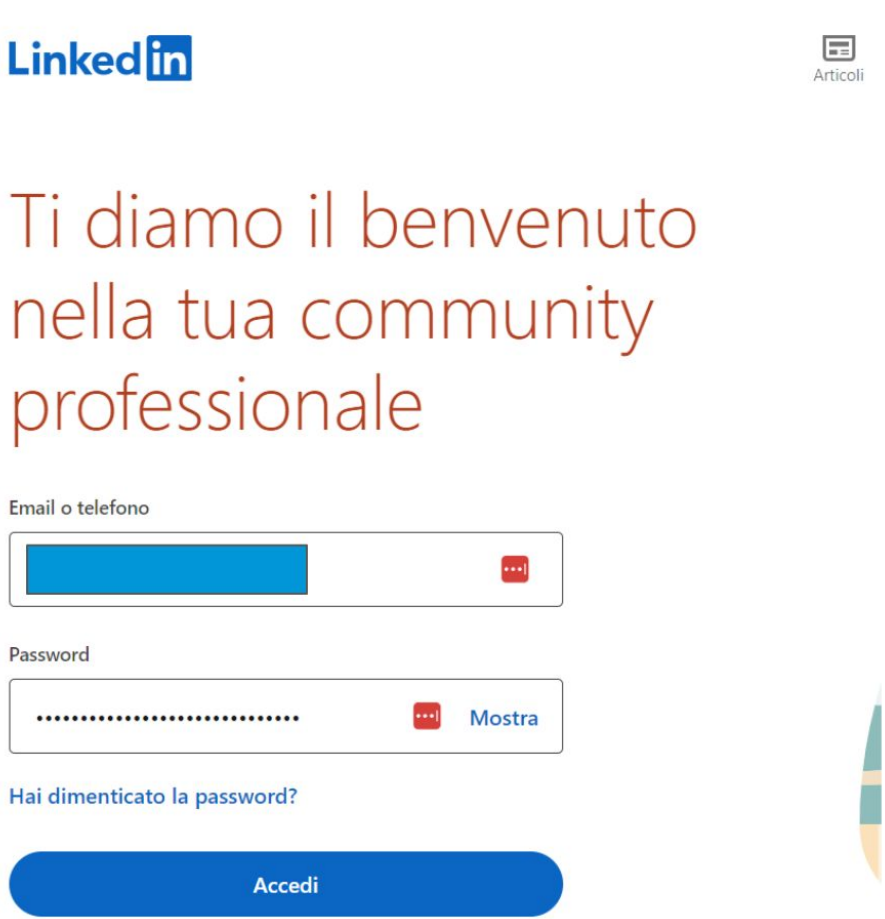


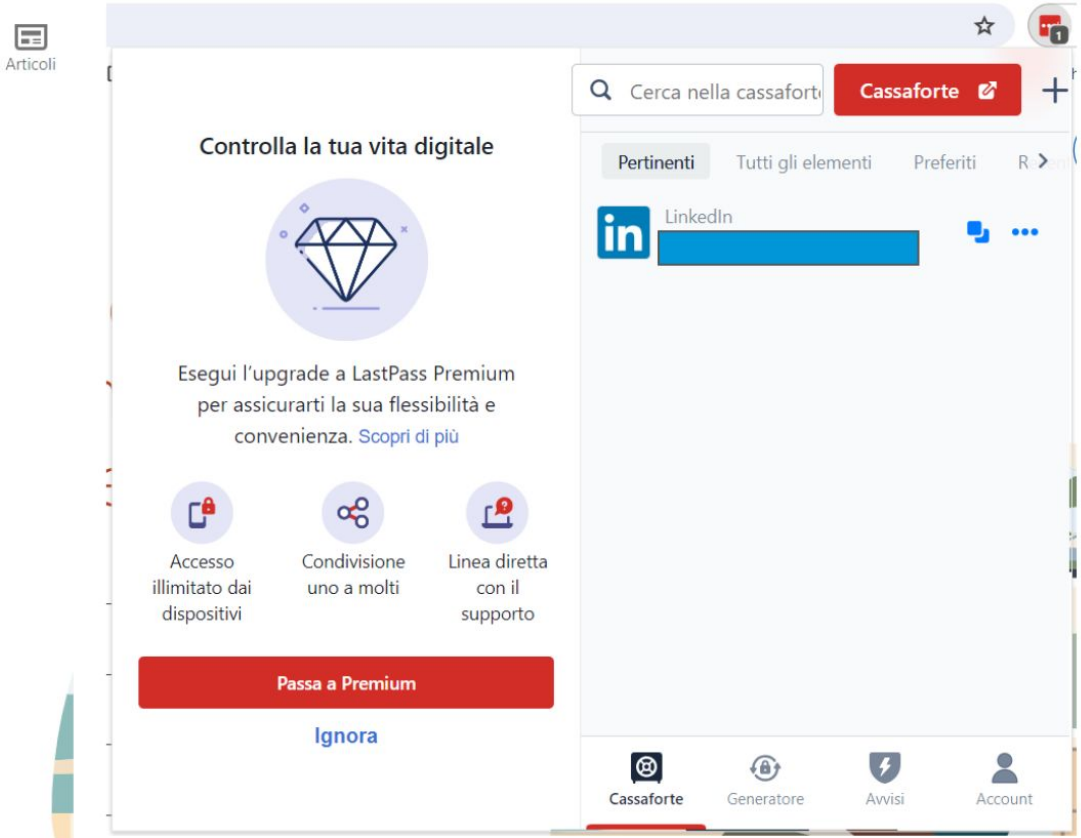
LASTPASS: ESTENSIONE ED ACCESSO RAPIDO

LASTPASS: HOME



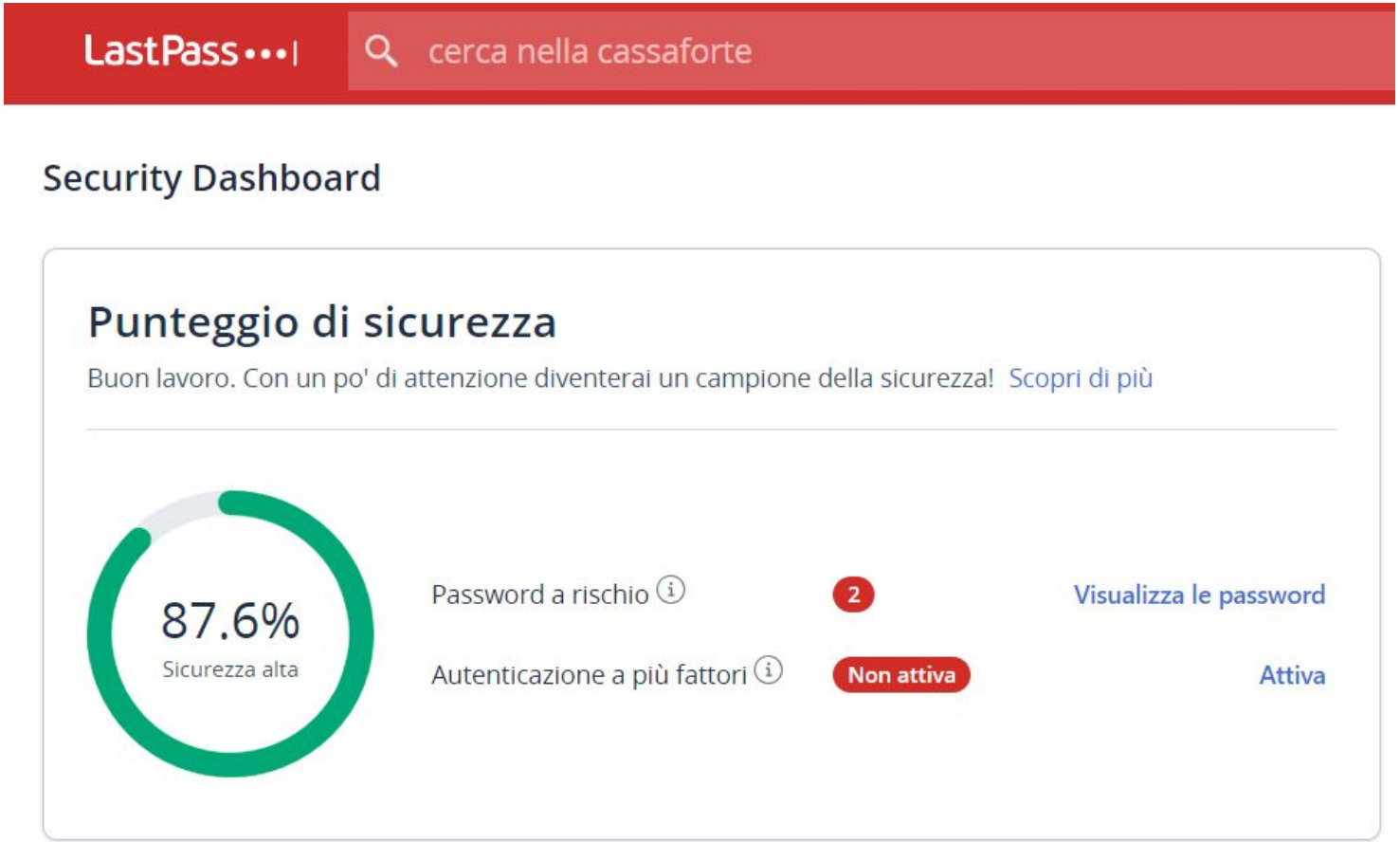
LASTPASS: INSERIMENTO CREDENZIALI



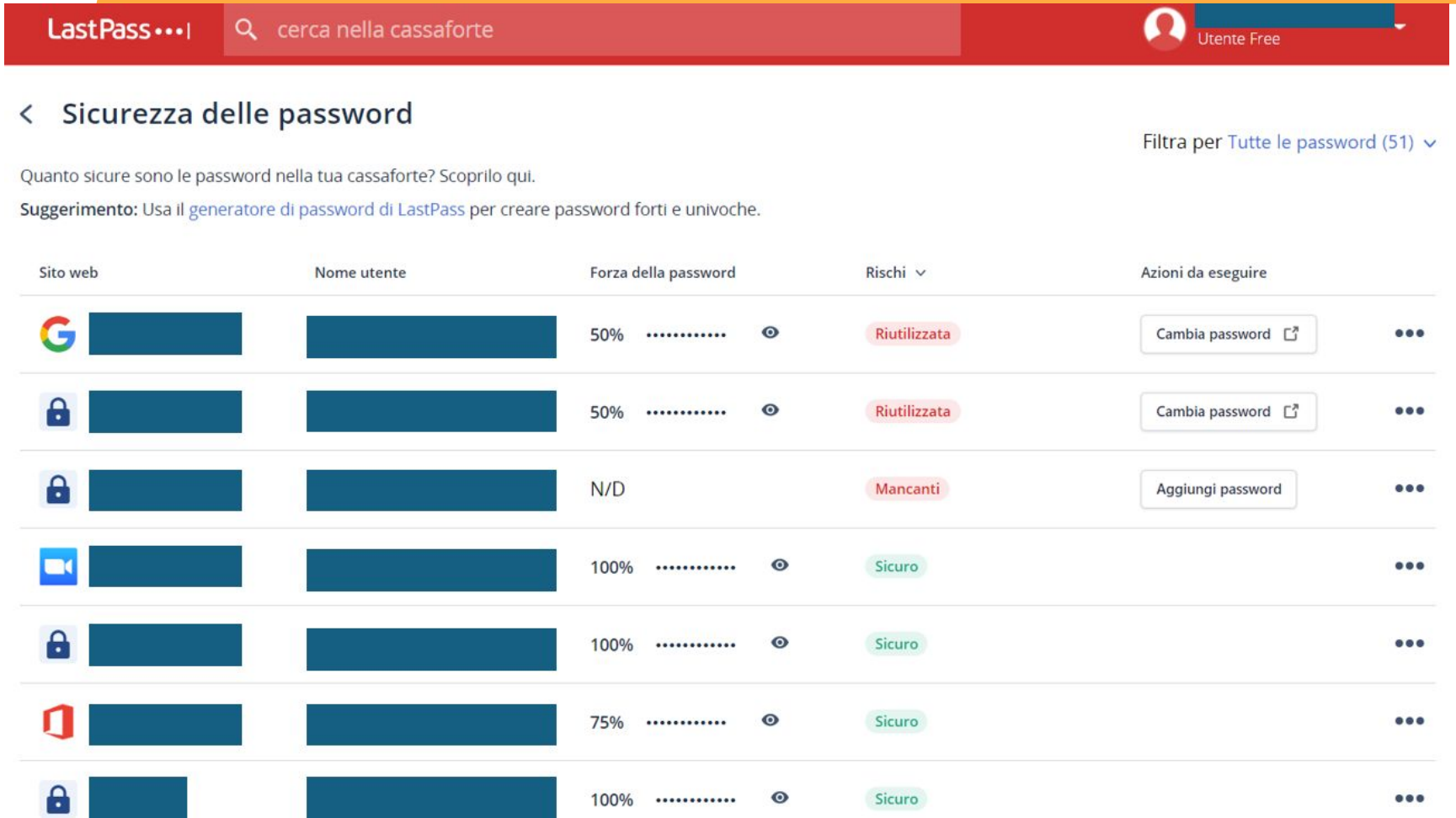


LASTPASS: GENERATORE DI PASSWORD

LASTPASS: SECURITY DASHBOARD - PUNTEGGIO DI SICUREZZA

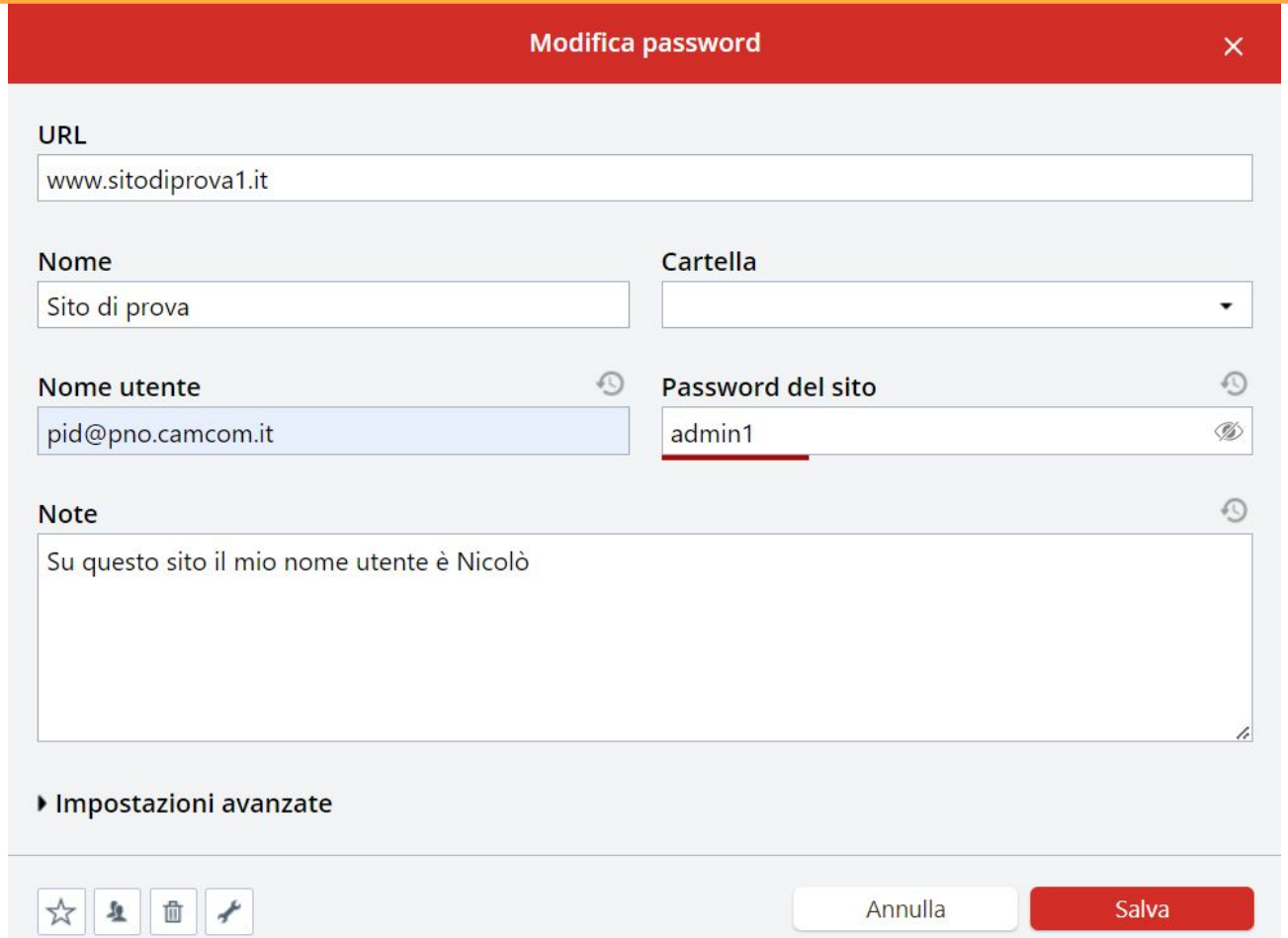


LASTPASS: SECURITY DASHBOARD - PUNTEGGIO DI SICUREZZA

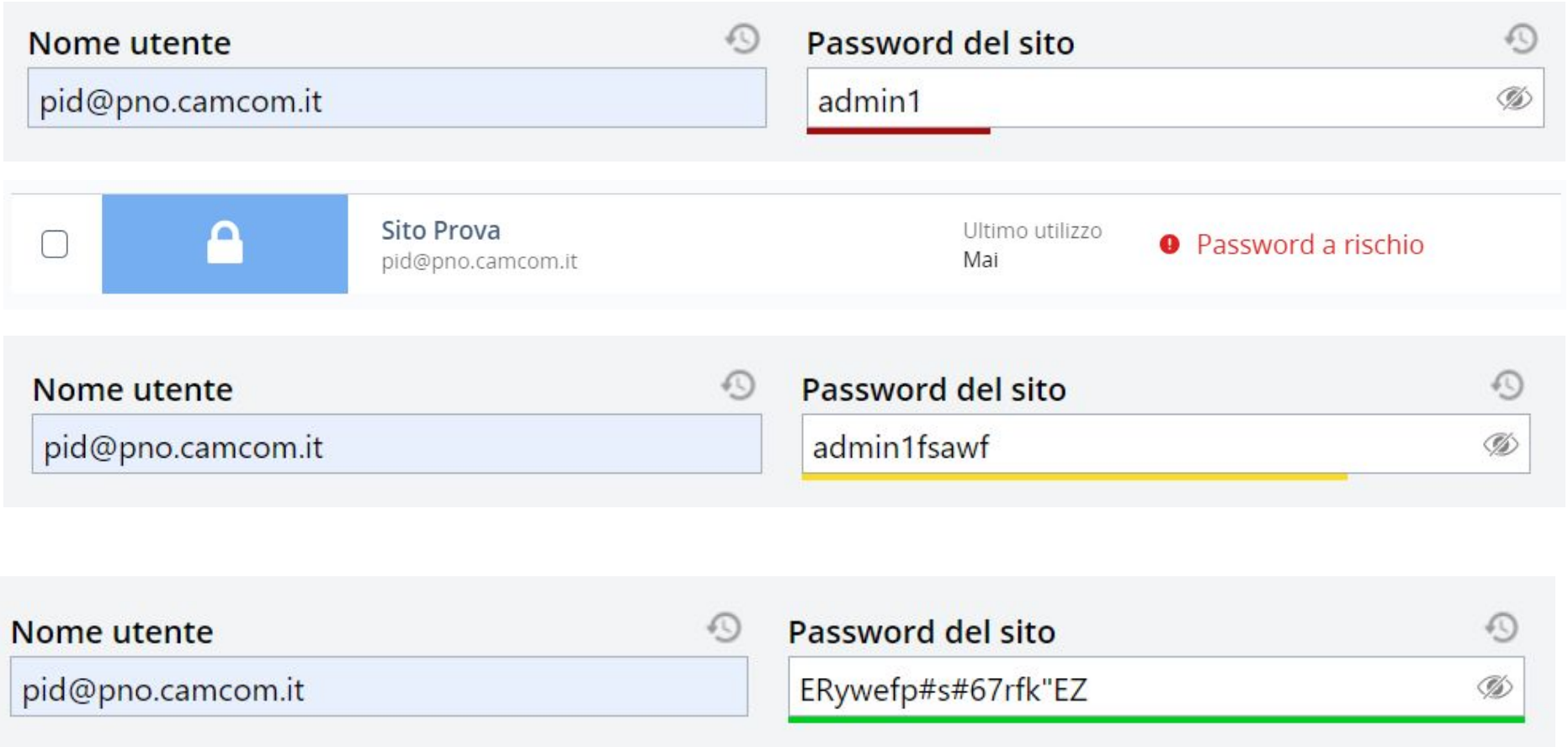


LASTPASS: SECURITY DASHBOARD - MONITORAGGIO DEL DARK WEB

LASTPASS: AGGIUNGERE UNA PASSWORD



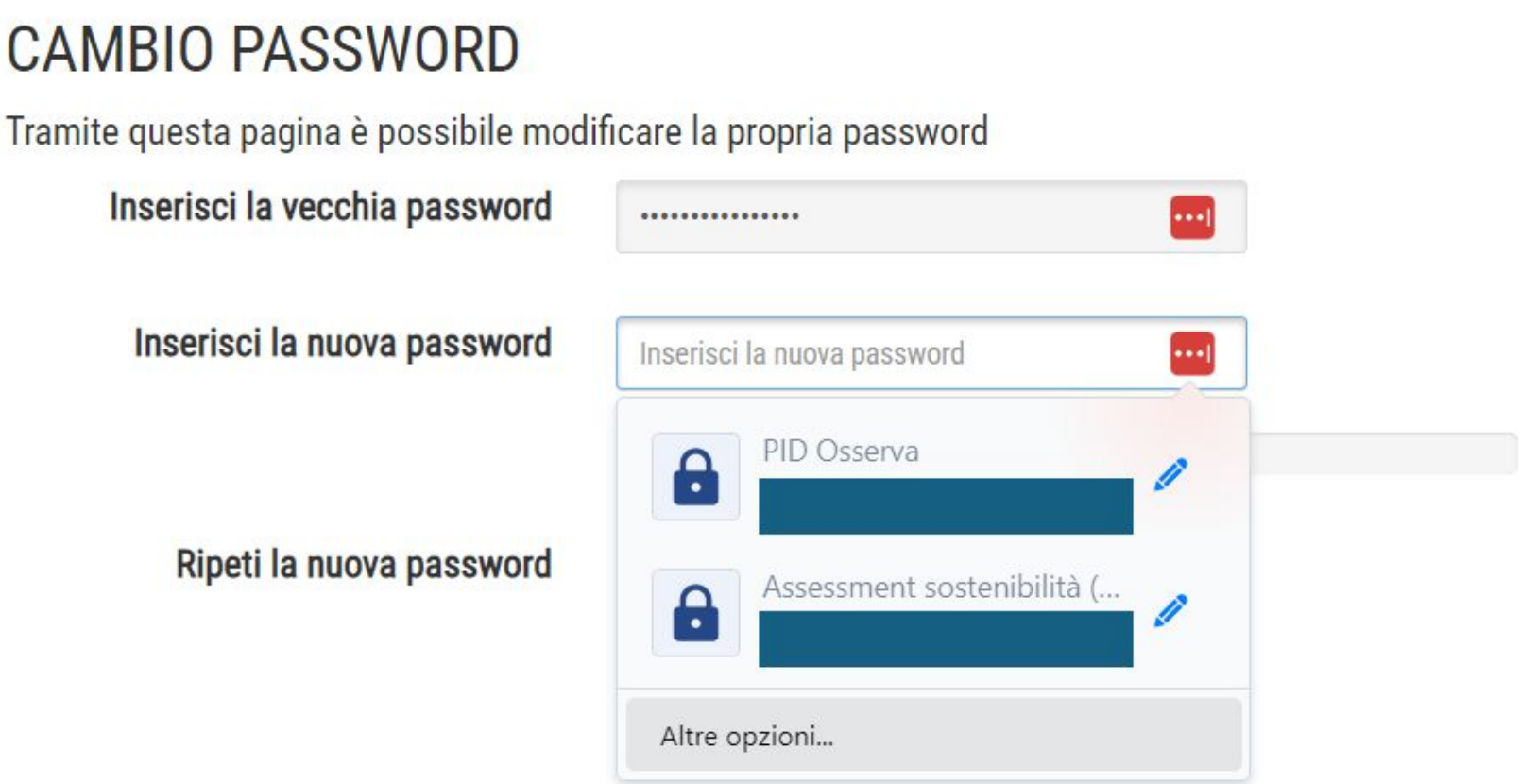
LASTPASS: SICUREZZA DELLA PASSWORD



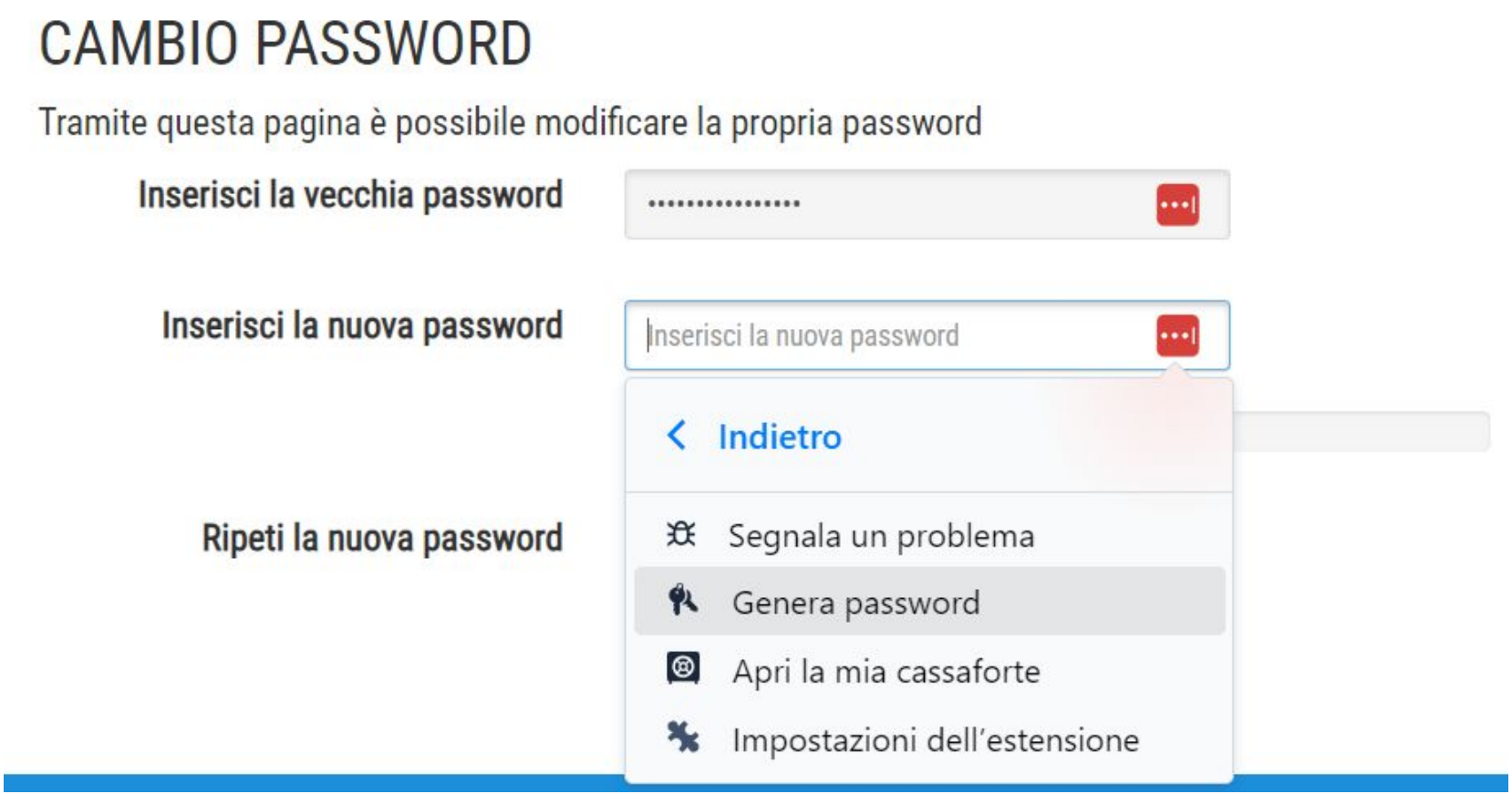
LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

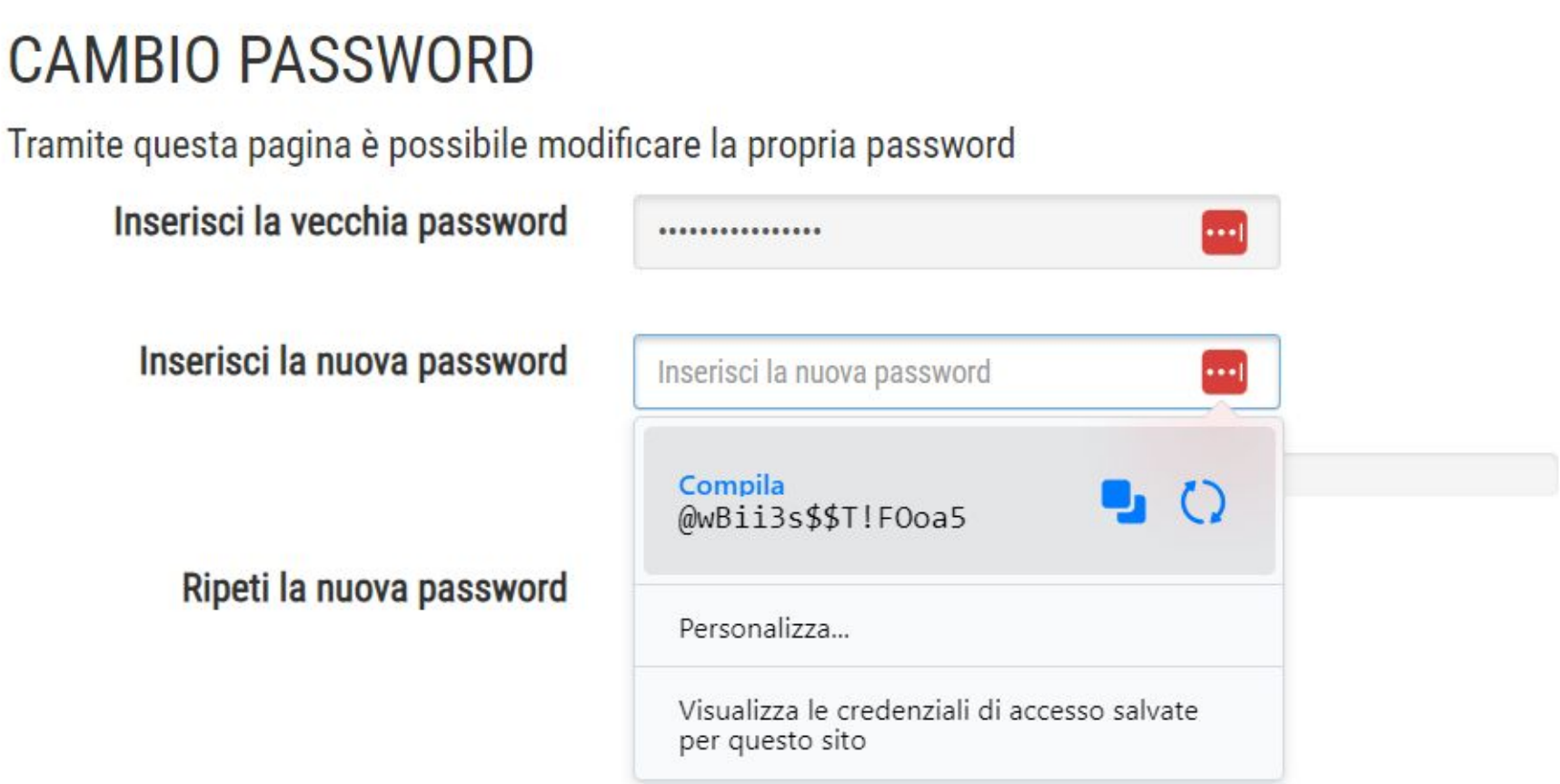
LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA



LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

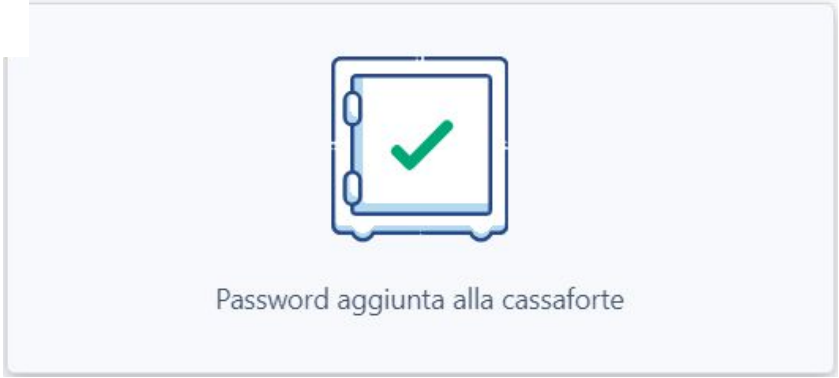


LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

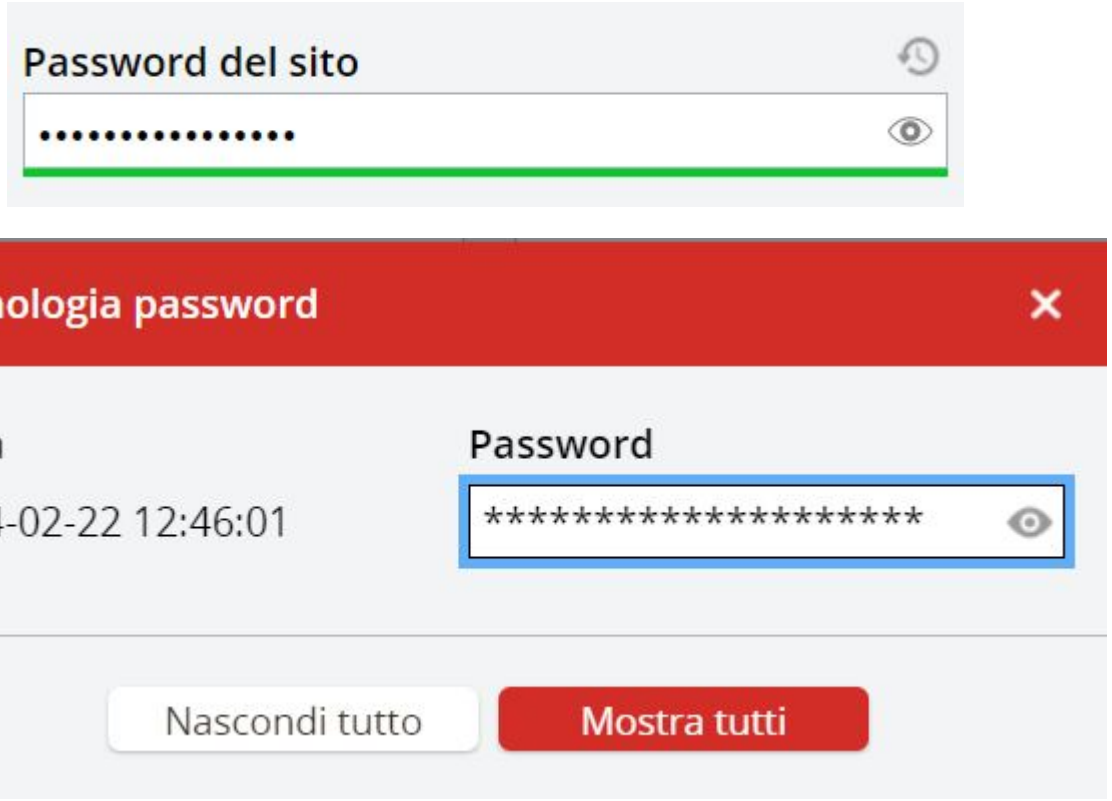


LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

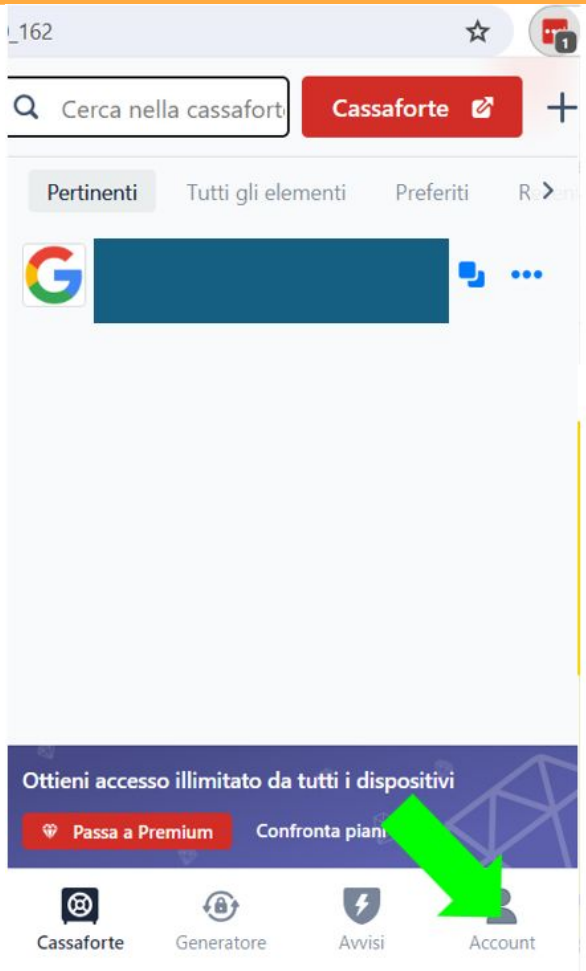
LASTPASS: CAMBIO/AGGIUNTA PASSWORD AUTOMATICA

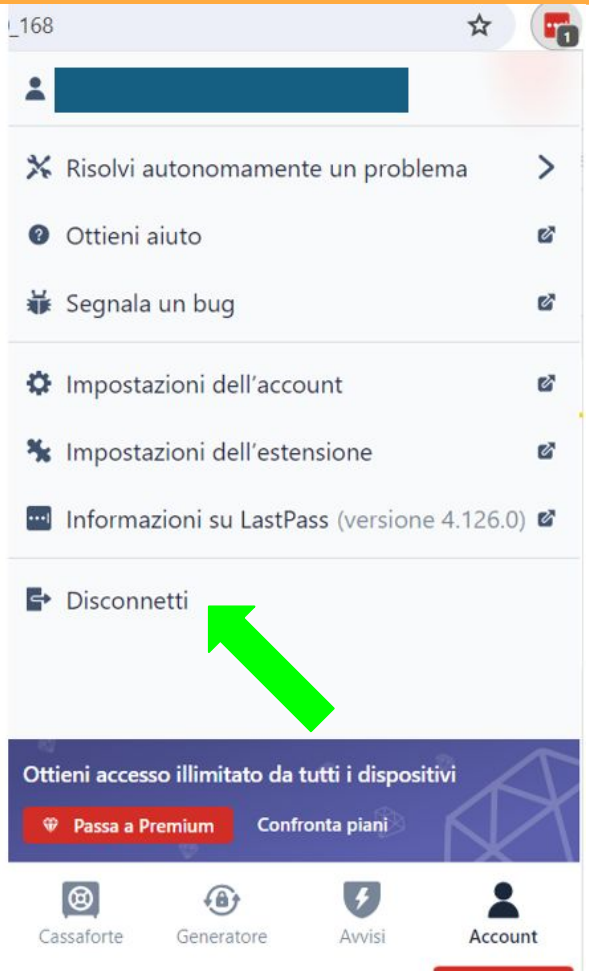


LASTPASS: RECUPERO DI VECCHIE PASSWORD



LASTPASS: DISCONNESSIONE





STRUMENTI DI LAVORO E BEST PRACTICE GENERALI

STRUMENTI DI LAVORO

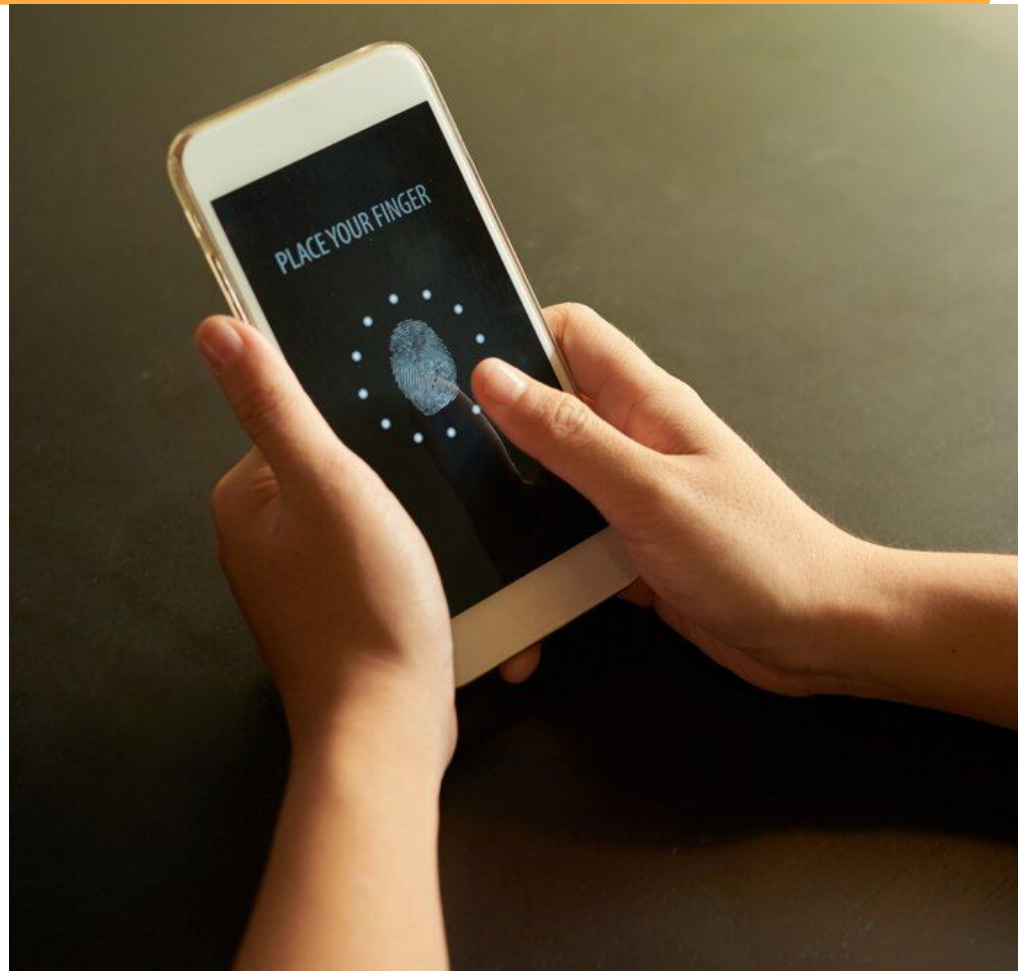
STRUMENTI DI LAVORO: APP E STORE

Solo app sicure e necessarie.

Attenzione ai permessi che vengono concessi.

STRUMENTI DI LAVORO: SMARTPHONE AZIENDALI

Protetto da codici e sblocchi (eventualmente condivisi con il superiore).

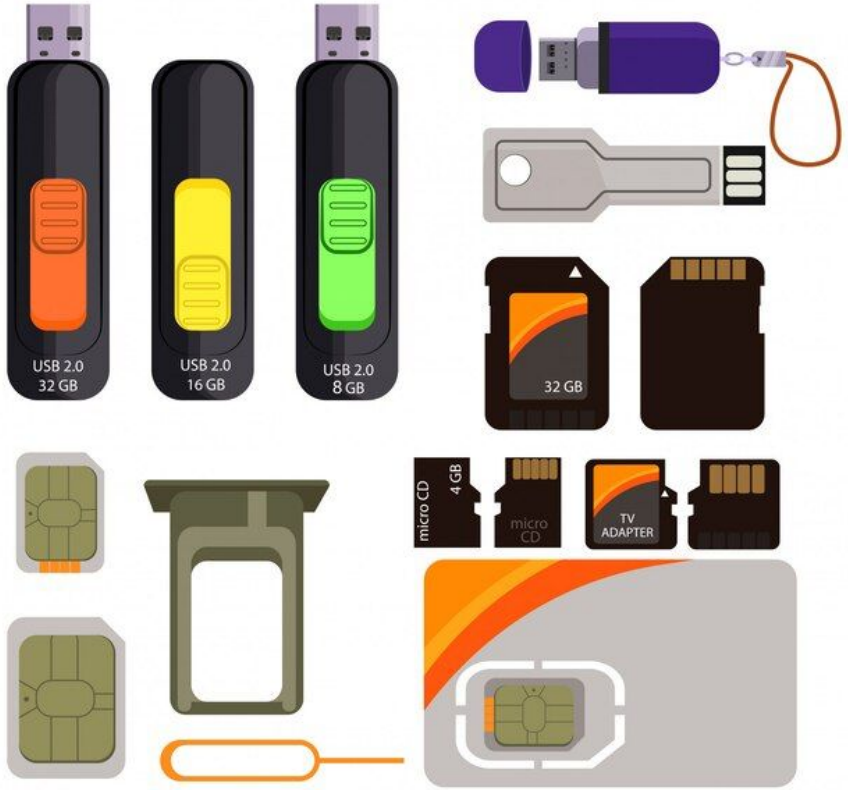


STRUMENTI DI LAVORO: DISPOSITIVI USB O CD/DVD

No accettarli da sconosciuti.

Non lasciarsi prendere dalla curiosità.

Disattivare l’autorun.

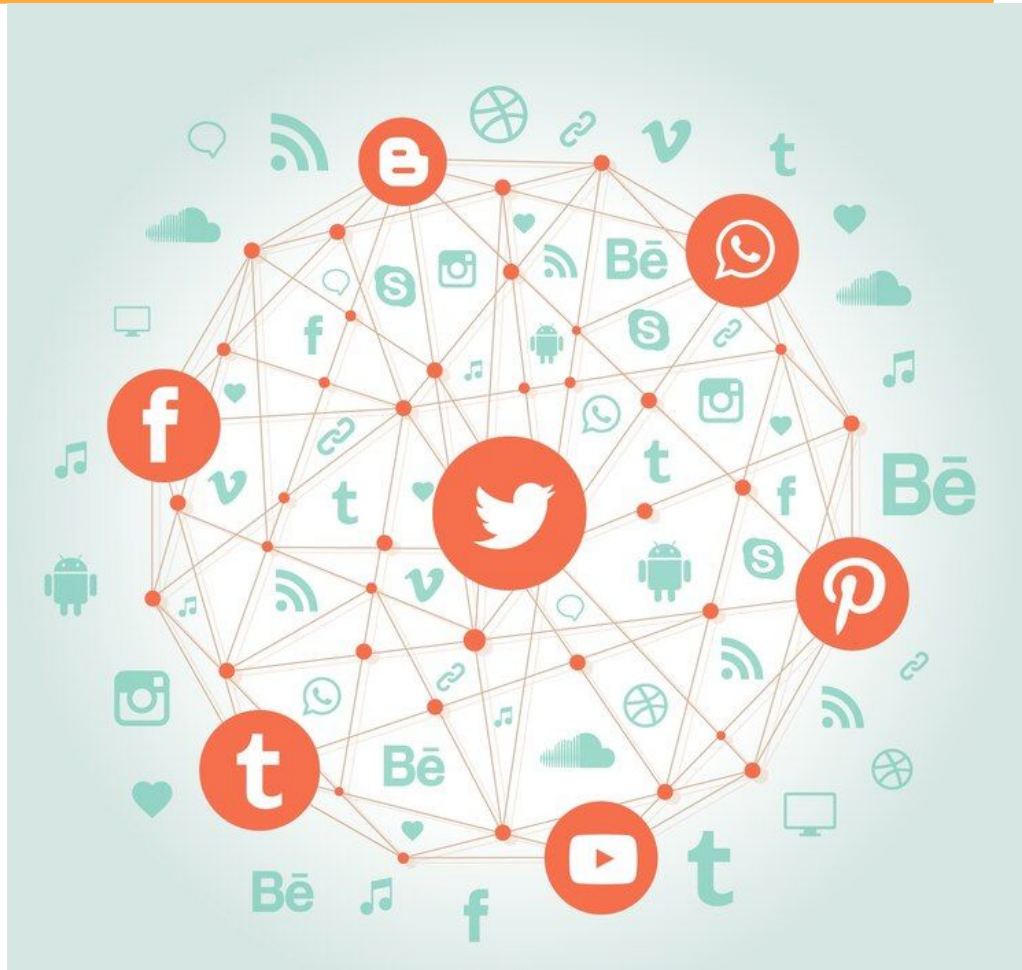


STRUMENTI DI LAVORO: SOCIAL NETWORK

Attenzione alla password.

Attenzione agli accessi alla pagina e alle autorizzazioni.

Attenzione agli accessi sospetti all’account.



STRUMENTI DI LAVORO: PIATTAFORME DI VIDEOCALL

Utilizzare le password per le riunioni (ed, eventualmente, autorizzare le iscrizioni manualmente).

UK Prime Minister Boris Johnson accidentally reveals Zoom ID for Cabinet meeting on Twitter, sparks security concerns

Prime Minister of UK Boris Johnson, who was tested positive for COVID-19, conducted his first-ever digital cabinet meeting on Zoom and shared a screenshot of the same on Twitter.

Listen to Story

Share

STRUMENTI DI LAVORO: RETI WI-FI APERTE E LIBERE

Mai utilizzare reti Wi-fi aperte e libere.

Eccellenze in Digitale

UNIONCAMERE

BEST PRACTICE GENERALI

BEST PRACTICES GENERALI: PRINCIPIO DEL MINIMO PRIVILEGIO

Concediamo **solo** gli accessi necessari: è una tutela per noi e per gli altri!

BEST PRACTICES GENERALI: ANALISI COMPORTAMENTALE

Sistemi che analizzano determinate operazioni “routinarie” dell’utente, segnalando quando ci sono azioni anomale.

BEST PRACTICES GENERALI: AUTENTICAZIONE A PIÙ FATTORI

Codici di sblocco

Impronta digitale

Riconoscimento del volto

Codici OTP

Notifiche o e-mail di avvenuto accesso

BEST PRACTICES GENERALI: BACKUP DEI DATI

Sempre avere più copie dei dati.

Programmare dei backup automatici

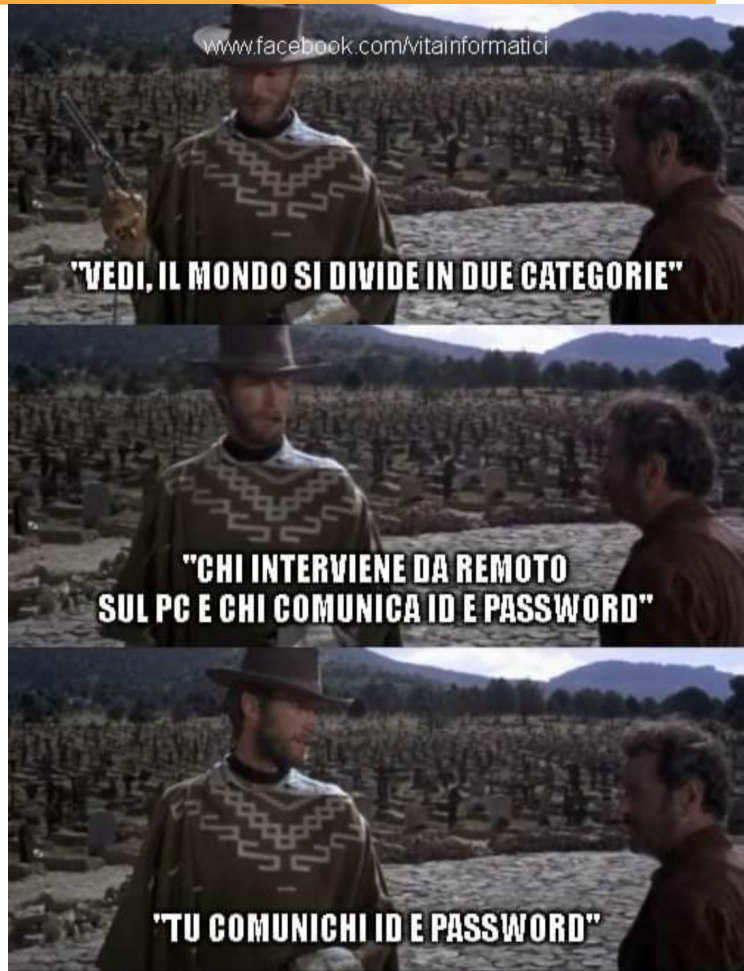
3-2-1 Backup Strategy

BEST PRACTICES GENERALI: CONDIVIDERE LE PASSWORD

Non condividere.

Se condivise, adottare delle policy.

Se “prestate”, cambiarle appena possibile.



BEST PRACTICES GENERALI: PENETRATION TEST

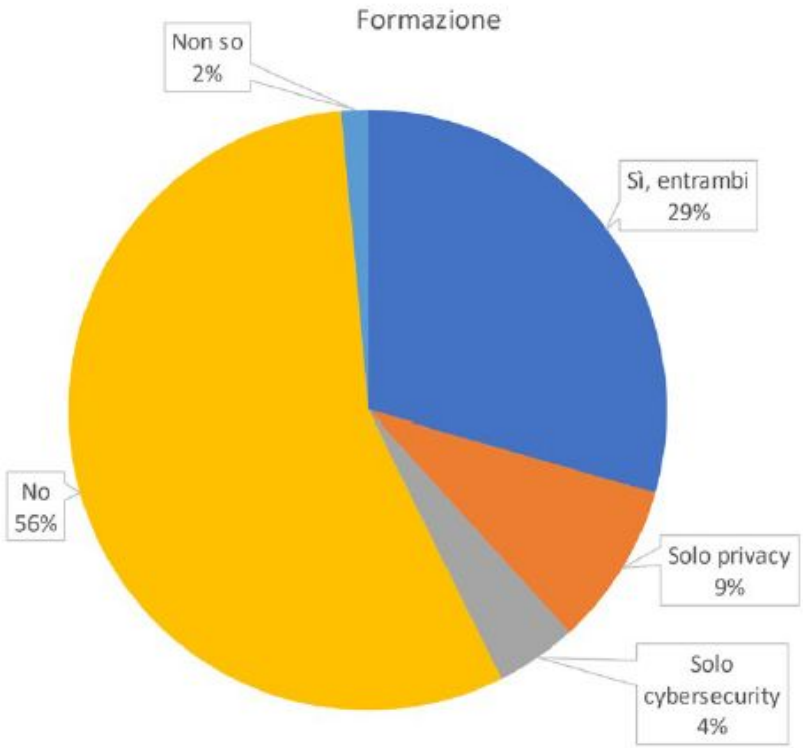
Simulazioni per capire quanto l’azienda e i dipendenti sono pronti a reggere un cyber attacco.

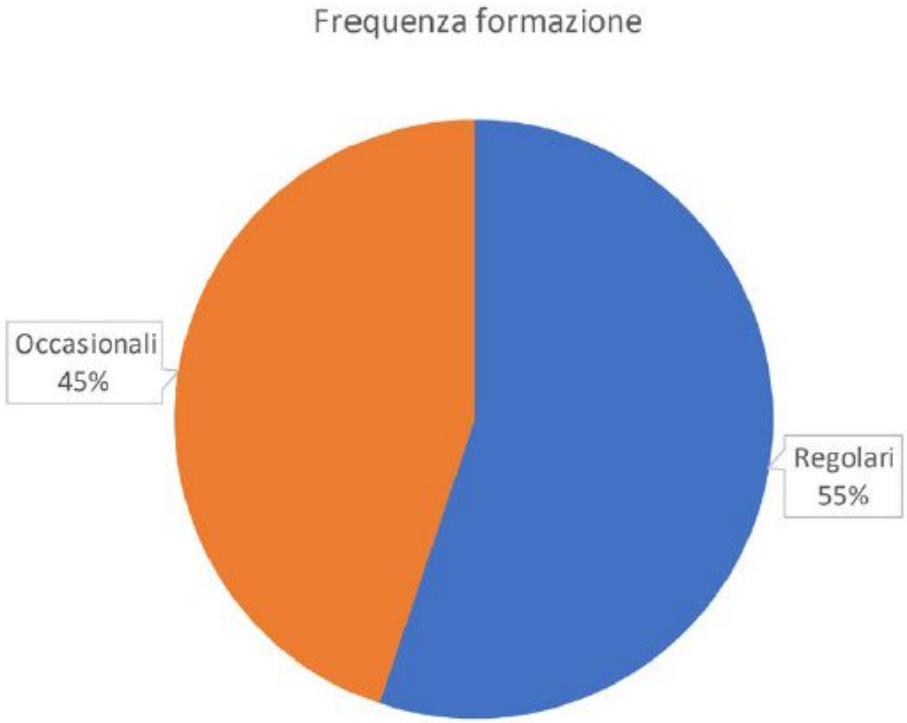
BEST PRACTICES GENERALI: FORMAZIONE

Fare formazione!!!

Fare formazione continua!!!

SOLO 1 PMI SU 6 PRESTA MOLTA ATTENZIONE AL TEMA





Fonte: Report CLUSIT 2023

PUNIZIONE O EDUCAZIONE?

Carta IT basata sul principio di non-punizione (Didier Danet).

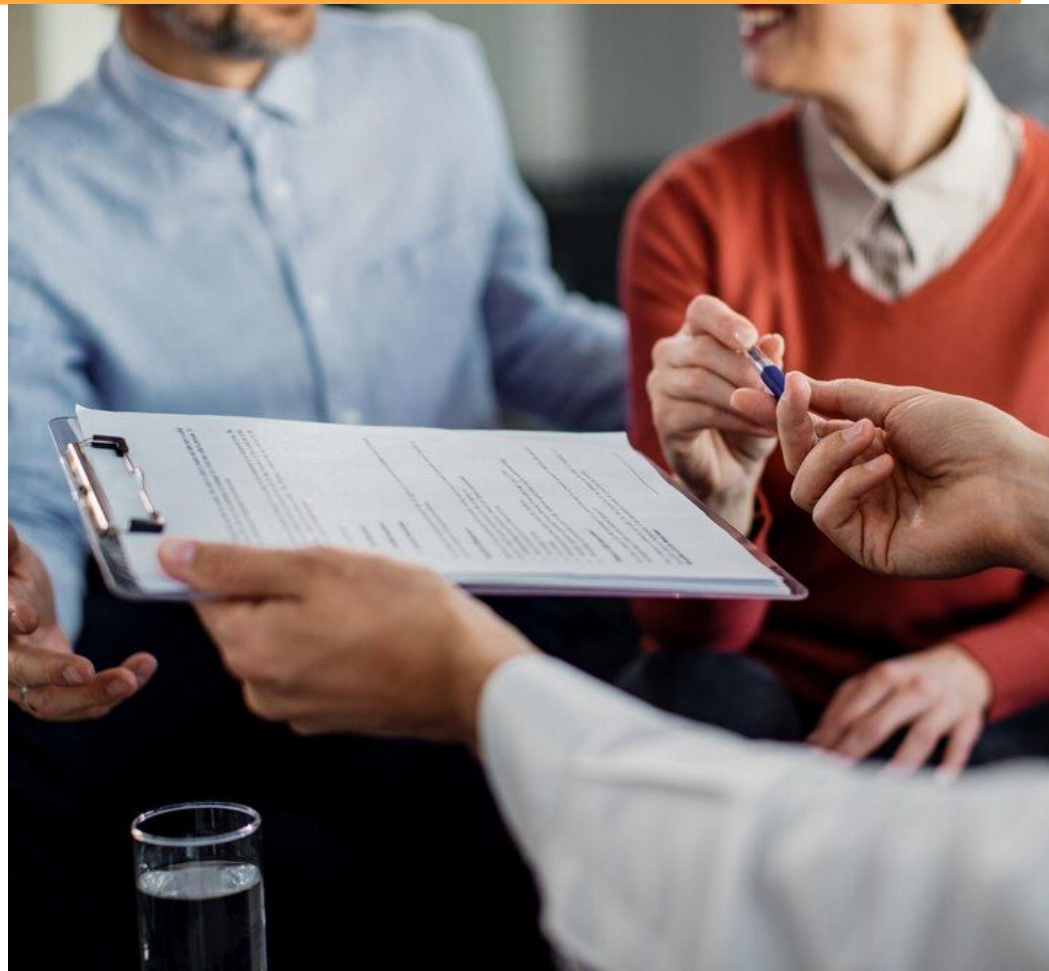
Perché?

- Difficilmente un danno è intenzionale.
- Si alimenta il silenzio per paura di colpa.

LE ASSICURAZIONI

Esistono assicurazioni che coprono danni e ripristino (ma, visti i trend, è sempre meno conveniente..).

Attenzione: non coprono le multe (andrebbero contro lo spirito della Legge!).



GDPR: PRINCIPIO DI INTEGRITÀ E RISERVATEZZA

Art. 5, paragrafo 1, lettera f del GDPR.

I dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, inclusa la protezione attraverso misure tecniche e organizzative adeguate. L'obiettivo è prevenire trattamenti non autorizzati o illeciti, nonché proteggere i dati personali dalla perdita, distruzione o danni accidentali. In altre parole, le organizzazioni sono tenute a adottare misure di sicurezza adeguate per proteggere l'integrità e la riservatezza dei dati personali che trattano.

IL CHECKUP SICUREZZA IT DEL PID: CASI REALI DELLA CCIAA

GLI ASSESSMENT SULLA CYBERSICUREZZA

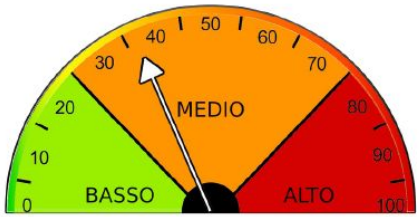
CHECKUP Sicurezza IT PID Cyber Check

CHECKUP Sicurezza IT Cyber Exposure Index

https://www.puntoimpresadigitale.camcom.it/paginainterna/assessment-checkup-sicurezza-it-imprese

IL PID CYBER CHECK

LIVELLO DI RISCHIO DI SICUREZZA INFORMATICA RILEVATO:



Livello del rischio: 37/100

Inappropriatezza del sistema/ configurazione scarsa	9710
Malware	5649
Danno Fisico	30240
Interruzione delle Comunicazioni	30
Rischio Complessivo	**275843.06 €**

l'esposizione di informazioni sensibili).

Violazione/manomissione del sistema: questa minaccia include gli attacchi che iniziano con un utente malintenzionato che ottiene l'accesso fisico agli elementi del sistema della vittima.

Inappropriatezza del sistema/configurazione scarsa: un utente malintenzionato può penetrare nel sistema sfruttandone la scarsa configurazione (ad esempio, utilizzando credenziali predefinite o ottenendo l'accesso a un archivio dati non protetto).

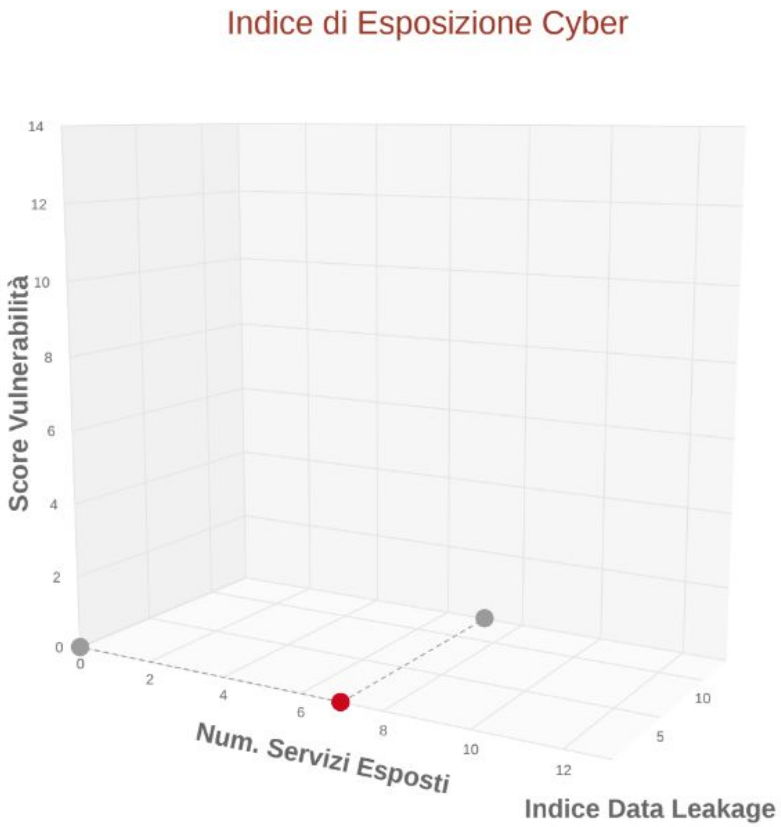
Malware: è un software progettato per causare interruzioni, divulgare informazioni riservate, ottenere accessi non autorizzati e altre azioni dannose.

Danno Fisico: danno fisico dell'hardware che provoca perdita di integrità e disponibilità delle risorse digitali.

Interruzione delle Comunicazioni: questa minaccia mira a intercettare o manomettere la comunicazione tra le parti comunicanti. Un utente malintenzionato può trovare un modo per decifrare la comunicazione (senza crittografia o con crittografia debole) o sfruttare le vulnerabilità di protocolli non sicuri.

https://www.cybersecurityosservatorio.it/Services/PIDCyberCheck.jsp?lang=it

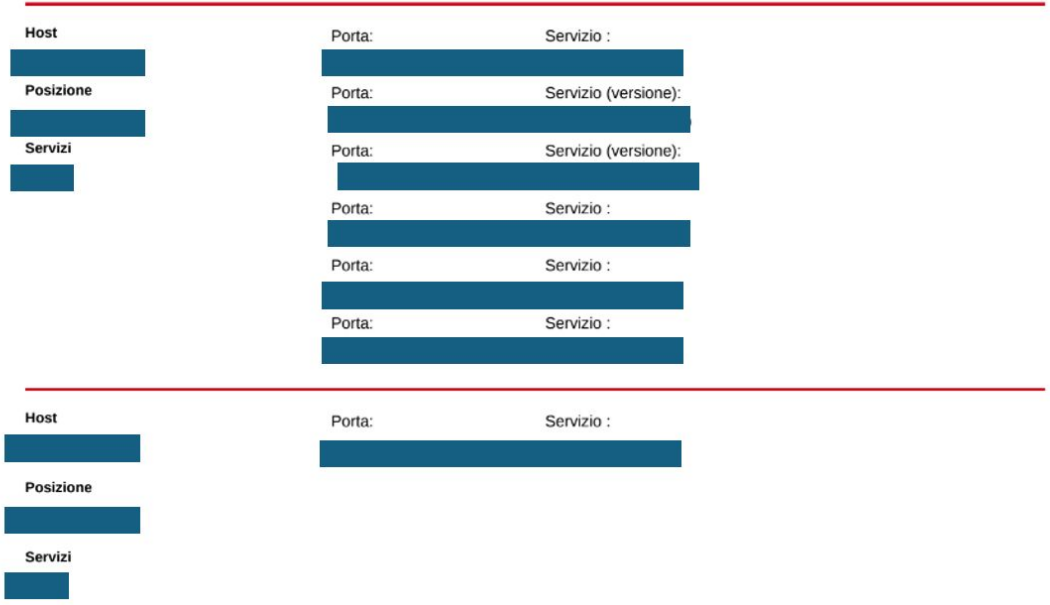
IL CYBER EXPOSURE INDEX



https://www.cybersecurity-pmi.infocamere.it/

NUMERO DI SERVIZI ESPOSTI

Numero di Servizi Esposti	7
Score delle Vulnerabilità	20*
Indice di Data Leakage	0



NUMERO DI SERVIZI ESPOSTI: RISOLTO

Numero di Servizi Esposti	3
Score delle Vulnerabilità	0
Indice di Data Leakage	87*

SCORE DELLE VULNERABILITÀ

Numero di Servizi Esposti	7
Score delle Vulnerabilità	20*
Indice di Data Leakage	0

Vulnerabilità

In questa sezione vengono rappresentati i *servizi esposti* con le annesse vulnerabilità di rete riscontrate.

Host : Porta

Posizione

Servizio (versione)

Nome:

Gravità:

Score:

Vettore di Attacco:

Data:

Descrizione:

SCORE DELLE VULNERABILITÀ: RISOLTO

Numero di Servizi Esposti	3
Score delle Vulnerabilità	0
Indice di Data Leakage	87*

INDICE DI DATA LEAKAGE

Numero di Servizi Esposti	8
Score delle Vulnerabilità	8*
Indice di Data Leakage	68*

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 06-02-2023 00:00

Passwords:

Password in Chiaro

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 24-01-2023 00:00

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 24-01-2023 00:00

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 04-11-2020 01:00

Passwords:

Hash della Password

INDICE DI DATA LEAKAGE: RISOLTO

Numero di Servizi Esposti	10
Score delle Vulnerabilità	0
Indice di Data Leakage	0

ATTENZIONE: LA SITUAZIONE PUÒ ANCHE PEGGIORARE

Servizi Esposti	2
Vulnerabilità	0
Data Leakage	5*

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 08-06-2022 00:00

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 06-05-2022 00:00

Account [redacted]

Sorgente del leak: [redacted]

Data di ultima rilevazione: 08-06-2022 00:00

Account [redacted]

Sorgente del leak: [redacted]

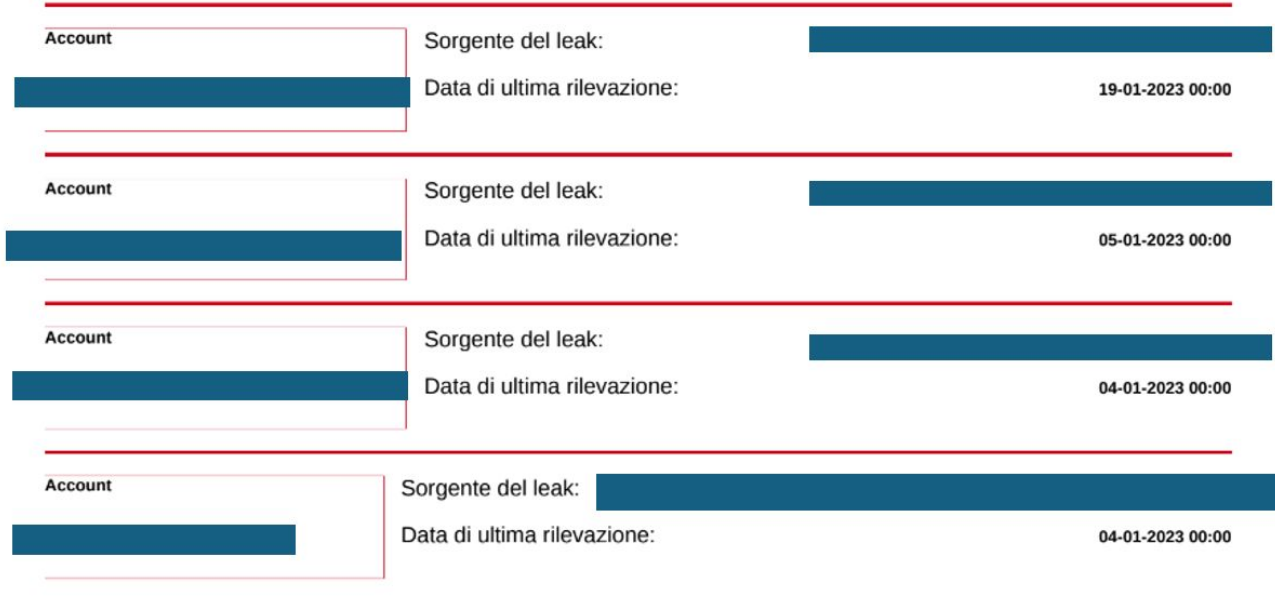
Data di ultima rilevazione: 16-12-2016 01:00

Passwords:

Password in Chiaro

ATTENZIONE: LA SITUAZIONE PUÒ ANCHE PEGGIORARE

Numero di Servizi Esposti	2
Score delle Vulnerabilità	0
Indice di Data Leakage	7*



IN CONCLUSIONE

IN CONCLUSIONE

Chiedere ad un tecnico di assicurare che non ci siano problemi
è come chiedere a un meccanico di assicurarci che non faremo mai incidenti:
lui può assicurarci che i freni frenino, ma il piede sul pedale chi ce lo mette?

IN CONCLUSIONE

Di più, nonostante tutte le precauzioni siamo responsabili per noi, non per quello che fanno gli altri.

Ma andare ai 60 all’ora invece che ai 100 farà si che in caso di incidente

si potrà magari parlare solo di un cofano da aggiustare, e non di una persona da operare.

IN CONCLUSIONE

Spesso (molto spesso) siamo uno dei migliori strumenti di difesa!

GRAZIE! Ci vediamo al prossimo incontro:

~~**Strumenti digitali della CCIAA >** giovedì 14 marzo 2024~~

~~**Cybersecurity >** mercoledì 20 marzo 2024~~

Sostenibilità > mercoledì 27 marzo 2024

Il Cloud di Google > mercoledì 17 aprile 2024

Il sito web con Google > mercoledì 24 aprile 2024

AI Generativa > mercoledì 22 maggio 2024

Storytelling > mercoledì 29 maggio 2024

RISORSE UTILI

UTILI PER APPROFONDIMENTI:

- Rapporto Clusit sulla sicurezza ICT in Italia
- Guida alla cybersicurezza per le piccole e medie imprese. 12 azioni per rendere sicura la propria impresa (Enisa).
- Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci! (Giorgio Sbaraglia).

IMMAGINI:

- Pixabay
- Freepick

Eccellenze in Digitale
UNIONCAMERE con il supporto di Google.org

punto impresa digitale

CAMERA DI COMMERCIO
MONTE ROSA LAGHI
ALTO PIEMONTE

RESTIAMO IN CONTATTO


Camera di Commercio Monte Rosa Laghi Alto Piemonte


CamCom Monte Rosa Laghi Alto Piemonte


Camera di Commercio Monte Rosa Laghi Alto Piemonte


pid@pno.camcom.it


Sito Camera di Commercio Monte Rosa Laghi Alto Piemonte


Michela Petrera


Giulia Bernini


Nicolò Mora