SICUREZZA INFORMATICA DEI SOCIAL NETWORK

Di Enrico Mancini

LA RETE COS'E'?

1969

Internet, prima di essere chiamata così, era nata nel 1969, si chiamava ancora Arpanet, dal nome dell'agenzia di ricerca americana che l'aveva progetta, l'Arpa (Advanced Research Project Agency) e aveva cominciato a usare i protocolli che ancora la fanno funzionare, cioè il TCP/IP (transfer Control Protocol/Internet)

LA RETE COS'E'?

I protocolli di rete

SCTP

HTTP

OSPF

RSVP

NBF

BGP

TCP e UDP

SNA

NDP

EIGRP

FTP

ARP

IGMP

ICMP

IPX

DCCP

LA RETE A COSA SERVE?

LA RETE: LE APP

#1 App per il lifestyle:

Fitness ..Incontri …Cibo …Musica …Viaggi

#2 App per i social network

Facebook …Instagram …Pinterest …Snapchat

#3 App utility

WhatsApp …Telegram …Promemoria …calcolatrice …torcia …meteo

#4 App di produttività

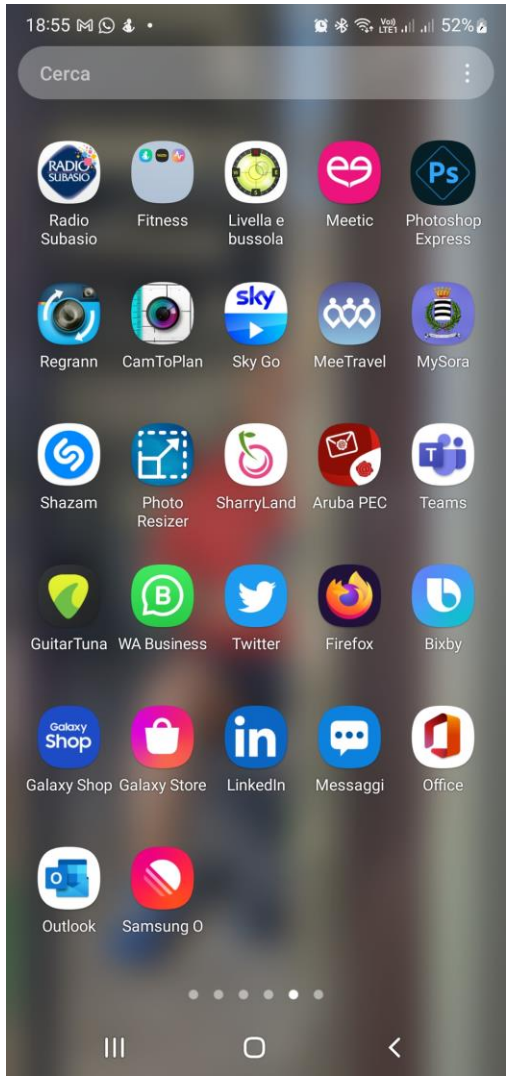
Docs …Sheets …Posta elettronica …PEC

#5 App di giochi/divertimento

#6 App aggregatrici di news/informazioni

LE APP: I Social Network

LE APP: I Social Network



I DEVICE: GLI SMARTPHONE

www.unionepolizialocaleitaliana.it

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

Anni 60 Arizona - “Miranda_warning”

“Hai il diritto di rimanere in silenzio.
Tutto quello che dici può essere
usato contro di te in tribunale.
Hai il diritto di parlare con un avvocato”.

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

I nostri dati possono diventare una minaccia per noi stessi

Oltre il **90%** degli attacchi informatici sono veicolati attraverso **l'e-mail**, che continua ad essere lo strumento di comunicazione più utilizzato, con oltre 300 miliardi di e-mail inviate ogni giorno nel mondo.

L'e-mail è utilizzata come vettore d'attacco soprattutto attraverso il **Phishing** e in modo ancora più efficace attraverso lo **spear phishing**, che è invece un attacco mirato ("spear" significa fiocina, quindi il pescatore vuole prendere proprio "quel" pesce).

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

I nostri dati possono diventare una minaccia per noi stessi

L'oggetto dell'attacco viene accuratamente selezionato e studiato (oggi è molto facile raccogliere informazioni su una persona, attraverso i social e il web). Gli attaccanti acquisiscono una profonda conoscenza delle vittime e le e-mail inviate sono preparate ad hoc per catturarne l'attenzione ed indurle in errore.

Ma molto, troppo spesso, è la vittima stessa a fornire – più o meno inconsapevolmente – queste informazioni all'attaccante.

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

I nostri dati possono diventare una minaccia per noi stessi

Il potenziale di attacco è ancora maggiore grazie alle frequenti violazioni di dati personali, quali il **data leak che ha colpito recentemente Facebook**:
I numeri di telefono e molte altre informazioni personali di circa **533 milioni** di utenti del social in tutto il mondo sono stati divulgati gratuitamente su un popolare forum di hacking; tra questi utenti, **circa 36 milioni** erano italiani (in pratica circa il 90% di tutti gli utilizzatori di Facebook nel nostro Paese).

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

I nostri dati possono diventare una minaccia per noi stessi

Vengono raccolte e aggregate le informazioni personali che gli utenti pubblicano spontaneamente sui propri profili social (***numero di telefono cellulare, sesso, città e data di nascita, profilo lavorativo, relazioni sentimentali, indirizzi email ecc.***).
Con una dotazione di informazioni così ampia, un attaccante sarà in grado di confezionare un attacco mirato, efficace perché estremamente credibile.

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

I nostri dati possono diventare una minaccia per noi stessi

È importante acquisire la consapevolezza che i social media rappresentano una delle principali fonti di raccolta di informazioni per le attività di **OSINT (Open Source INTelligence),** che sono propedeutiche a un attacco. Non parliamo di password che ci vengono rubate con tecniche più o meno sofisticate, ma dei dati che siamo noi stessi a "**regalare**" alla Rete.

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

Pensiamoci due volte prima di pubblicare qualcosa

Molte persone espongono su Facebook la propria data di nascita, per avere poi tanti messaggi di auguri via social nel giorno del proprio compleanno, messaggi da persone che si conoscono appena.
Ma una campagna mirata di **spear phishing** o **smishing** (**acronimo di SMS phishing**) sarà assai più convincente nel farci cliccare sul link infetto o fraudolento se l'attaccante conosce la nostra data di nascita o il nostro codice fiscale (che può essere abbastanza facilmente ricostruito conoscendo la data di nascita, appunto, e poche altre informazioni).

Meta

www.unionepolizialocaleitaliana.it

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

Non pubblichiamo informazioni private

E ancora, smettiamo di pubblicare informazioni private su piattaforme social pubbliche: programmi di viaggio, interessi personali, dettagli sui membri della famiglia o notizie sulla nostra attività lavorativa.
Tutte queste informazioni possono essere usate per guadagnare la nostra fiducia e ingannare noi o i nostri colleghi o amici. Per esempio, un **criminal hacker** potrebbe scoprire le storie personali dai nostri social media, quindi inviare un'e-mail di phishing che dice qualcosa come: "**Congratulazioni per il tuo nuovo lavoro**" O anche: "**Mi dispiace per la morte del tuo genitore, lo conoscevo bene**".
Anche i più piccoli dettagli, che malintenzionati sicuramente riusciranno ad aggregare dalle piattaforme social, possono essere rivelatori di cose delle nostra vita.

Meta

www.unionepolizialocaleitaliana.it

I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

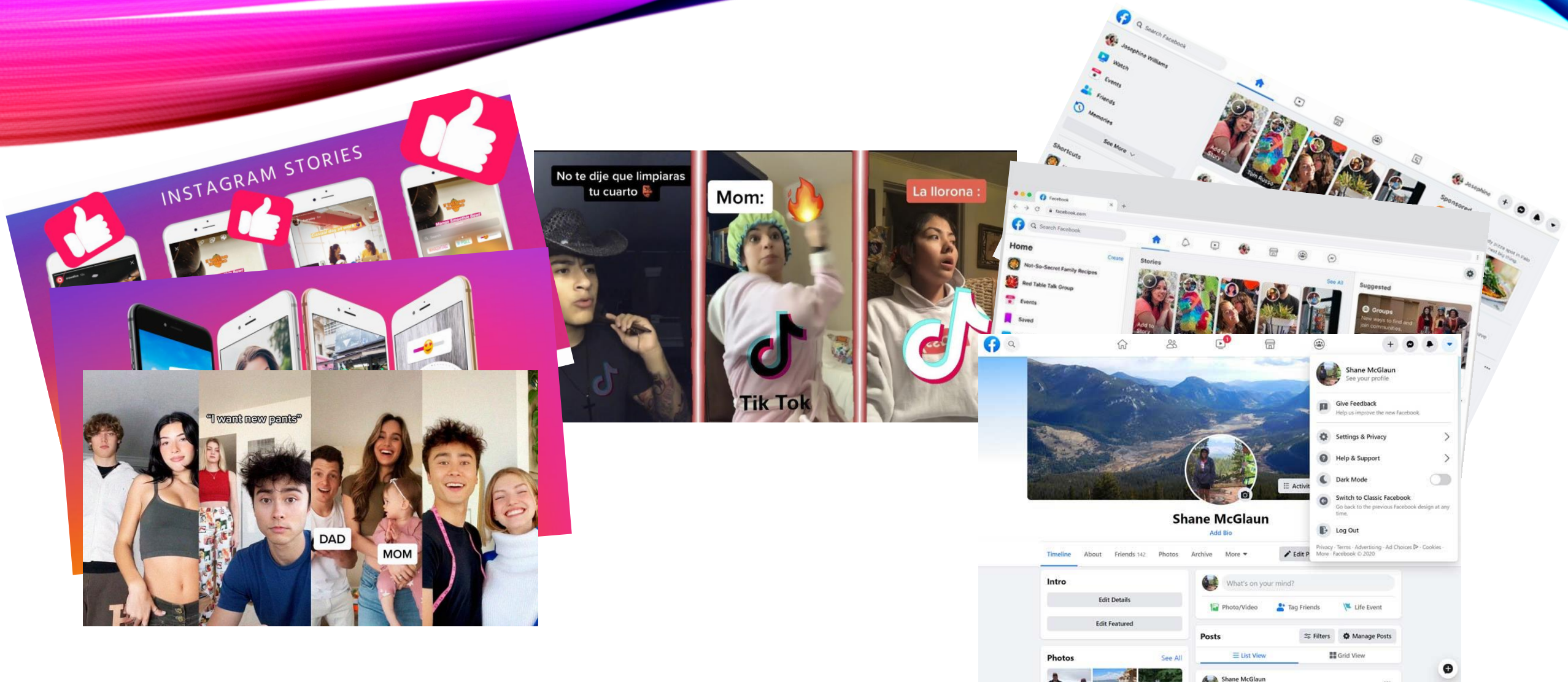
Usiamo diverse immagini di profilo sulle piattaforme social

Le attività di **OSINT** e di **acquisizione** di informazioni attraverso il web vengono fatte in modo automatico, con **tool software** che utilizzano anche **AI (Intelligenza Artificiale)** e riescono così rapidamente a correlare i vari account dei social media alla ricerca di corrispondenze tra le immagini del profilo, così come altre caratteristiche comuni **(nome utente, amici, città, interessi)**.
Per esempio, se qualcuno usa la stessa immagine del profilo su **Instagram** e **Facebook**, l'IA potrà dedurre che gli account appartengono alla stessa persona, anche se i nomi utente sono diversi. Gli attaccanti possono quindi ad aggregare un'enorme quantità di informazioni su di noi, da usare per attaccarci o per impersonarci più efficacemente.

Meta

ETHICA SOCIETAS UPLI

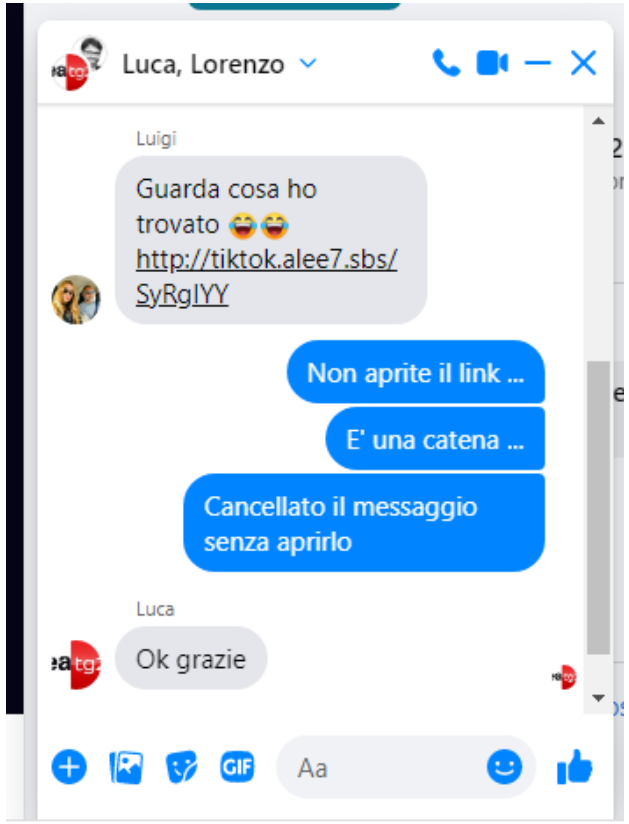
www.unionepolizialocaleitaliana.it

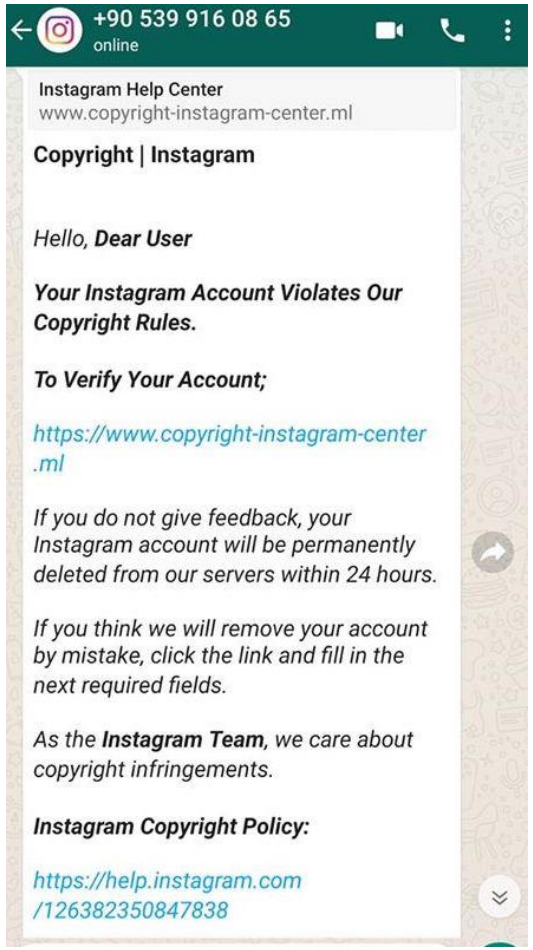


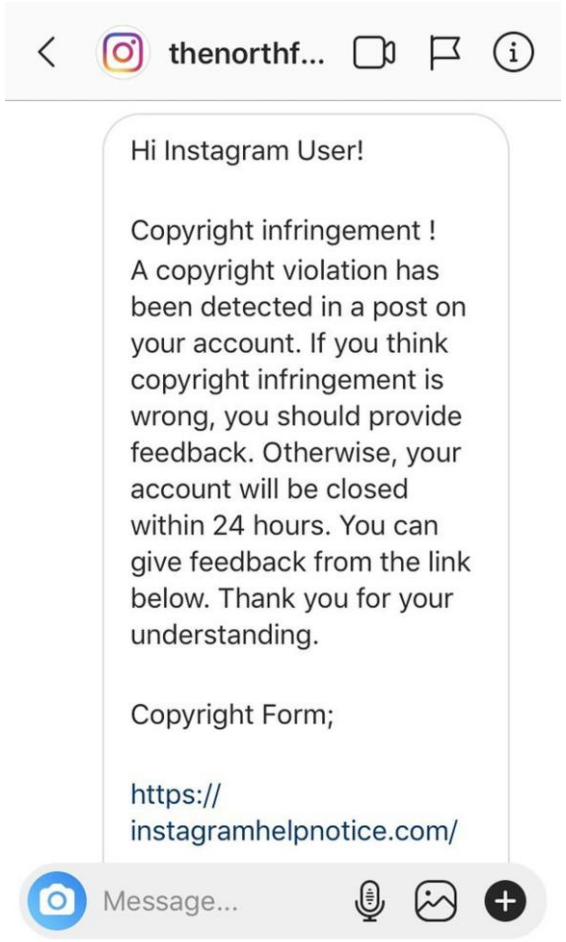
LE APP: I Social Network

www.unionepolizialocaleitaliana.it

SICUREZZA: PHISHING







SICUREZZA: PHISHING

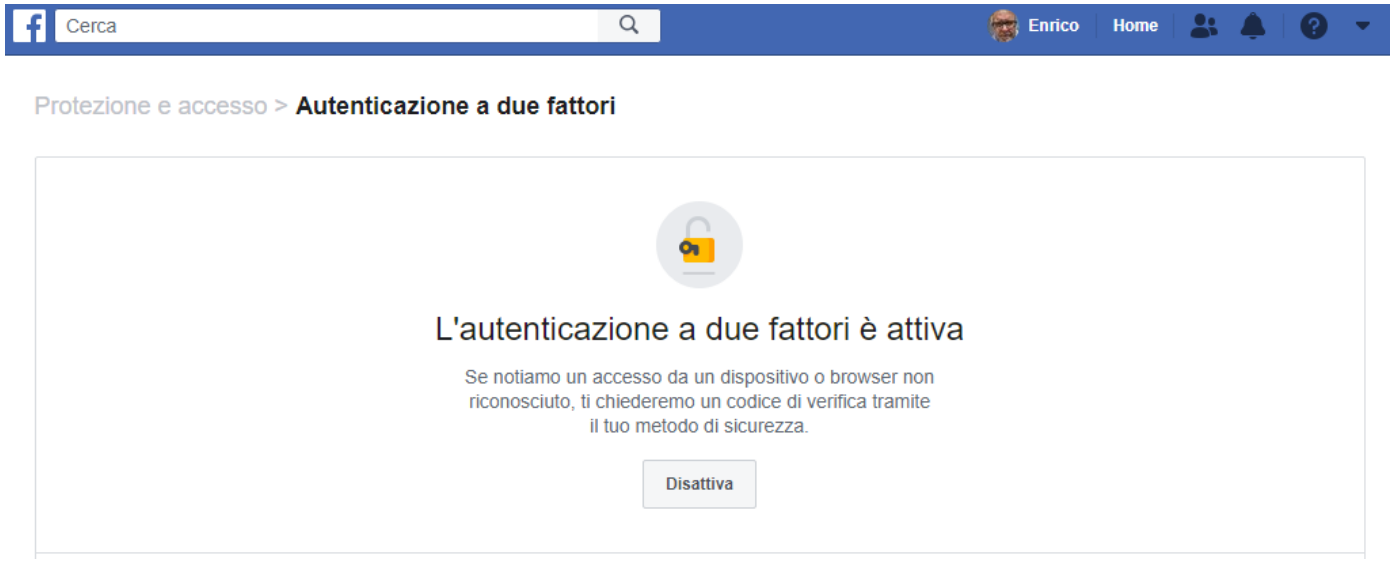
www.unionepolizialocaleitaliana.it

Meta

SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

ETHICA SOCIETAS UPLI

www.unionepolizialocaleitaliana.it

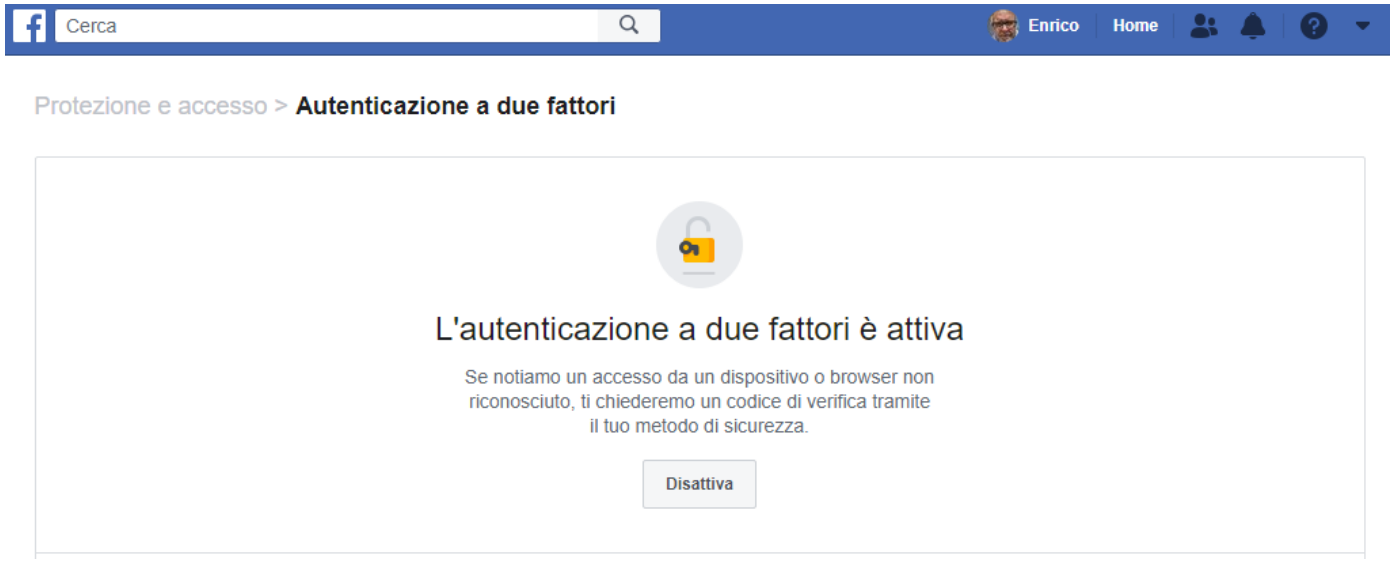


Meta

SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

ETHICA SOCIETAS UPLI

www.unionepolizialocaleitaliana.it

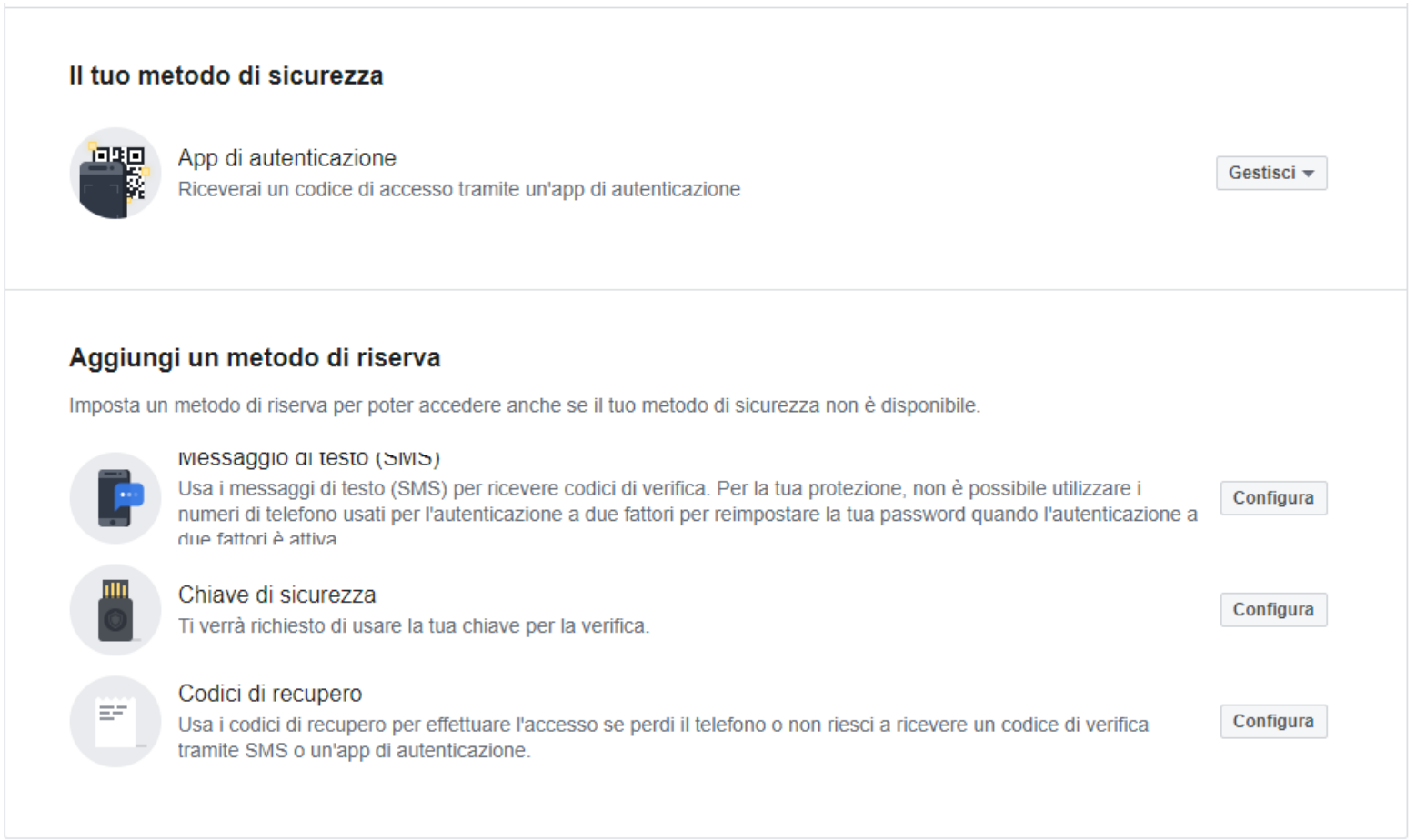


Meta

SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

ETHICA SOCIETAS UPLI

www.unionepolizialocaleitaliana.it



SICUREZZA: AUTHENTICAZIONE A DUE FATTORI