

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 progettata, 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
TCP e UDP BGP SNA
NDP
EIGRP
IGMP ICMP FTP ARP
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

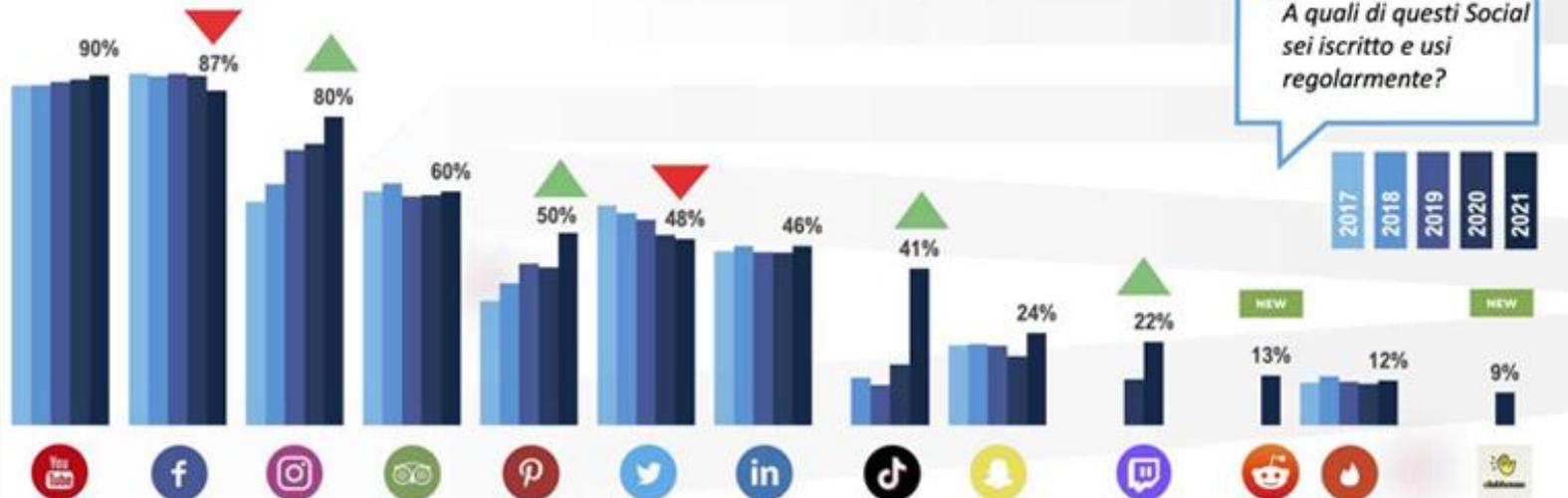
#6 App aggregatrici di news/informazioni



LE APP: I Social Network

IL SORPASSO DI FACEBOOK, L'IMPENNATA DI TIKTOK, LA CRESCITA DI INSTAGRAM E TWITCH, E LA 'METEORA' DI CLUBHOUSE

% utilizzatori social



A quali di questi Social sei iscritto e usi regolarmente?



ASSIRM
Ricerca. Conoscenza. Futuro.

MRF21
MARKETING RESEARCH FORUM

blogmeter
INTEGRATED SOCIAL INTELLIGENCE

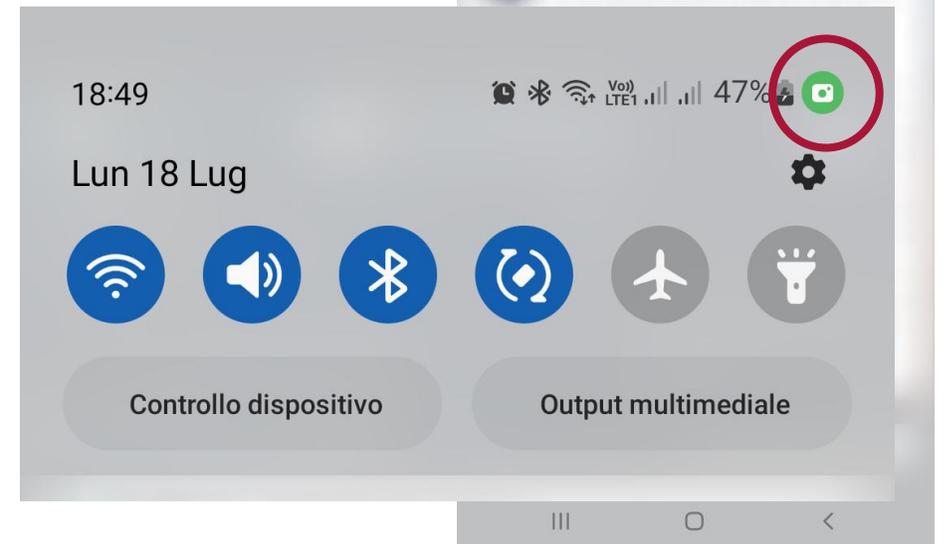
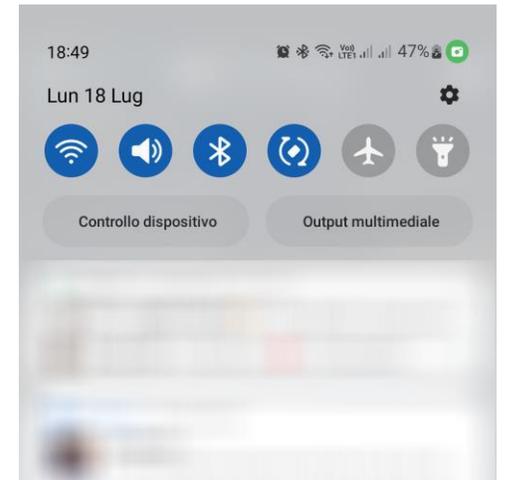
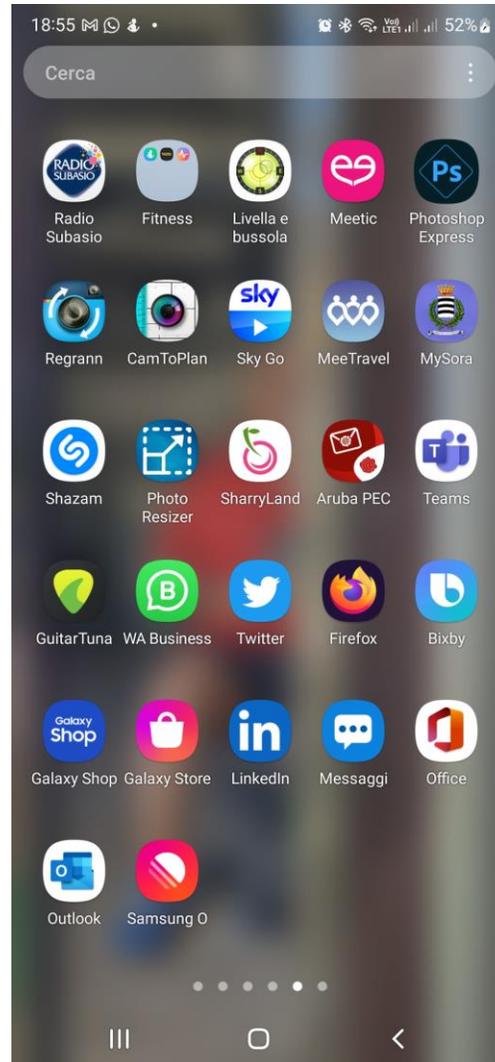
Base: 2017 N=1501 / 2018 N=1500 / 2019 N=1510 / 2020 N=1462 / 2021 N=1490 15-64enni
Iscrizione ad almeno un social/messenger



www.unionepolizialeitaliana.it

LE APP: I Social Network





I DEVICE: GLI SMARTPHONE

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.

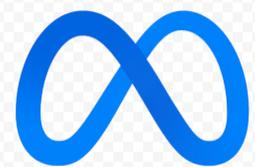


I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

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



I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

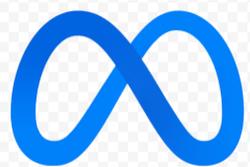
Non pubblichiamo informazioni private

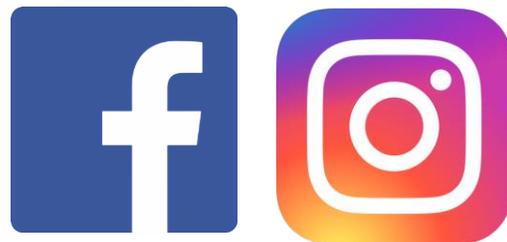
E ancora, smettiamo di pubblicare informazioni private su piattaforme social pubbliche: programmi di viaggio, interessi personali, dettagli sui membri della famiglia o notizie sulla nostra attività lavorativa.

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 della nostra vita.



 Meta



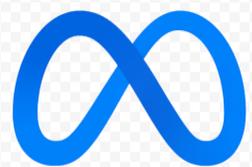
I SOCIAL: ATTENTI A QUELLE CHE PUBBLICHIAMO

Usiamo diverse immagini di profilo sulle piattaforme social

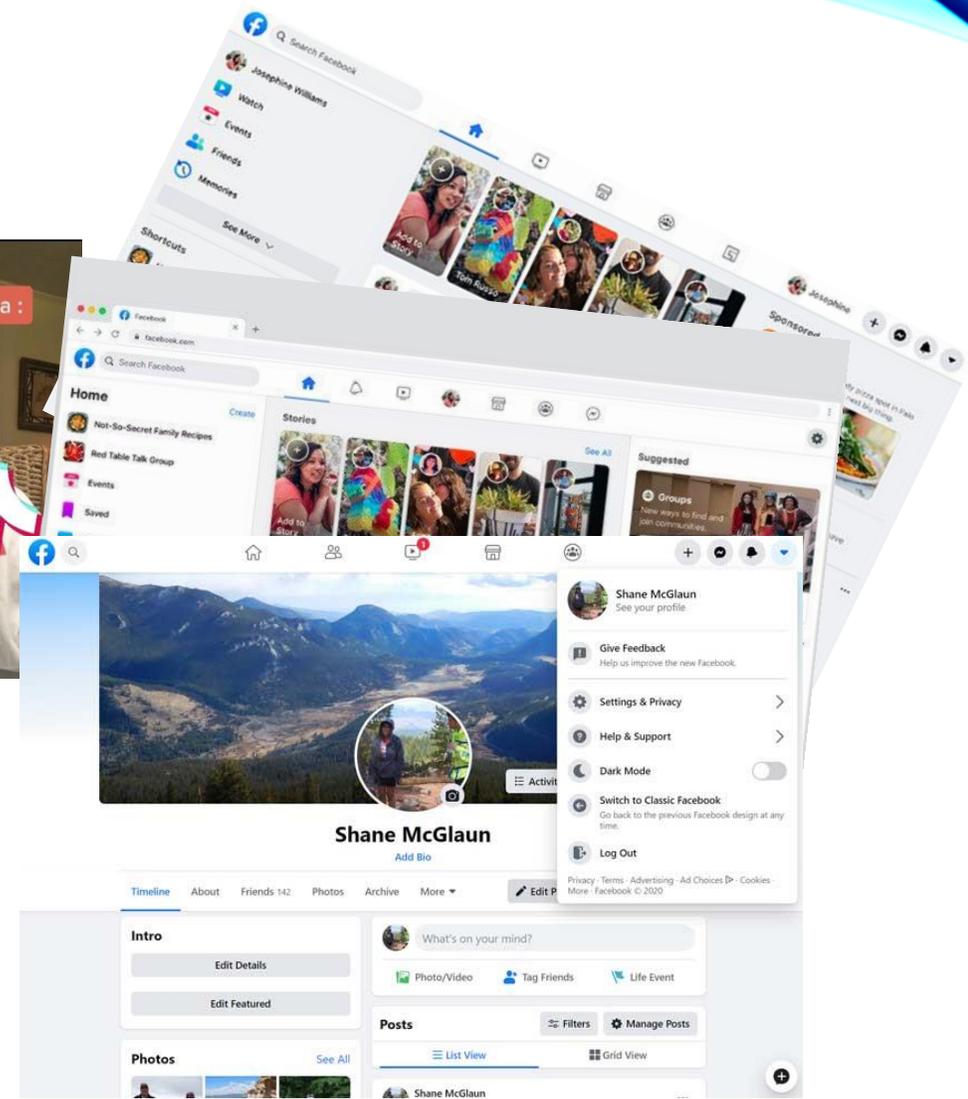
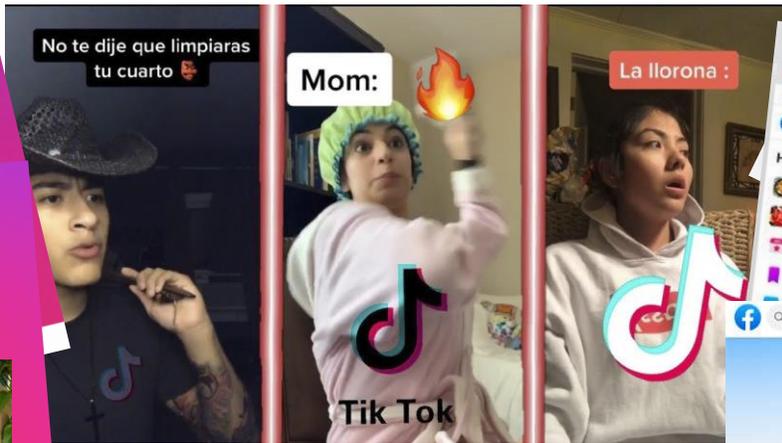
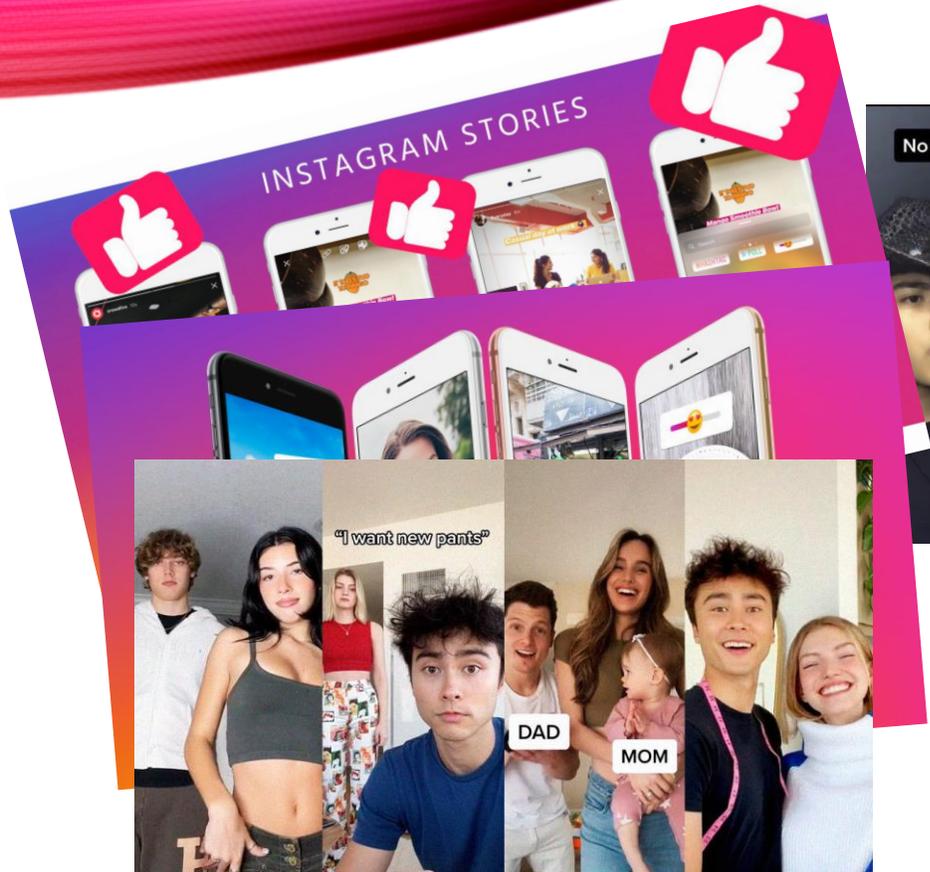
Le attività di **OSINT** e di **acquisizione** di informazioni attraverso il web vengono fatte in modo automatico, con **tool software** che utilizzano anche **AI (Intelligenza Artificiale)** e riescono così rapidamente a correlare i vari account dei social media alla ricerca di corrispondenze tra le 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





LE APP: I Social Network

20:26

< Banca MPS



Giovedì 13 Maggio 2021



Sistema Iosicuro
E stata richiesta un autorizzazione di spesa per euro di 251,78 se non e stata lei seguire il seguente link <https://mpsopen.me/accedi/>

18:39

aruba.it
THE WEB COMPANY

Gentile Cliente,

Si prega di notare che il rinnovo è stato respinto nonostante diverse richieste da parte nostra.

Affrontiamo sempre il rifiuto con la sua banca quando tentiamo di addebitare i costi dell'ultimo rinnovo dei suoi servizi che ammontano a 6,11 €.

COME RINNOVARE?

Vi invitiamo comunque a compilare manualmente il modulo di rinnovo dei vostri servizi seguendo le istruzioni sul link qui sotto.

<https://www.aruba-pagamento-sys.com>
Fare clic o toccare per aprire il collegamento.

ACCEDETE AL VOSTRO MODULO DI PAGAMENTO

CHE COSA ACCADE SE NON RINNOVI?

Vi invitiamo comunque a compilare manualmente il modulo di rinnovo dei vostri servizi seguendo le istruzioni sul link qui sotto.

<https://www.aruba-pagamento-sys.com>
Fare clic o toccare per aprire il collegamento.

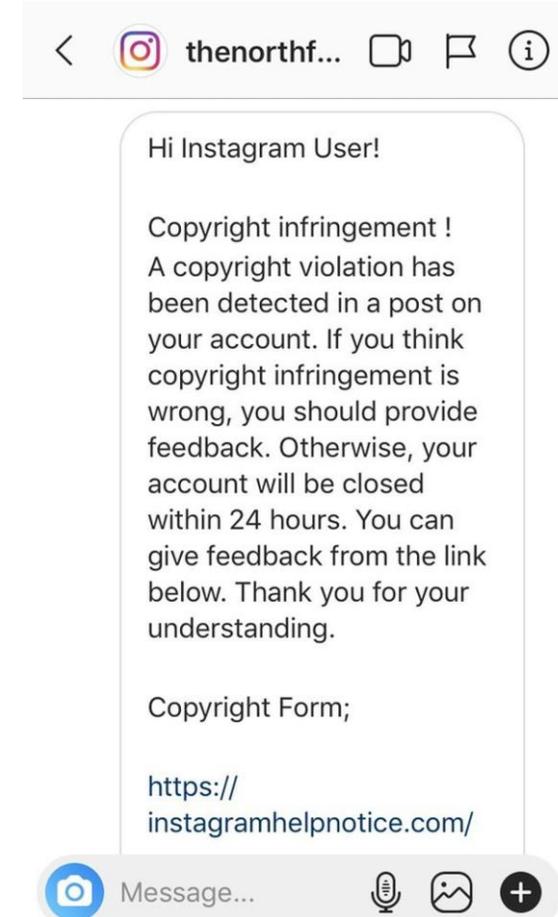
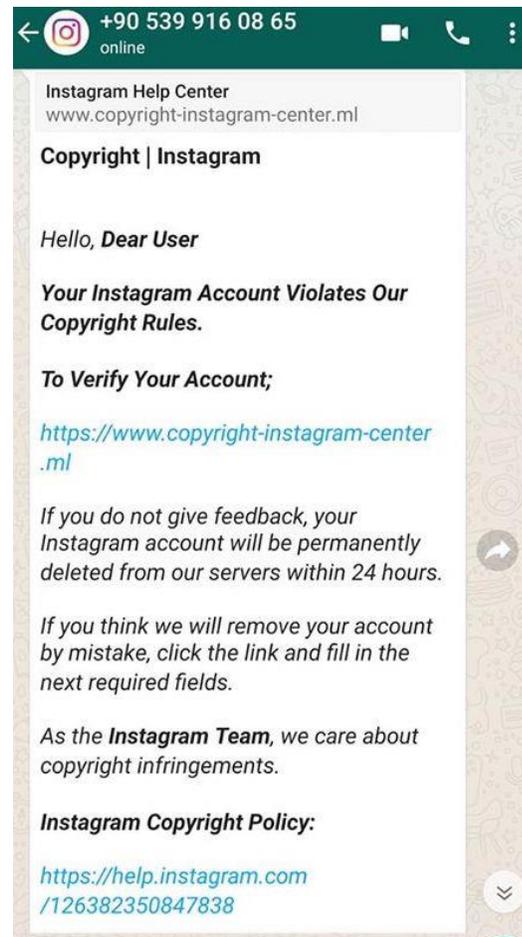
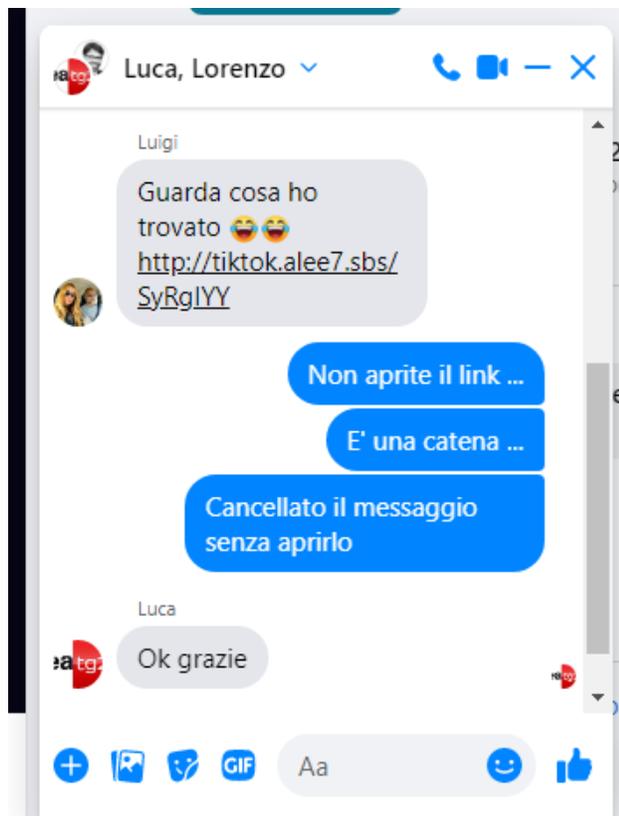
ACCEDETE AL VOSTRO MODULO DI PAGAMENTO

CHE COSA ACCADE SE NON RINNOVI?

SICUREZZA: PHISHING



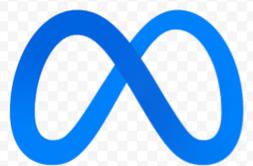
www.unionepolizialeitaliana.it



SICUREZZA: PHISHING





 Meta

SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

Dove hai effettuato l'accesso

- PC Windows · Sora, Italy
Chrome · **Sessione attiva ora**
- Samsung Galaxy S22 Ultra 5G · Sora, Italy
App Facebook · 17 ore fa

Mostra altro

Accesso

- Modifica password
Ti consigliamo di usare una password sicura che non utilizzi altrove [Modifica](#)
- Salva le tue informazioni di accesso
Le tue informazioni saranno salvate solo sui browser e dispositivi che scegli [Modifica](#)

Autenticazione a due fattori

- Usa l'autenticazione a due fattori
Si • Se rileviamo un tentativo di accesso da un dispositivo o browser non riconosciuto, ti chiederemo un codice. [Modifica](#)
- Accessi autorizzati
Analizza una lista di dispositivi dove non dovrai usare un codice di accesso [Visualizza](#)



SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

Configurazione di una funzione di protezione aggiuntiva



Ricevi avvisi sugli accessi non riconosciuti

Si • Ti comunicheremo se qualcuno accede da un dispositivo o browser che non usi di solito

Modifica

Avanzate



E-mail di notifica crittografate

Aumenta il livello di sicurezza delle e-mail di notifica di Facebook (solo tu puoi decrittografare queste e-mail)

Modifica



Vedi le e-mail recenti da Facebook

Vedi una lista di e-mail che ti abbiamo inviato di recente, comprese le e-mail relative alla sicurezza

Visualizza



Cerca



Enrico

Home



Protezione e accesso > Autenticazione a due fattori



L'autenticazione a due fattori è attiva

Se notiamo un accesso da un dispositivo o browser non riconosciuto, ti chiederemo un codice di verifica tramite il tuo metodo di sicurezza.

Disattiva



www.unionepolizialeitaliana.it



SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

Configurazione di una funzione di protezione aggiuntiva



Ricevi avvisi sugli accessi non riconosciuti

Si • Ti comunicheremo se qualcuno accede da un dispositivo o browser che non usi di solito

Modifica

Avanzate



E-mail di notifica crittografate

Aumenta il livello di sicurezza delle e-mail di notifica di Facebook (solo tu puoi decrittografare queste e-mail)

Modifica



Vedi le e-mail recenti da Facebook

Vedi una lista di e-mail che ti abbiamo inviato di recente, comprese le e-mail relative alla sicurezza

Visualizza



Cerca



Enrico

Home



Protezione e accesso > Autenticazione a due fattori



L'autenticazione a due fattori è attiva

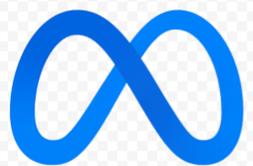
Se notiamo un accesso da un dispositivo o browser non riconosciuto, ti chiederemo un codice di verifica tramite il tuo metodo di sicurezza.

Disattiva



www.unionepolizialeitaliana.it



 Meta

SICUREZZA: AUTHENTICAZIONE A DUE FATTORI

Il tuo metodo di sicurezza



App di autenticazione

Riceverai un codice di accesso tramite un'app di autenticazione

Gestisci ▾

Aggiungi un metodo di riserva

Imposta un metodo di riserva per poter accedere anche se il tuo metodo di sicurezza non è disponibile.



Messaggio di testo (SMS)

Usa i messaggi di testo (SMS) per ricevere codici di verifica. Per la tua protezione, non è possibile utilizzare i numeri di telefono usati per l'autenticazione a due fattori per reimpostare la tua password quando l'autenticazione a due fattori è attiva

Configura



Chiave di sicurezza

Ti verrà richiesto di usare la tua chiave per la verifica.

Configura



Codici di recupero

Usa i codici di recupero per effettuare l'accesso se perdi il telefono o non riesci a ricevere un codice di verifica tramite SMS o un'app di autenticazione.

Configura



www.unionepolizialeitaliana.it