Lezione 22 08/05/2025

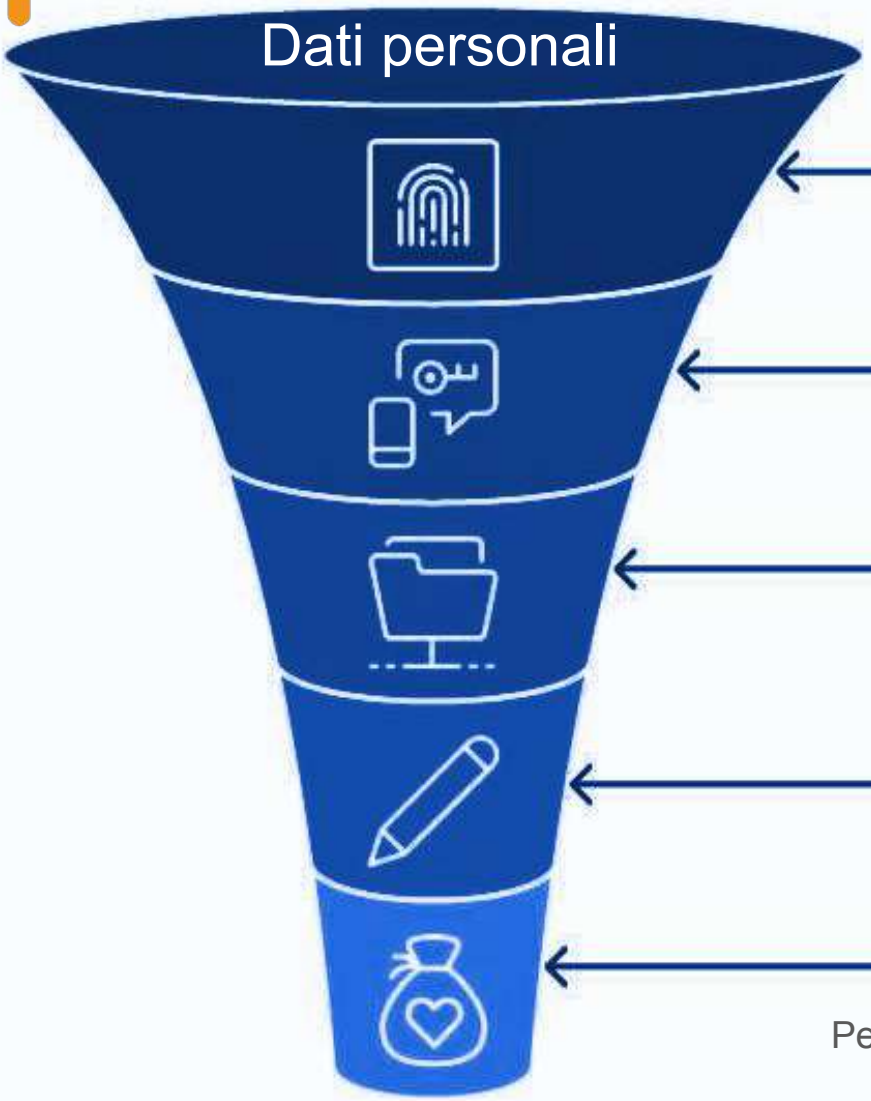
Truffe

Corso android per smartphone

Docenti Dott.ssa Roberta Lai Ing. Massimo Terrosu

cadadie.it

Truffa del doppio SPID: come funziona



Clonazione Identità

Raccolta dati sensibili (CI, TS, selfie, su social /web tramite phishing e/o dark web)

Attivazione Secondo SPID

All’insaputa dell'utente. Le PA permettono due SPID con stesso CF ma diverso numero telefono e Mail

Accesso ai Portali

Entrata nei sistemi governativi (INPS, Agenzia delle Entrate, Sistema Sanitario

Modifica Dati

In particolare l’IBAN

Dirottamento Fondi

Pensione, rimborsi 730, firma digitale documenti, attivazione abbonamenti, apertura conti correnti….

Truffa del doppio SPID: come proteggersi

- **Consapevolezza e Vigilanza.**
- **Autenticazione a Due Fattori (2FA.)**
- **Verifica Periodica degli IBAN.** Registrarsi su portali pubblici per rilevare eventuali variazioni.
- **Gestione cauta dei Dati e delle comunicazioni.** Accedere sempre ai siti ufficiali digitando l'indirizzo direttamente nel browser.
- **Monitoraggio degli Account e Password Sicure.** Utilizzare password complesse e uniche per ogni servizio.
- **Segnalazione di Attività Sospette legate al furto di identità.** Rivolgersi alla Polizia Postale e all'AgID (Agenzia per l'Italia Digitale).
- **Monitoraggio del Conto Corrente.** Nei mesi successivi a un presunto furto di dati attivando gli alert bancari
- **Verificare periodicamente gli SPID attivi a proprio nome.** Controllare sul sito dell'Agenzia per l'Italia Digitale (AgID) quali identità digitali risultano attive a proprio nome e segnalare eventuali anomalie. La segnalazione all'AgID può contribuire al blocco del secondo SPID fraudolento.

Truffa del doppio SPID: cosa fare se si è vittima della truffa

- **Sporgere immediatamente denuncia alla Polizia Postale.** Tramite il commissariato di Polizia Postale online
- **Avvisare tempestivamente l'Identity Provider (gestore dell'identità digitale) che ha rilasciato le credenziali SPEED.** Cambiare subito la password di SPID per impedire a chi ha commesso la truffa di continuare a utilizzarla.
- **Bloccare immediatamente le carte coinvolte e contattare la propria banca.**
- **Monitorare attentamente i movimenti del proprio conto corrente anche nei mesi successivi.**
- **Altroconsumo fornisce una lettera di reclamo per richiedere il rimborso alla banca.**
- **Agire rapidamente.**

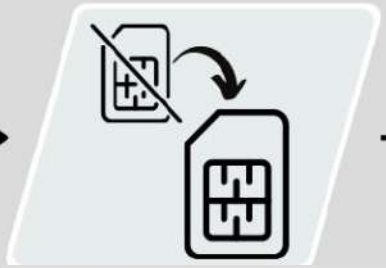
Truffa dello SIM Swapping

- **Mezzo di attacco**: I truffatori convincono l'operatore telefonico a trasferire il numero della vittima su una nuova SIM.
- **Pericolosità**: Molto alta, permette l'accesso a conti bancari e altri servizi protetti da autenticazione a due fattori.
- **Diffusione**: Bassa ma in crescita, particolarmente mirata a persone con asset digitali di valore.
- **Difesa**: Utilizzare PIN aggiuntivi per l'account telefonico, non usare il numero di telefono come unico metodo di autenticazione a due fattori, preferire app di autenticazione come Google Authenticator.

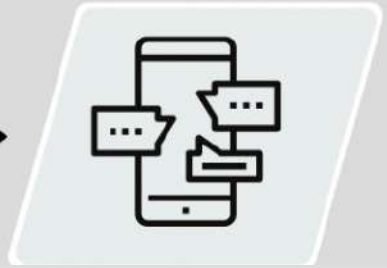
SIM Swap Scam Process

Il truffatore ottiene i dati personali dell'utente tramite phishing

Il truffatore chiama l'operatore telefonico e, con tecniche di persuasione, ottiene il trasferimento del numero (SIM)



L'operatore telefonico trasferisce il numero dell' utente sulla SIM del truffatore



Il truffatore adesso riceve gli SMS e le chiamate della vittima che è ignara fino all' uso del telefono

Il truffatore bypassa facilmente la 2FA

Il truffatore ruba i soldi e cancella tutto

Truffe: altre tipologie

Applicazioni malware

- **Mezzo di attacco**: App che sembrano legittime ma contengono codice malevolo, spesso distribuite attraverso store non ufficiali.
- **Pericolosità**: Alta, possono rubare dati, spiare l'utente o bloccare il dispositivo.
  Anche per app non malevole attenzione al **microfono** (Preferenze>Privacy>Gestione autorizzazioni)
  Attenzione alle impostazioni Wapp (**Ultimo accesso e Online** **e** **STATUS**)
- **Difesa**: Scaricare app solo dagli store ufficiali (Google Play, App Store), verificare le recensioni e il numero di download, controllare le autorizzazioni richieste prima dell'installazione, utilizzare un antivirus per dispositivi mobili.Usare **Google Play Protect**

Truffe di supporto tecnico

- **Mezzo di attacco**: Falsi avvisi di virus o problemi tecnici che spingono a chiamare numeri a pagamento o installare "soluzioni".
- **Pericolosità**: Media-alta, può portare a perdite economiche dirette.
- **Difesa**: Ignorare pop-up allarmistici, non installare software suggeriti da questi avvisi, utilizzare solo canali ufficiali di supporto tecnico.

Reti Wi-Fi fasulle

- **Mezzo di attacco**: Hotspot Wi-Fi che imitano reti legittime per intercettare dati.
- **Pericolosità**: Alta, può portare all'intercettazione di comunicazioni e credenziali.
- **Difesa**: Utilizzare una VPN quando ci si connette a reti pubbliche, verificare con attenzione il nome della rete, evitare operazioni sensibili (come accesso a conti bancari) su reti pubbliche.

Truffe romantiche/sentimentali

- **Mezzo di attacco**: Relazioni false costruite tramite app di dating o social media per estorcere denaro.Se ti scrivono per sbaglio è sbagliato rispondere (truffa “*Scusami ho sbagliato numero”*).
- **Pericolosità**: Media-alta, può causare gravi perdite finanziarie oltre a danni emotivi.
- **Difesa**: Essere scettici di fronte a richieste di denaro, fare ricerche sulla persona (ricerca immagini inversa), limitare le informazioni personali condivise online, non inviare mai denaro a persone mai incontrate di persona.
-

DECALOGO per la sicurezza

Password diverse per ogni servizio e cambiarla frequentemente

Aggiornare sempre il dispositivo mobile

Google Play per Installare le applicazioni e attenti alle autorizzazioni concesse

Controllare con attenzione gli **A**llegati, mail e sms anche da persone fidate

Evitare di connettersi a **Re**ti pubbliche o non protette

Inserire sempre un **B**locco allo smartphone e evitare di disattivare il PIN di blocco della SIM

Installare un buon **A**ntimalware (Malwarebytes)

Evitare di raccontare attraverso i **S**ocial le proprie attività, informazioni personali e spostamenti

TANTA

ATTENZIONE…Attenzione…ATTENZIONE

A richieste da evadere con Urgenza
A richiesta di qualunque tipo di pagamento o informazioni personali anche banali
A minacce di sospensione account/pensione/conto Corrente….

Gli screenshot

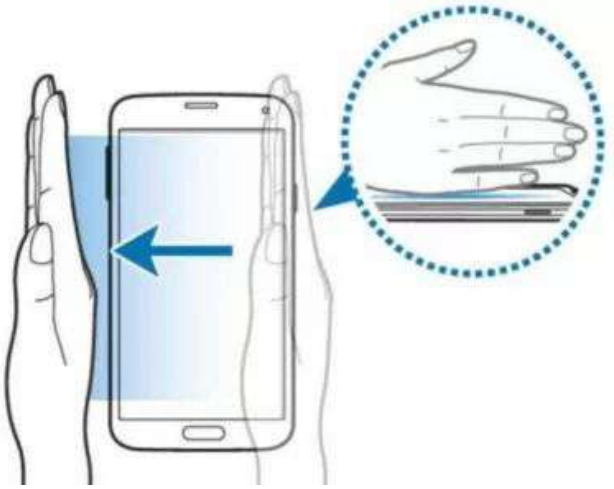
Uno **screenshot** è una cattura istantanea di ciò che appare sullo schermo dello smartphone. E' utile per salvare informazioni importanti, condividere contenuti o conservare prove di conversazioni e acquisti.

Dove Trovare gli Screenshot

- Galleria o Foto:
  - Aprire l'app Galleria o Google Foto
- Gestione File:
  - Utilizzare l'app File o Gestione File per navigare nella memoria del dispositivo.
  - Poi cartella Pictures o Immagini, quindi aprire la cartella Screenshots.

Come fare uno screenshot

Come fare con smartphone Samsung



Palm Swipe (scorrimento con il palmo)

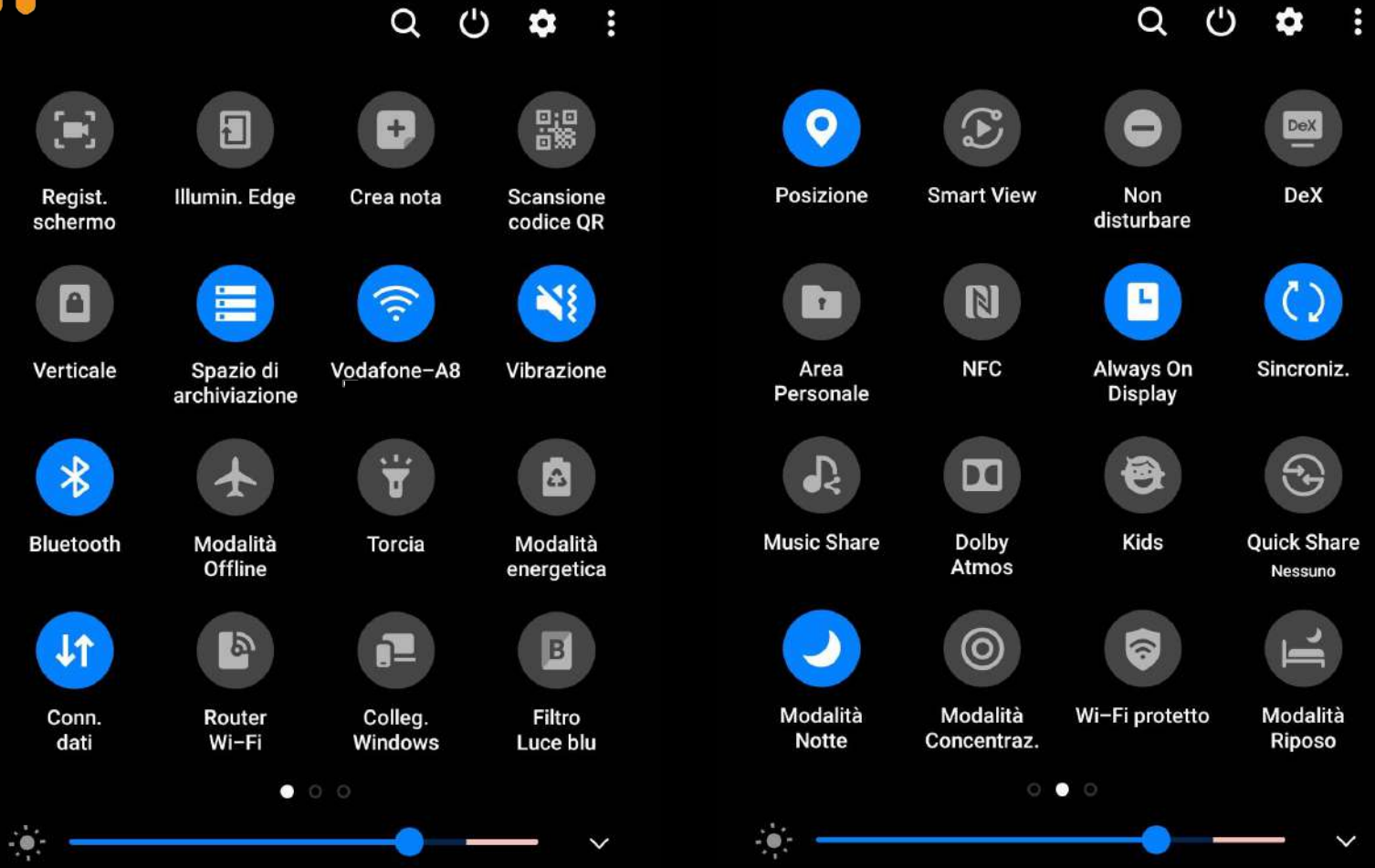
Dal **menù di scelta rapida**>Acquisizione schermata

Come fare screenshot su tutti gli smartphone

Con **ok Google**
Impostazioni > digitare nel motore di ricerca: *voice match*
Se non salva l'immagine mettere un flag su:*usa contesto dello schermo*

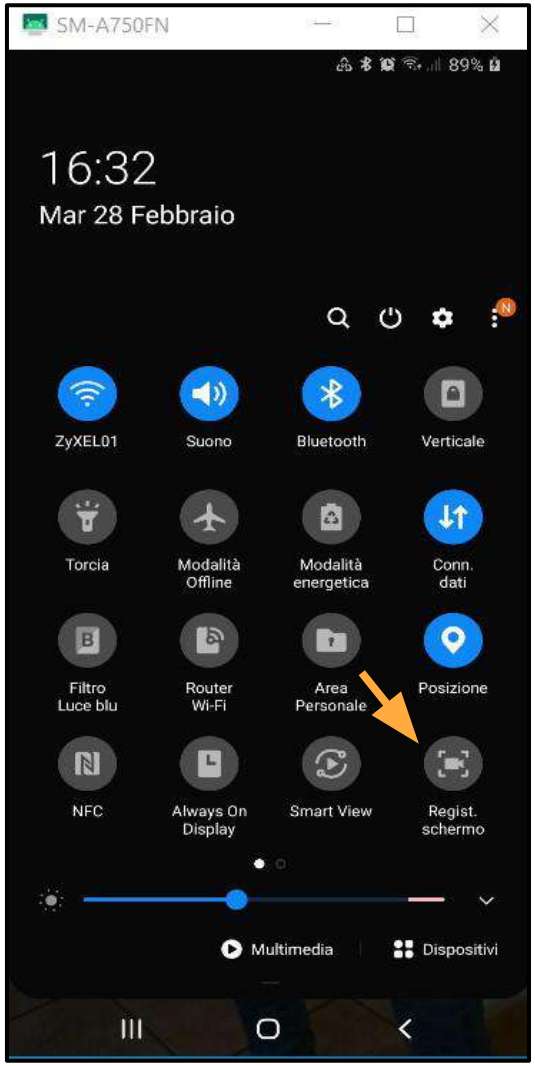
Google Play Rapido screenshot

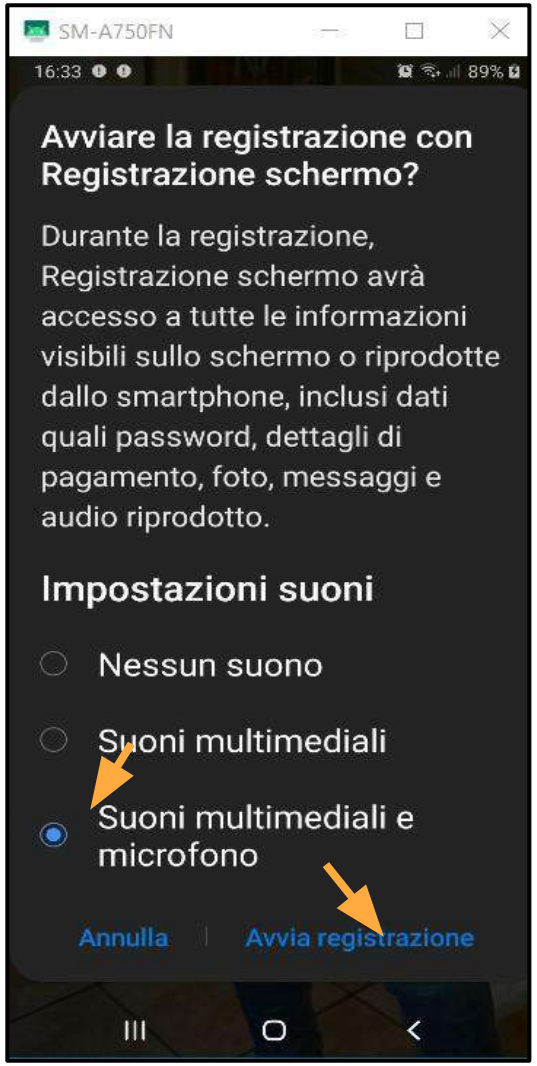
Menu di scelta rapida



Come registrare lo schermo

Facendo uno swipe verso il basso sul dispositivo si accede a un **menù di scelta rapida o a un pannello di controllo** che mostra diverse icone e opzioni.Queste icone possono variare leggermente a seconda del sistema operativo e del modello del dispositivo, ma in generale, queste sono le funzioni più comuni che si possono trovare





Truffe usando l'Intelligenza Artificiale (DeepFake)

I deepfake sono foto, video e audio creati grazie a **software di intelligenza artificiale (AI)** che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

VIDEO DEEPFAKE

Questi video utilizzano l'intelligenza artificiale per sostituire perfettamente il volto di una persona con quello di un'altra, creando l'illusione che stia dicendo o facendo qualcosa che non ha mai fatto. Questo può essere utilizzato per impersonare amministratori delegati, politici o celebrità a scopo di lucro, ricatto o danno alla reputazione.

CLONAZIONE DELLA VOCE

L'intelligenza artificiale può essere utilizzata per creare simulazioni realistiche della voce di una persona, consentendo ai truffatori di impersonarla al telefono, nei messaggi vocali o persino nelle conversazioni dal vivo. Questo può essere usato per ingannare le vittime e indurle a inviare denaro o a fornire informazioni sensibili.

GENERAZIONE DEL TESTO

L'intelligenza artificiale può essere utilizzata per generare testi realistici e credibili, che possono essere usati per creare articoli di notizie false, post sui social media o persino email. Questo può essere usato per diffondere disinformazione, manipolare l'opinione pubblica o truffare un individuo.

Truffe usando l'Intelligenza Artificiale (DeepFake)

DeepFake quiz: quale è la foto reale?

Foto 1

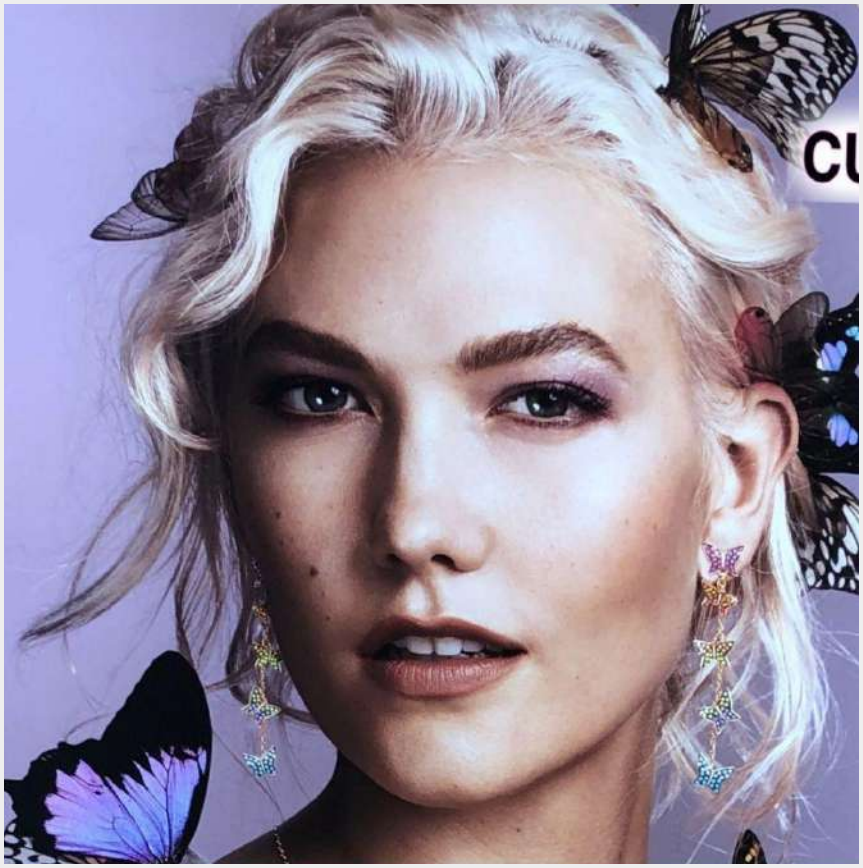


Foto 2

DeepFake quiz: quale è la foto reale?

Foto 1

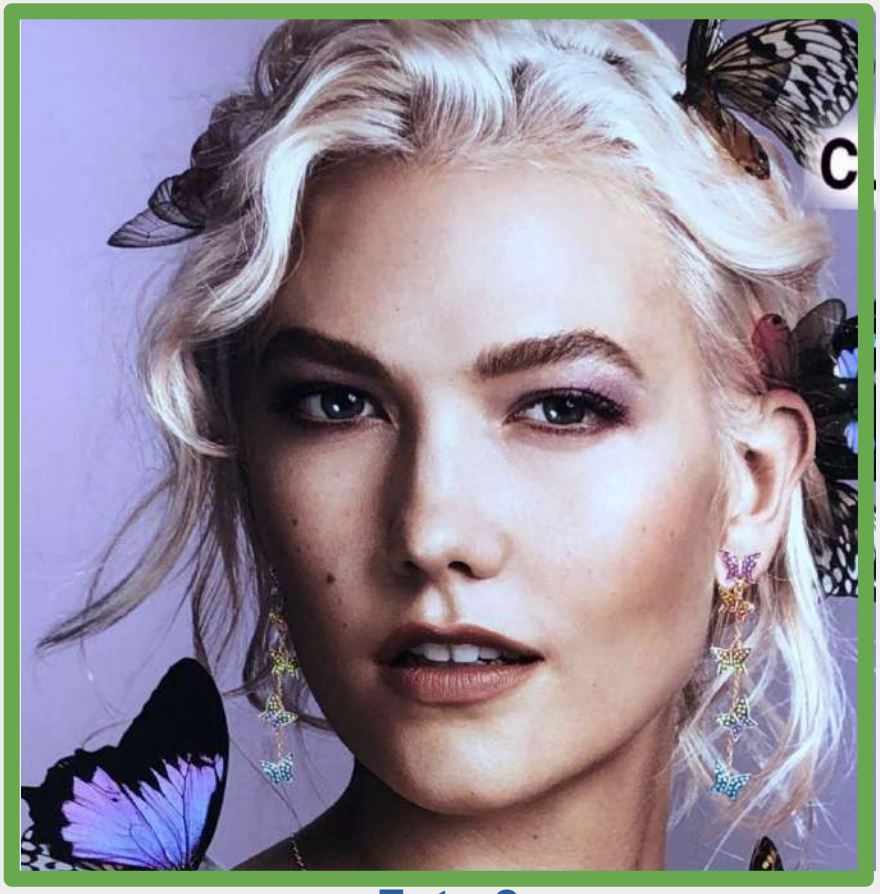


Foto 2

DeepFake quiz: quale è la foto reale?

Foto 1

Foto 2

DeepFake quiz: quale è la foto reale?

Foto 1

Foto 2

DeepFake quiz: quale è la foto reale?

Foto 1

Foto 2

DeepFake quiz: quale è la foto reale?

Foto 1

Foto 2