TRUST aWARE

FONDAZIONE Mondo Digitale

Enhancing Digital Security, Privacy and TRUST in softWARE

Come utilizzare i Social Network in sicurezza

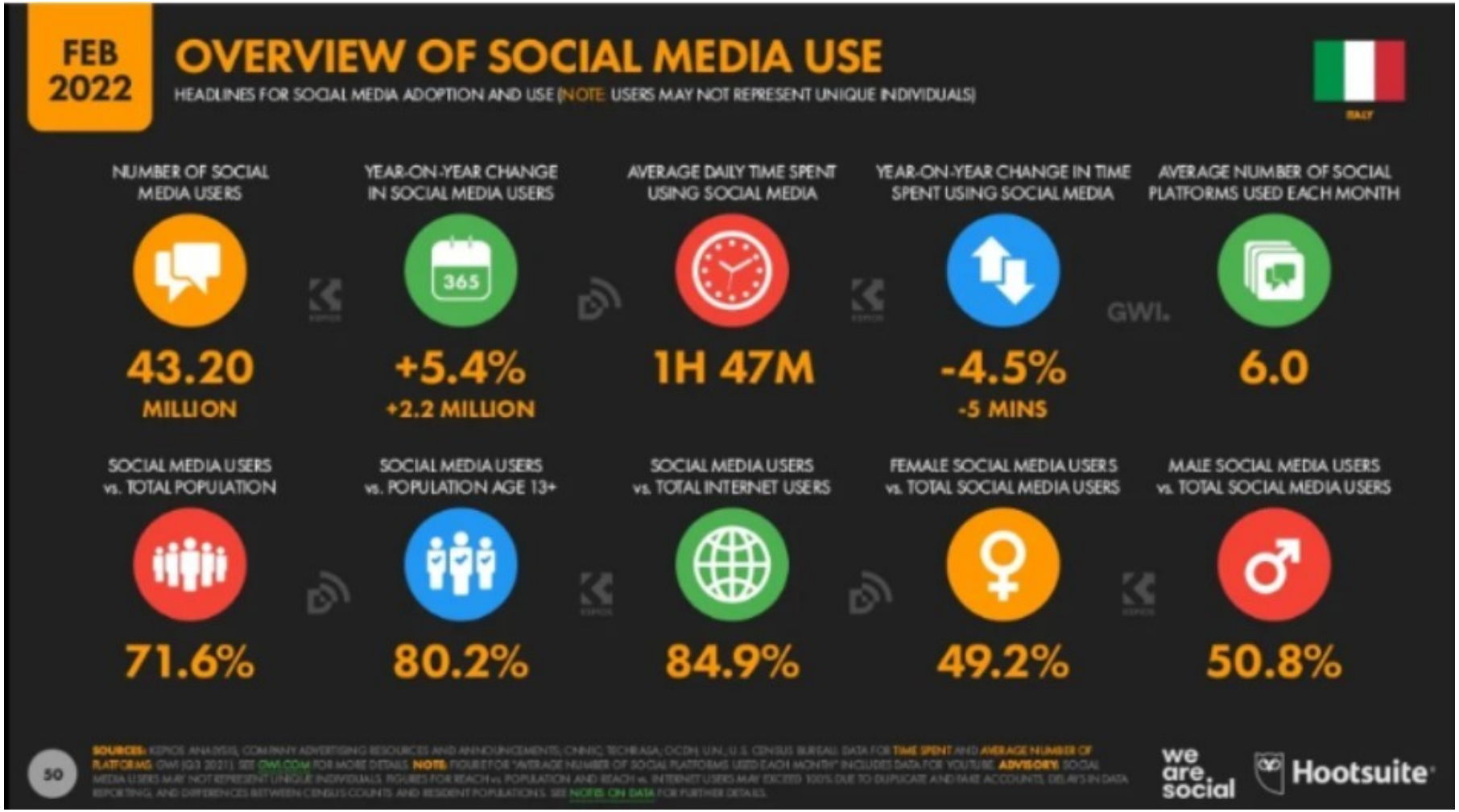
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

FONDAZIONE Mondo Digitale

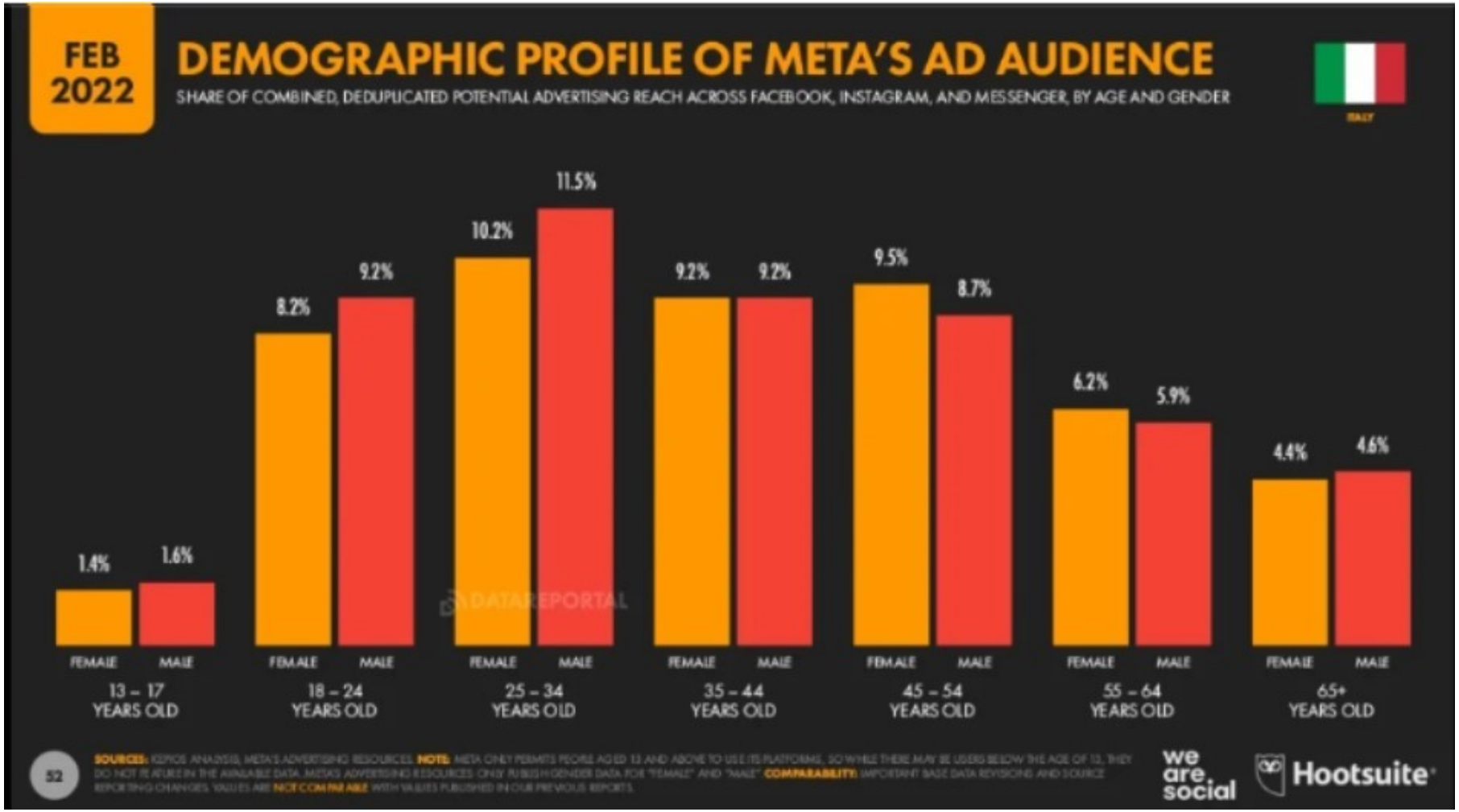
Index

Social Media Trends 2022



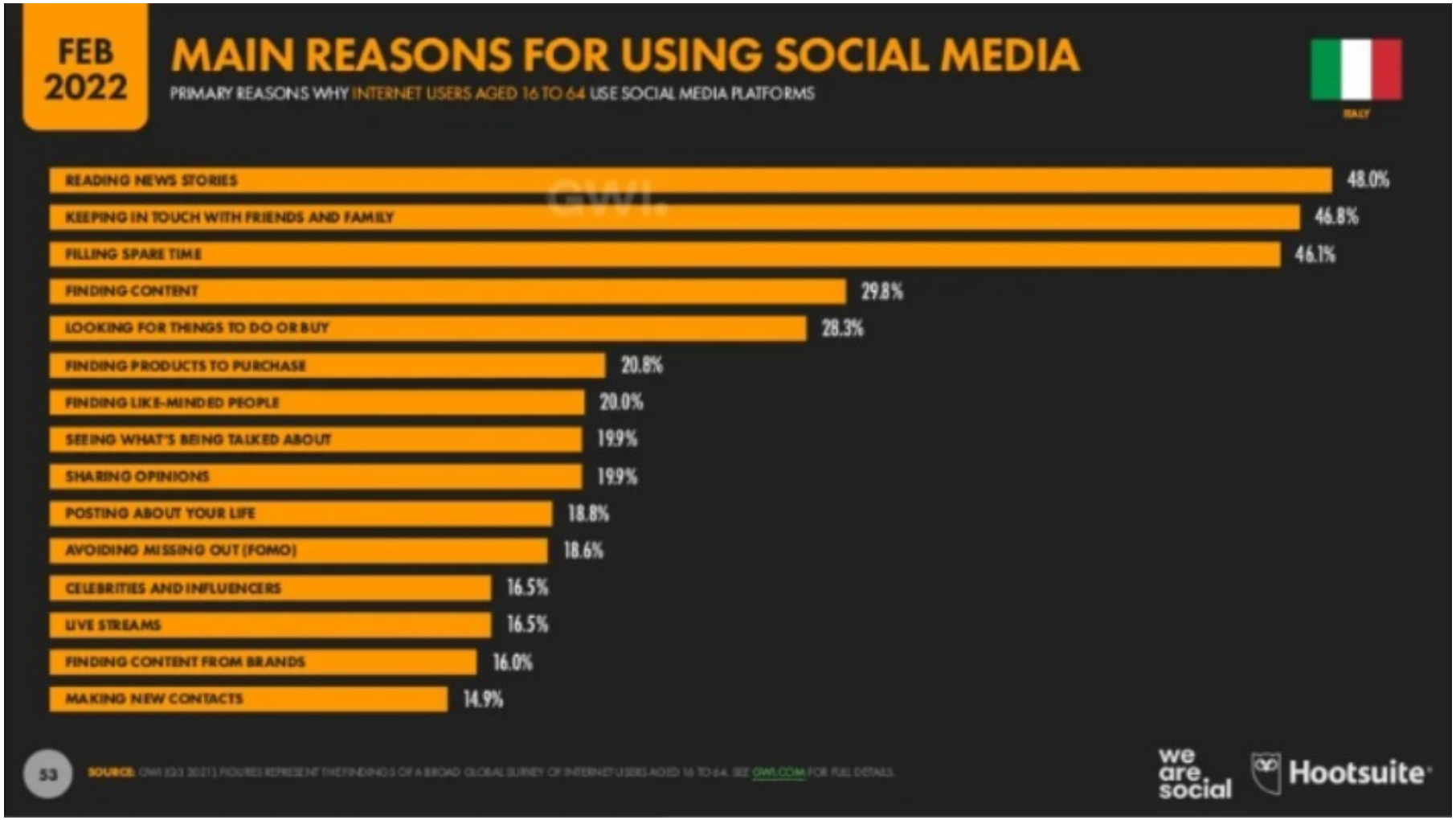
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Social Media Trends 2022



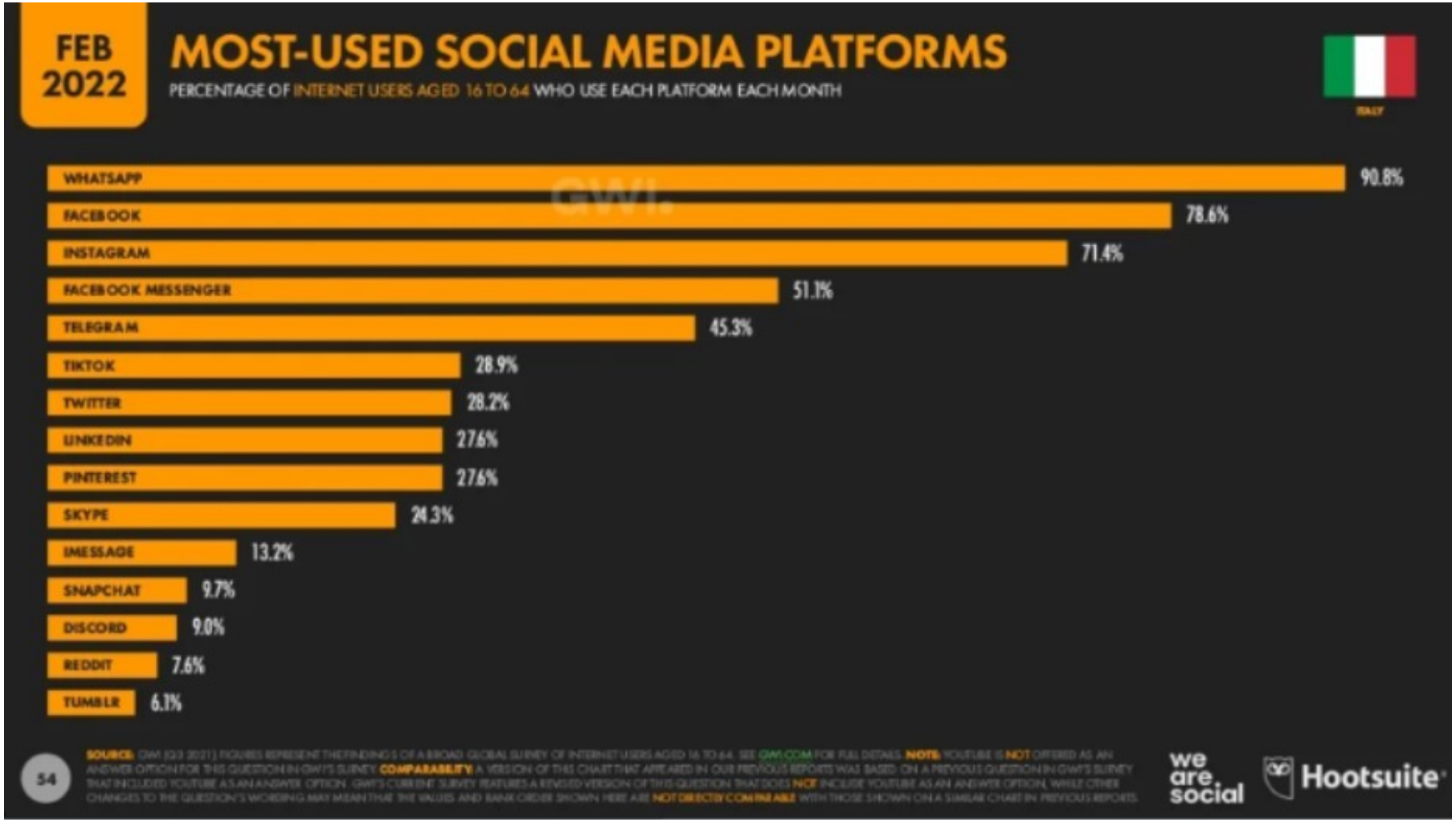
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Social Media Trends 2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Social Media Trends 2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Social Network: questione di età

Età per aprire legalmente un account sulle piattaforme

- Facebook
- Instagram
- YouTube
- Tik Tok
- Twitter
- Discord
- Twitch

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Social Network: questione di età

Età per aprire legalmente un account sulle piattaforme:

- LinkedIn
- WhatsApp

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

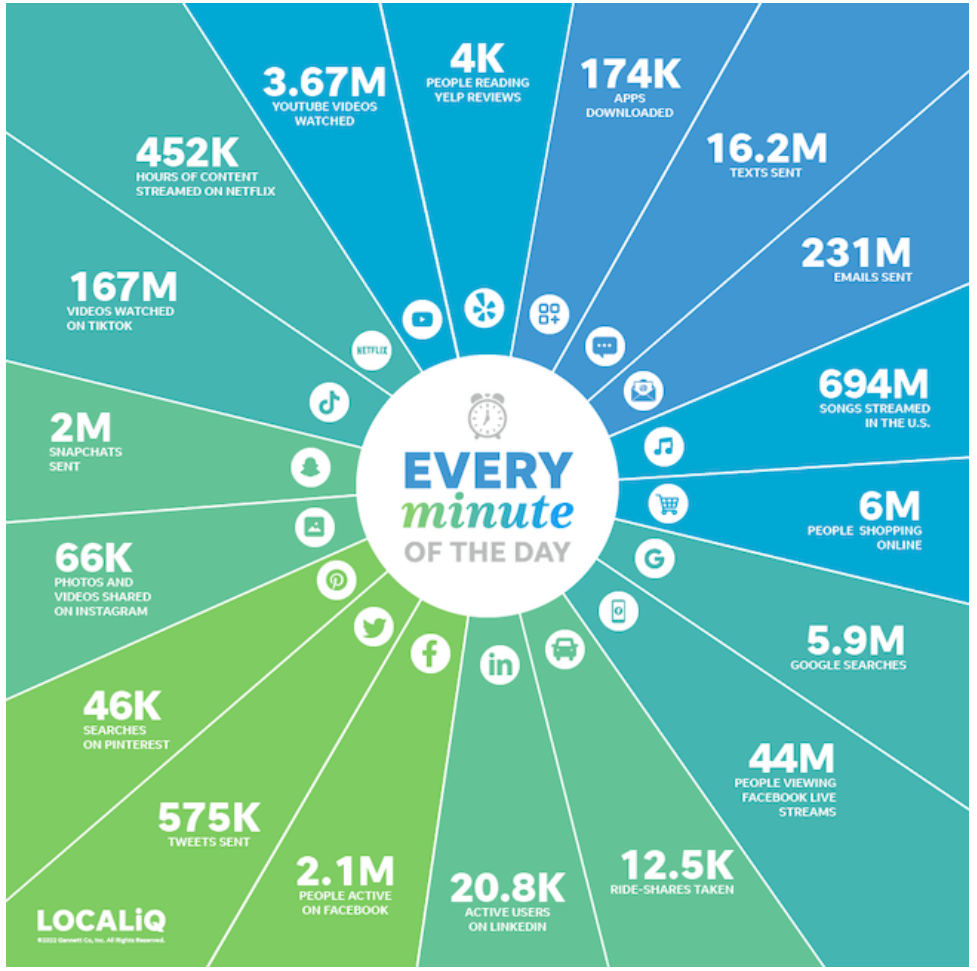
Social Network: questione di età

Se decidiamo di aprire / lasciar aprire un account sulle piattaforme Social non rispettando il limite minimo di età, dobbiamo:

- Controllare e settare tutte le impostazioni riguardanti la privacy del minore
- Supervisionare la tipologia di contenuti con cui viene a contatto
- Aprire un dialogo con il minore sulla sua conoscenza della piattaforma e dell'importanza di proteggere i propri dati
- Aggiornare i sistemi di sicurezza sui device in cui avviene il collegamento alla piattaforma social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Cosa succede in 1 Minuto online - 2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

I contenuti: i dati che condividiamo

Condividiamo quotidianamente un numero enorme di dati, spesso, senza rendercene conto.

Tutti i giorni online vengono condivisi:

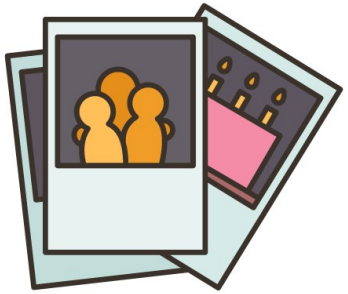
- Foto e video
- Abitudini e interessi
- Posti in cui ci troviamo o viaggiamo
- Informazioni personali e dati sensibili di vario tipo

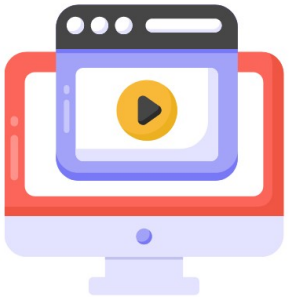
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

I contenuti: i dati che condividiamo

Prestiamo attenzione:

- **Cosa condividiamo**: limitiamo la pubblicazione e l'invio di foto o video dove veniamo ritratti in contesti che potrebbero essere decontestualizzati (ad esempio, una foto in costume)





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

I contenuti: i dati che condividiamo

Prestiamo attenzione:

- **Con chi condividiamo**: accettiamo solamente collegamenti con persone che conosciamo anche nella vita reale e scegliamo, di volta in volta, cosa condividere con loro. In caso di messaggi o comunicazioni strane e diverse dalle solite, avvisare la persona in questione: potrebbe aver subito un hackeraggio dell'account senza saperlo

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

I contenuti: i dati che condividiamo

Prestiamo attenzione:

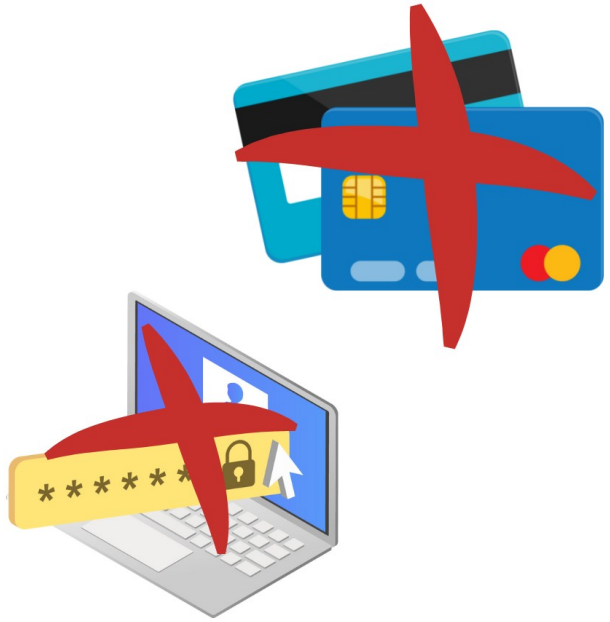
- **Condividere la nostra posizione**: annunciare una partenza di più giorni, registrarci in un luogo in cui siamo al momento della pubblicazione, dichiarare di essere soli/e nel momento in cui si scrive possono mettere a rischio la sicurezza personale; organizziamo le pubblicazioni in maniera ragionata.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

I contenuti: i dati che condividiamo

Prestiamo attenzione:

- **Condivisione di dati sensibili**: evitiamo, anche in chat private con persone che conosciamo, di inviare foto intime, carte di credito e relativi numeri e codici di sicurezza, credenziali di accesso a qualsiasi tipologia di account (social media, e-mail, online banking, ecc)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Privacy & Cookie Policy

Tutti i Social Network hanno una sezione di **Privacy e Cookie Policy** da cui reperire le informazioni in merito a

- <u>Trattamento dei dati personali dei membri</u>: come vengono registrati, archiviati e gestiti i dati personali condivisi, il tempo di conservazione e il responsabile del trattamento; è possibile trovare anche le informazioni sulla modalità di cancellazione totale dei propri dati (Diritto all'Oblio)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Privacy & Cookie Policy

Tutti i Social Network hanno una sezione di Privacy e Cookie Policy da cui reperire le informazioni in merito a

- <u>Tracciamento delle azioni eseguite sulla piattaforma dai membri</u>: quanti e quali dati vengono tracciati, per quali scopi e come è possibile scegliere le varie autorizzazioni (accettazione completa, parziale o rifiuto dei Cookies)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Privacy Dei Contenuti

Oltre al trattamento di dati e tracciamenti, all'interno di ogni piattaforma social è possibile scegliere quali contenuti vogliamo che siano pubblici e quali no.

Si può infatti impostare una privacy

- Per l'account: chi può cercare il nostro account (tutti, solo gli amici, gli amici degli amici), come è possibile trovare il nostro account (solo nome e cognome, e-mail, numero di telefono, tutti o nessuno dei precedenti)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Privacy Dei Contenuti

- Per i contenuti: chi può leggere i post (tutti in rete, tutti sulla piattaforma social, gli amici degli amici, solo gli amici, solo io)
- Per i commenti: chi può commentare i miei post (tutti, gli amici degli amici, solo gli amici, solo selezionate persone)
- Per i messaggi: chi può contattarci in chat/messaggio privato (tutti, amici degli amici, solo gli amici)

Queste impostazioni valgono per la maggior parte delle piattaforme social, per Instagram, ad esempio, possiamo decidere se tenere l'account privato o pubblico oppure bloccare la visione dei nostri contenuti o la ricezione dei messaggi solo a determinate persone

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autorizzazioni alle App Social Media

Utilizzo di app: utenti che si collegano da

- Smartphone: 85%
- Tablet: 10%
- Pc: 5%

Ogni app richiede delle autorizzazioni prima di essere utilizzata:

- Accesso ai contatti in rubrica/nel device
- Accesso alla foto/videocamera
- Accesso al microfono dello smartphone/device
- Accesso alla posizione (GPS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autorizzazioni alle App Social Media

Le app accedono ai nostri contenuti a seconda delle autorizzazioni date; questo permette loro di funzionare al meglio delle prestazioni e di profilarci per proporci solamente ciò a cui siamo interessati.

Possiamo scegliere quale opzioni attivare

- Consenti sempre
- Consenti solo questa volta/per alcuni minuti
- Consenti solo quando l'app è in uso

Possono essere modificate e revocate in qualsiasi momento

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

La **Password** ci consente di limitare l'accesso ad un account privato e proteggere i nostri dati e contenuti.

La Password non deve:

- Essere condivisa con nessuno
- Essere la stessa per tutti gli account/device
- Essere troppo facile da indovinare
- Contenere date di nascita, nomi di persone care, squadre tifate, ecc
- Scritta in posti facili da scoprire (ad esempio, un foglietto nel portafoglio, su una lavagnetta in casa, in una rubrica in un cassetto di libero accesso, ecc..)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

Per evitare di perdere le password o doverle cambiare ripetutamente, possiamo utilizzare un'app specifica: il gestore di password!

Ne esistono molte tipologie scaricabili sia per Android che per IoS, tra le più famose, sicure ed utilizzate:

- NordPass (a pagamento)
- Bitwarden (gratuita)
- Google Smart Lock

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password: sceglierne una efficace

Consigli per una password efficace:

- La **lunghezza**: minimo 8 caratteri
- La **complessità**: parole di scarso utilizzo o complessa scrittura
- La **grafia**: utilizzare lettere maiuscole e minuscole, numeri e caratteri speciali in maniera mista; sostituire le lettere con i numeri e viceversa (cane = c4n3 / 1980 = l98o)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

L'**Autenticazione a 2 Fattori** (o verifica a due passaggi) è un livello di sicurezza maggiore che possiamo attivare sui nostri account Social.

Ci permette di bloccare qualsiasi tentativo di accesso da parte di un hacker.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Password efficace: facciamo un check!

https://howsecureismypassword.net/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

Attivandola, ogni qual volta si effettua l'accesso al nostro account da un browser/device sconosciuto, ci arriverà una notifica con orario, data e luogo dell'accesso.
In caso non fossimo noi, sarà possibile bloccare l'accesso e procedere con un cambio password.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Autenticazione a 2 Fattori: questione di sicurezza

Come si attiva:

- Nelle impostazioni di Privacy e Sicurezza del nostro account Social
- Scegliere di attivare l'Autenticazione a 2 Fattori
- Scegliere la modalità:
  - Codice SMS
  - Codici di Sicurezza (lista di codici da utilizzare una sola volta e rigenerare al bisogno)
  - App di autenticazione (esempio: Google Authenticator)
- Completare la procedura guidata

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Glossario - Definizioni Treccani

- **Social Network**: servizio informatico on line che permette la realizzazione di reti sociali virtuali
- **Account**: registrazione presso un provider di un utente che voglia accedere a un determinato servizio e, per estensione, l'insieme delle informazioni (nome, password, ecc.), depositate presso il provider medesimo, che identificano l'utente.
- **Password**: parola di riconoscimento impiegata a scopo di sicurezza per garantire che l'uso di una risorsa sia concesso solo agli utenti autorizzati
- **Autenticazione a due Fattori**: una procedura di sicurezza in cui l'accesso a un servizio avviene in due passaggi o "fattori" separati, ad esempio una password e un codice usa e getta. Ad esempio, potresti dover inserire una password e poi un codice inviato al tuo telefono oppure creato da un'app.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

Grazie per l’attenzione.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377