CYBERBULLISMO

COME DIFENDERSI

COMINCIAMO DAL PC

ANTI-VIRUS E AGGIORNAMENTI

Se il vostro PC ha un antivirus scaduto, non aggiornato o addirittura assente, consentite a migliaia di virus e hacker di accedere al vostro PC e rubarvi dati o immagini provate per poi ricattarvi.
Lo stesso vale per il sistema operativo (Windows, Linux, iOS ecc.), va sempre aggiornato.

COPRITE WEBCAM E MICROFONI

Quando non vengono utilizzati per sicurezza è meglio coprire webcam e microfoni del PC.

PASSWORD

Impostate le password per accedere al vostro sistema operativo o alle cartelle più importanti. La password DEVE essere alfanumerica e più lunga possibile: non condividetela con nessuno. Cambiatela ogni mese.

NAVIGAZIONE INTERNET

PASSWORD

Impedite a qualsiasi browser (Chrome, Explorer ecc.) di salvare le password quando accedete a email, social network ecc.

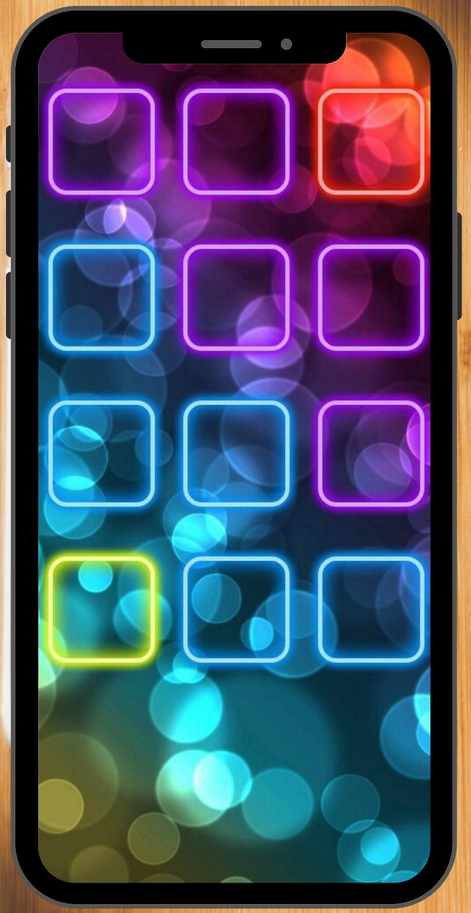
NAVIGAZIONE IN INCOGNITO

Navigate "in incognito", è una opzione del browser per navigare con maggiore sicurezza in internet.

NON APRIRE SITI WEB, LINK O FILE SOSPETTI

Non navigate su siti web non sicuri (spesso vengono segnalati dal browser stesso come "non sicuro" e comunque sono siti che cominciano per http e non in httpS), non aprite mai link o allegati di cui non conoscete la provenienza

TELEFONO



Usate doppio PIN: PIN normale e PIN di crittografia dati

Usate per sblocco riconoscimento facciale o digitale

Aggiornate sempre tutte le APP (le app non aggiornate sono più vulnerabili) e il sistema operativo.

Non lasciare mai il telefono incustodito

Salvate le foto su un hard disk esterno o su cloud sicuro, poi svuotate la memoria del vostro telefono

Ove possibile, preferite Telegram a Whatsapp e ricordatevi di cancellare i dati.

LE CHAT

SOLO CON PERSONE CHE CONOSCETE

NON INVIATE FOTO O MESSAGGI COMPROMETTENTI

Potrebbero essere usati non solo da chi è presente nella chat, ma anche da hacker nascosti

NON APRITE SITI WEB, LINK O FILE SOSPETTI

Non navigate su siti web non sicuri (spesso vengono segnalati dal browser stesso come "non sicuro" e comunque sono siti che cominciano per http e non in httpS), non aprite mai link o allegati di cui non conoscete la provenienza

SOCIAL NETWORK

NON ACCETTARE AMICIZIE DI ESTRANEI

Spesso sono coloro con cui non condividete amicizie. Fare riferimento alla pagina "Profili Fake Italia".

AUMENTARE AL MASSIMO LE IMPOSTAZIONI DI PRIVACY

Questo impedirà a male intenzionati di vedere (e salvare) i vostri post e la vostra gallery

DISATTIVARE LA GEOLOCALIZZAZIONE

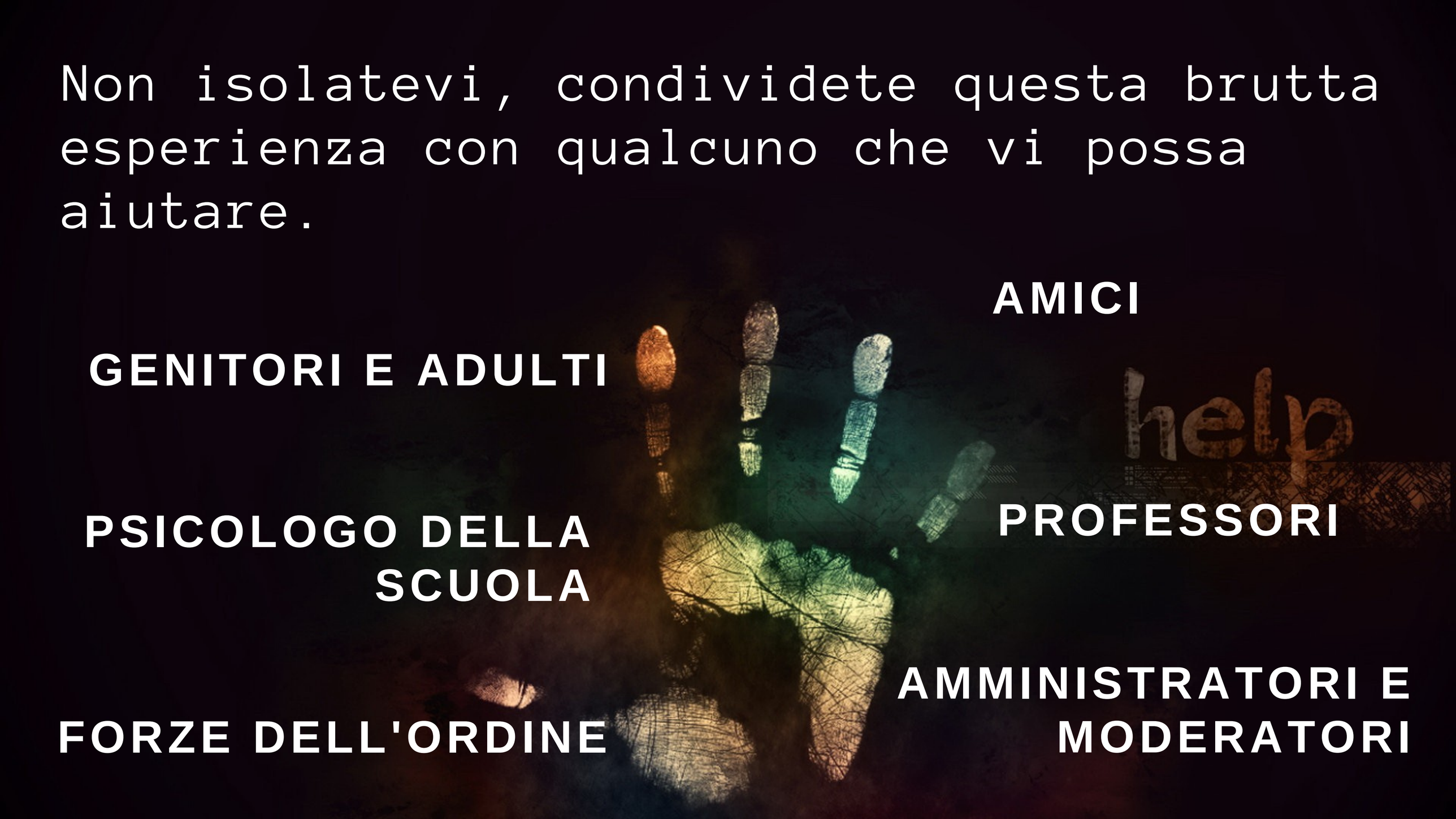
Vale per i social, come per le App: disattivare la geolocalizzazione. Chiunque potrebbe conoscere in ogni momento la vostra posizione o i percorsi che solitamente fate.

RICONOSCERE UN PROFILO FAKE

- Zero amicizie in comune
- Verifica della foto con Google Immagini
- Foto scarse, sempre da solo o di immagini trovate su Internet
- Controllare la data di creazione del profilo
- Controllare la frequenza dei post
- Non viene mai taggato in post o foto
- Utilizzo dell'italiano non corretto
- Strane proposte (finanziamento o foto di nudo)
- Segnalate a Facebook (e nei gruppi dedicati) ogni abuso con le apposite funzioni.


COSA FARE
A CHI RIVOLGERSI

Non isolatevi, condividete questa brutta esperienza con qualcuno che vi possa aiutare.



AMICI

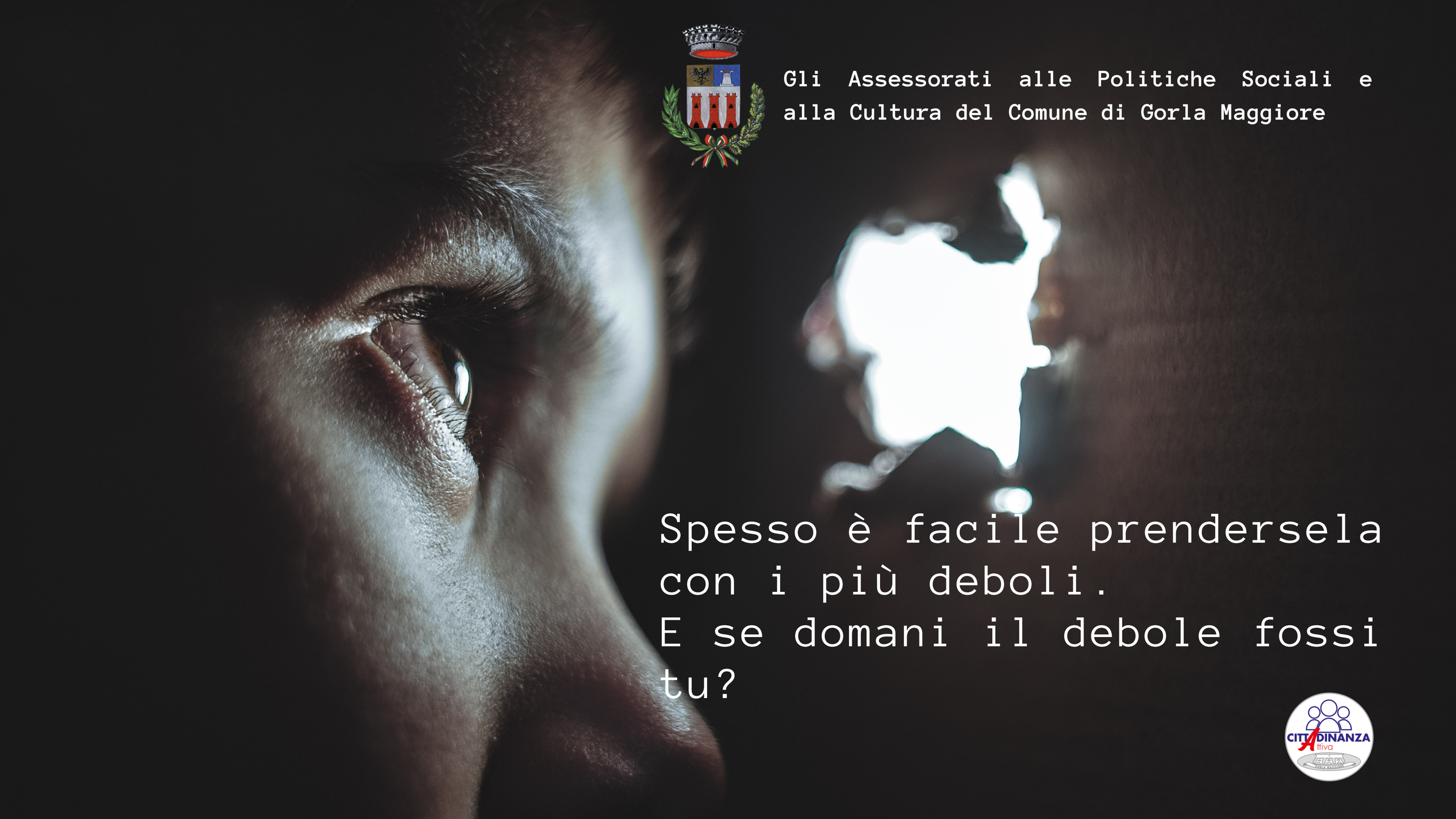
GENITORI E ADULTI

PSICOLOGO DELLA SCUOLA

PROFESSORI

AMMINISTRATORI E MODERATORI

FORZE DELL'ORDINE



Gli Assessorati alle Politiche Sociali e alla Cultura del Comune di Gorla Maggiore

Spesso è facile prendersela con i più deboli.
E se domani il debole fossi tu?