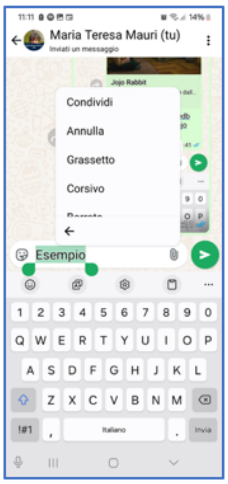
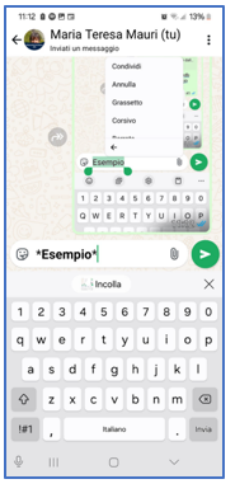
Sei proprio sicura/sicuro di saper usare WhatsApp?

Come formattare il testo di un messaggio

Scrivi un messaggio nella barra della chat, premi sul testo che vuoi formattare per selezionarlo e clicca sui **(:)** del menù.

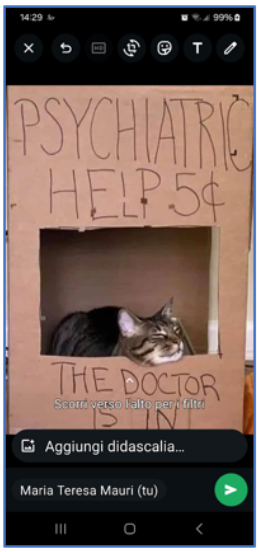
Seleziona l'opzione che desideri tra quelle che compaiono: **Grassetto, Corsivo, Barrato, ecc.**

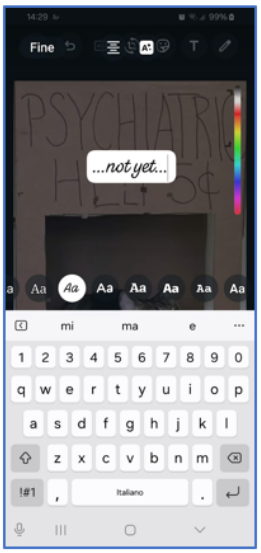




Se vuoi formattare i messaggi che invii su WhatsApp da PC poiché non puoi sfruttare un menu specifico che consenta di fare ciò, puoi comunque scrivere in grassetto, corsivo, barrato, etc. utilizzando i simboli **(*), (_), (~)** e **(`)** prima e dopo la parola o la frase che vuoi inviare a uno dei tuoi contatti.

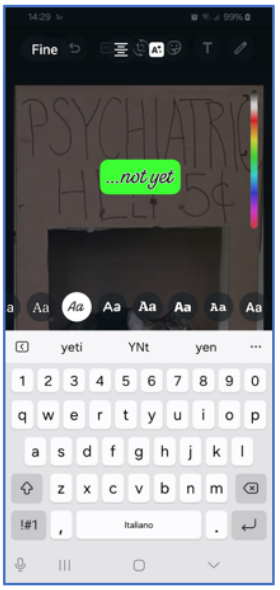
Se vuoi inviare una foto con del testo personalizzato, puoi aggiungere alla foto scelta una scritta cambiando il font, il colore o disegnare per rendere il tutto più bello.



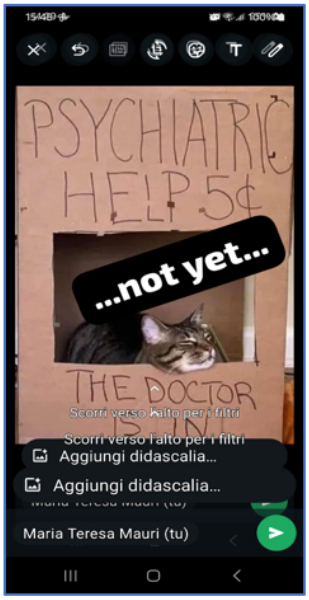


Una volta composto il testo, per cambiare il font devi cliccare sulla **T** in alto a destra in modo da scorrere tra i font disponibili e scegliere.

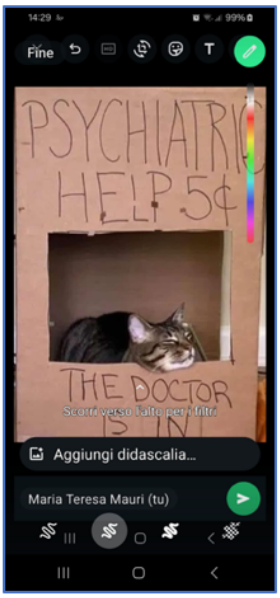
Invece tramite la barra colorata sulla destra, puoi anche **decidere il colore** che questa scritta deve assumere.

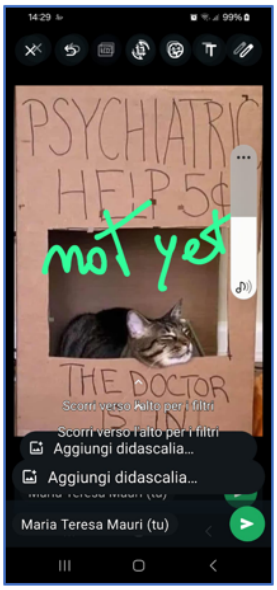


Una volta terminate le modifiche, clicca su un punto della foto esterno alla scritta per tornare alla schermata d'invio e, se desideri **cambiare la dimensione o il posizionamento** della scritta, puoi farlo da qui appoggiando il dito sopra e trascinandola oppure usando due dita e muovendole in modo divergente o convergente rispetto al centro per ingrandirla o rimpicciolirla, proprio come nelle foto.

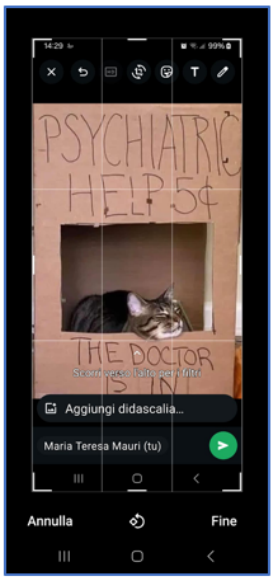


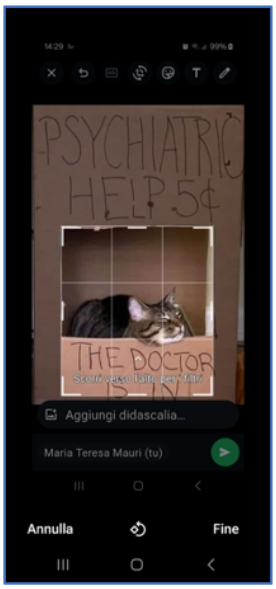
Per aggiungere invece un disegno ad una foto selezionata, posso cliccare sul simbolo della matita in alto destra e scrivere o disegnare ciò che voglio scegliendo anche il colore che preferisco, dalla barra laterale e lo spessore tra quelli presenti in basso in fondo alla schermata.





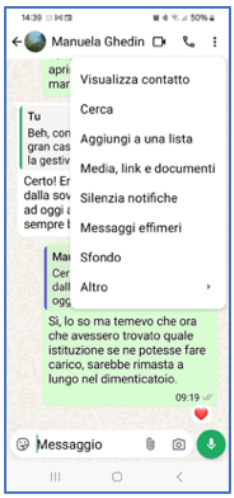
È possibile anche selezionare l'icona "ritaglia" per potere poi selezionare l'immagine e ruotarla oppure per ritagliare solo una parte della stessa che voglio inviare.



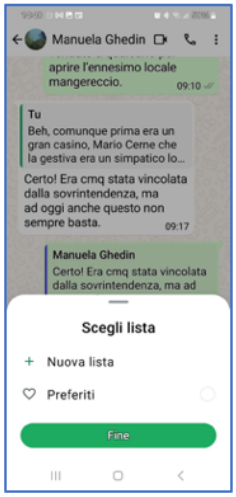


Come aggiungere un contatto ai Preferiti

Apri la Chat che ti interessa e clicca sui (⋮) in alto a destra per aprire il menù poi clicca su **Aggiungi a una lista** e seleziona **Preferiti** e clicca su **Fine**



Se invece clicchi su **Nuova lista** si apre una schermata all'interno della quale poi creare una nuova lista, darle un nome e aggiungere altri contatti

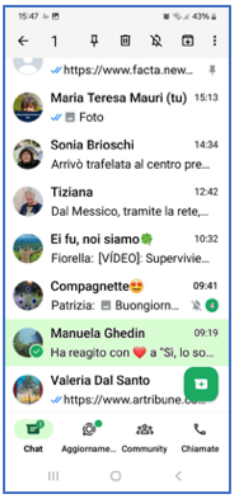


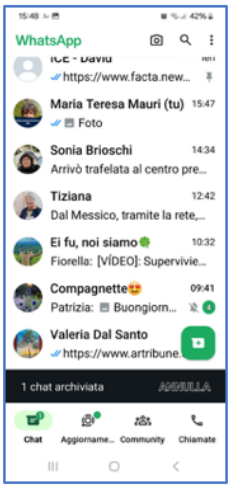
© A cura di Maria Teresa Mauri - Quarto incontro: mercoledì 28/01/2026 8

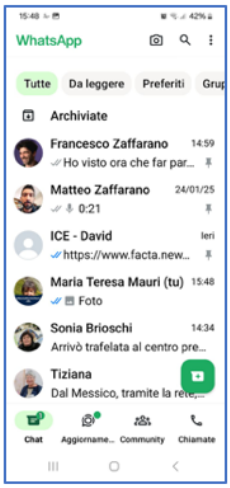
Al contrario per **rimuovere** un contatto salvato in una lista o in **Preferiti** basta fare lo stesso procedimento e togliere il segno di spunta dal contatto salvato.

Come archiviare/rimuovere una chat

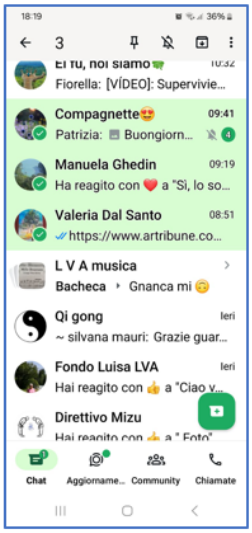
Vai alla **Chat,** selezionala tenendo premuto il dito finché compare il segno di spunta clicca poi sull'icona della **scatola con freccia giù** all'interno.

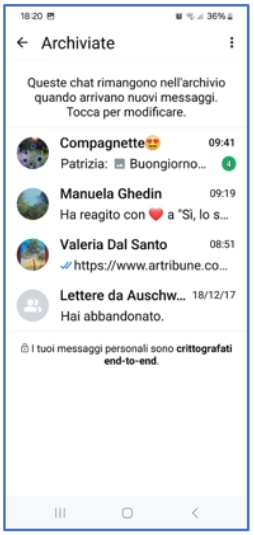




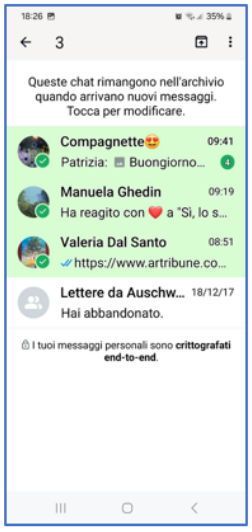


Allo stesso modo puoi procedere anche per archiviare più chat contemporaneamente.





Per rimuovere le chat archiviate si selezionano all'interno di **Archiviate** poi clicco sull'icona questa volta **della scatola con la freccia all'insù.**



Come difendersi dai truffatori su WhatsApp

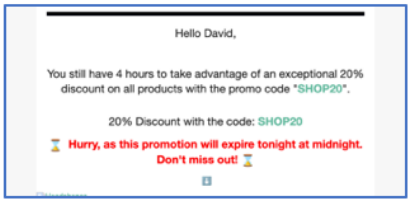
È bene sapere che WhatsApp **non invia messaggi e richieste** agli utenti di propria iniziativa. Si verrà contattati dall'azienda solo in seguito alla richiesta di supporto. In tutti gli altri casi, si potrebbe trattare di una truffa.

Il Phishing

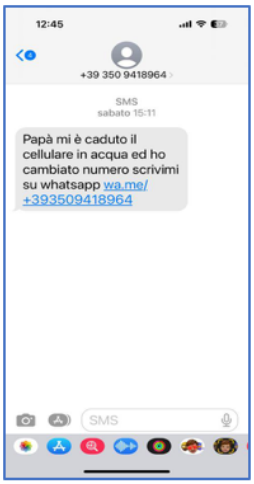
Il termine **phishing** è una storpiatura del verbo inglese **fishing**, in italiano pescare. Si tratta di un'**attività truffaldina** che avviene principalmente tramite **posta elettronica, ma sempre più spesso anche attraverso altri sistemi di comunicazione come i messaggi privati nei social network o nelle app di messaggistica (facebook, instagram, whatsapp…) e addirittura anche tramite semplici sms telefonici,** con cui i malintenzionati cercano con l'inganno di fare "**abboccare**", appunto, alle loro proposte e sottrarre **dati anagrafici, di carta di credito e di accesso ai conti correnti online.**

Lo Smishing

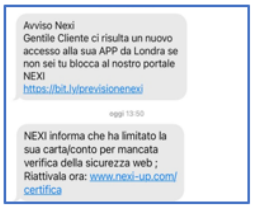
Lo Smishing, cioè le truffe via **Sms o messaggi di WhatsApp ecc.**
I malfattori inviano **un messaggio di testo che replica in modo più o meno credibile le richieste di un'organizzazione.**
Può essere ad esempio un corriere, un istituto bancario oppure un ecommerce. Lo scopo può essere duplice: **estorcere denaro o credenziali sensibili**


Hello David,
You still have 4 hours to take advantage of an exceptional 20% discount on all products with the promo code "SHOP20".
20% Discount with the code: SHOP20
⌛ Hurry, as this promotion will expire tonight at midnight. Don't miss out! ⌛


CONSEGNA DEL
PACCO SOSPESO!
Status: Fermo presso il centro di distribuzione (Imposta doganale in sospeso)
Potrebbero essere applicati costi di consegna
Il tuo codice di tracciamento:
D541472056IT
Programma La Consegna Ora


12:45
+39 350 9418964
SMS
sabato 15:11
Papà mi è caduto il cellulare in acqua ed ho cambiato numero scrivimi su whatsapp wa.me/+393509418964
SMS


E' stato effettuato un pagamento di 545,47 EUR con la carta ***** presso PayPal . Se non riconosci questo pagamento, bloccalo: https://


Avviso Nexi
Gentile Cliente ci risulta un nuovo accesso alla sua APP da Londra se non sei tu blocca al nostro portale NEXI
https://bit.ly/previsionenexi
oggi 13:50
NEXI informa che ha limitato la sua carta/conto per mancata verifica della sicurezza web ; Riattivala ora: www.nexi-up.com/certifica


ATTENZIONE TRUFFA!

Truffe online

Possiamo classificare le **frodi on line** in tre macro-categorie

- **Frodi negli acquisti:** vengono messi in vendita a prezzi notevolmente vantaggiosi oggetti che non arriveranno mai a domicilio o si riveleranno, nella migliore delle ipotesi, di pessima qualità**.**
- **Truffe affettive:** la vittima viene spinta a prestare aiuto economico a persone che asseriscono di essere in forte difficoltà personali
- **Finte lotterie:** un messaggio annuncia la vincita di una somma ingente ad una lotteria e con la quale viene chiesto di pagare una piccola somma per "rilasciare" le vincite, da versare su un conto personale estero.

...alcuni esempi...

Truffa codice WhatsApp a 6 cifre

La prima cosa da controllare è sicuramente il **numero del contatto**, spesso il criminale utilizza un numero temporaneo.

In realtà si tratta **del codice di verifica WhatsApp dell'account della vittima**. Una volta ricevuto, il truffatore utilizza il codice per registrare l'account del malcapitato su un nuovo dispositivo, prendendone così il pieno controllo.

Chiamate e messaggi da numeri sconosciuti

Sempre in relazione al numero di telefono, spesso può capitare di ricevere messaggi o chiamate da **numeri esteri con prefissi di Paesi lontani**. Queste sono quasi sempre chat false nelle quali qualcuno prova a guadagnarsi la tua fiducia iniziando a chattare con te amichevolmente.

Truffa telefonica con la tecnica wangiri

Il **wangiri** consiste in **una chiamata senza risposta da un numero estero**. Se la vittima richiama, viene automaticamente indirizzata verso **un numero a pagamento in grado di addebitare uno o due euro in pochi secondi**.

Ora si parla già di **wangiri 2.0**, ossia un'evoluzione per cui, quando la vittima richiama, viene **riprodotto il suono di un numero che squilla** facendo sì che creda di essere in attesa quando invece è già connesso alla chiamata e gli stanno rubando credito.

+216 (Tunisia): utilizzato per truffe chiamate "Wangiri", dove si viene richiamati con costi salatissimi.

+255 (Tanzania): usato per frodi legate a bollette esorbitanti.

+370 (Lituania): specializzato nel furto di dati personali.

+371 (Lettonia): noto per le truffe internazionali.

+373 (Moldavia): usato per richieste di pagamento urgenti.

+375 (Bielorussia): aggiunge una tariffa maggiorata durante la conversazione telefonica.

+218 (Libia): usato per frodi internazionali.

+381 (Serbia): la conversazione con l'operatore ha costi nascosti.

+383 (Kosovo): in realtà è un prefisso tunisino, richiamando, si pagano costi maggiorati.

+53 (Cuba) e +563 (Cile): numeri truffa a pagamento che sperano di essere richiamati.

+678 (Vanuatu) e +27 (Sudafrica): questi numeri sono in grado di rubare informazioni personali.

+33 (Francia): prevede una conversazione con costi maggiorati.

+218 (Libia): utilizzato anche per frodi internazionali.

Ovviamente non è detto che tutte le chiamate che provengono da questi Paesi siano un pericolo.

Chi sono le vittime più a rischio?

Privati con poca familiarità tecnologica: tendono a fidarsi più facilmente, questo li espone a un rischio maggiore.

Aziende con elevato volume di chiamate internazionali: organizzazioni come call center, uffici commerciali e team di assistenza clienti sono obiettivi preferiti dei truffatori.

Adolescenti: l'uso intensivo dello smartphone, la scarsa esperienza nel riconoscere truffe e la loro tendenza a non controllare i costi delle chiamate o a rispondere impulsivamente a notifiche rendono questa fascia di utenti una preda facile.

Come proteggersi?

- Per proteggerti, è importante **non richiamare né inviare messaggi ai numeri sconosciuti** che interrompono la chiamata.
- I numeri esteri sospetti devono essere bloccati, soprattutto se hanno prefissi poco familiari.
- Ci sono delle App gratuite che ti aiutano ad individuare il numero che ti chiama, come **Pagine Bianche, Pagine Gialle, Caller ID o Truecaller**

Una buona soluzione è utilizzare app antispam come Truecaller, che identifica le chiamate sospette segnalate nel suo database e avvisa l'utente in tempo reale

Per concludere

1. Se un messaggio sembra sospetto o troppo bello per essere vero, non cliccarci su, non condividerlo e non inoltrarlo.
2. Guarda sempre attentamente il link o il file prima di aprirlo perché può sembrare valido, ma in realtà potrebbe essere dannoso.
3. Se non hai la certezza della veridicità o della provenienza del messaggio che hai ricevuto, non inoltrarlo
4. Se non hai la certezza dell'identità di un contatto sconosciuto, poni una domanda personale per confermare la sua identità. Potresti anche fare una chiamata vocale o una videochiamata per verificare l'identità dell'altra persona.