Quarto incontro: giovedì 30/01/2025

Buono a sapersi…

- **Come formattare il testo di un messaggio di Whatsapp:**
  - individua la chat nella quale vuoi inviare un messaggio e digitalo nella barra
  - tieni premuto sulla parte del testo che vuoi formattare per selezionarla
  - clicca sui **(⋮)** nel menu che compare a fianco delle scritte Taglia, Incolla ecc. e seleziona l'opzione che desideri tra quelle che compaiono **Grassetto**, **Corsivo**, **Barrato** o **Monospaziato**, a seconda di come desideri formattare il testo.

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.

- **Come inviare una foto con l'aggiunta di un testo che puoi modificare**

  - Scegli la chat dalla quale vuoi mandare la foto. Nella barra per la scrittura del testo, clicca sul simbolo della macchina fotografica per **accedere alla fotocamera**. In questo modo puoi scegliere se scattare un'istantanea oppure scegliere una foto dalla **Galleria**.
  - Per poter scrivere sulla foto inerita devi cliccare sulla lettera **T** che si trova in alto nello schermo. Fatto questo ti appare la tastiera del tuo smartphone e un cursore al centro della foto, in modo da permetterti di scrivere tutto ciò che desideri.
  - Una volta composto il testo, per cambiare il font devi fare cliccare ancora sulla **T** in modo da scorrere tra i font disponibili. Ogni volta che clicchi ti permette di passare a quello successivo, quindi puoi provarli tutti prima di scegliere quello che preferisci. Tramite la barra colorata sulla destra inoltre, 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.
- È possibile anche selezionare l'icona "ritaglia" per potere poi selezionare una parte dell'immagine che voglio inviare.

- **Come aggiungere/ rimuovere un contatto ai Preferiti**

È possibile aggiungere un contatto che abbiamo salvato in Rubrica alla lista dei **Preferiti.**

- apri la Chat che ti interessa e clicca sui **(⋮)** in alto a destra per aprire il menù
- clicca su **Aggiungi a una lista**
- 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 in seguito altri contatti
- 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.
- puoi procedere allo stesso modo per archiviare un intero **Gruppo**. Anche in questo caso è sufficiente fare un **tap prolungato sul Gruppo** di tuo interesse e premere sulla stessa icona sempre in alto a destra.
- per rimuovere una chat archiviata basta fare lo stesso procedimento partendo dall'interno della scatola **Archiviate**, si selezionano le chat che voglio rimuovere dall'archivio poi clicco sempre sull'icona questa volta **della scatola con la freccia all'insù.**

- **Come difendersi dai truffatori su WhatsApp**

Le **truffe on line** sono un fenomeno criminoso molto diffuso, a molti di noi è sicuramente capitato di incappare in un tentativo di truffa perpetrato da un hacker.

Possiamo classificare le **frodi on line** in tre macro-categorie nelle quali ha un forte peso, rispetto ad altri fattori, l'identità assunta dal truffatore:

- **frodi negli acquisti,** vengono messi in vendita a prezzi notevolmente vantaggiosi oggetti che puntualmente non arriveranno a domicilio o si riveleranno, nella migliore delle ipotesi, di pessima qualità**;**
- **truffe affettive** la vittima viene spinta, attraverso una narrazione convincente, a prestare aiuto (quasi sempre economico) a persone che asseriscono di essere in forte difficoltà personali – ad esempio per un parente malato o in difficoltà– facendo leva sul rapporto di fiducia precedentemente stabilito;
- **finte lotterie:** si riceve una email o un SMS che 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.
  Oppure promesse di premi virtuali, fisici o monetari ottenibili con sforzo limitato o nullo, come buoni sconto di valore eccessivamente elevato ad esempio il **Buono Sconto Esselunga da €500 o €1000.**

Le frodi on line vengono effettuate con diverse modalità:

- **Phishing:** il truffatore utilizza un messaggio che, riferendo **problemi di registrazione o sicurezza**, invita a fornire i **propri dati di accesso** al servizio e altre informazioni sensibili di solito rimandando ad un sito web **solo apparentemente dell'istituto bancario**.
- **Vishing:** simulando l'esistenza di un call center, magari di una banca, il truffatore convince le vittime che è nel loro interesse, **fornire i propri dati all' operatore**.
- **Smishing:** la truffa consiste in un attacco alla sicurezza informatica basato sul **phishing** messo in atto con messaggi di testo inviati tramite cellulare, via **SMS, WhatsApp o Telegram**
- **Spoofing:** si tratta di un attacco informatico basato sulla **falsificazione dell'identità**. Il truffatore si impadronisce di una serie di dati col fine di impersonare qualcuno di attendibile e conosciuto dalla vittima.
- **Quishing:** ultima modalità in ordine di tempo ma non meno pericolosa delle precedenti, e utilizza i **QR code per ingannare gli utenti** e sottrarre loro informazioni sensibili. L'allarme mondiale è stato lanciato da alcuni istituti bancari, dal National Cyber Security Centre e dalla Federal Trade Commission. In Italia, ad esempio, è stata segnalata una campagna di quishing ai danni dei clienti Unicredit.

Tra le truffe online più diffuse in Italia che circolano su WhatsApp, vediamo qui di seguito quelle che hanno **suscitato particolare attenzione** da parte dei media e delle autorità:

1. **Truffa codice WhatsApp a 6 cifre**

La truffa del codice WhatsApp inizia quando il malintenzionato contatta un utente fingendosi un amico e sostenendo di avergli inviato per sbaglio il suo codice di verifica.
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.
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.

2. **Money muling**

Il **money muling** è una truffa tramite WhatsApp, Telegram ma anche Instagram in cui le vittime vengono ingaggiate per trasferire denaro illecito, con la proposta di una nuova opportunità di lavoro del tutto legale.
Il money muling è una truffa finanziaria che coinvolge utenti ignari nel trasferimento di denaro proveniente da attività illegali. I truffatori tramite WhatsApp contattano le vittime con una falsa offerta di lavoro che sembra legittima e ben retribuita. La proposta solitamente richiede alla persona di fare da intermediario per spostare denaro tra diversi conti bancari, presentandolo come parte di un incarico aziendale. In realtà, il denaro trasferito è **frutto di attività criminali**.
La vittima accetta di compiere questi trasferimenti, senza rendersi conto di essere coinvolta in un **meccanismo di riciclaggio di denaro** e di rischiare quindi conseguenze penali. Il money muling è anche una delle più comuni truffe su Telegram: in ogni caso, diffidate da offerte di lavoro che richiedono il trasferimento di fondi o l'uso di conti bancari personali, perché spesso si tratta di truffe.

3. **Truffa del figlio**

La truffa su WhatsApp del figlio sfrutta l'emotività e l'urgenza per ingannare le vittime. Il truffatore contatta l'utente da un numero sconosciuto, fingendosi il figlio o un parente

stretto, e sostiene di essere in difficoltà, spesso inventando una scusa come aver perso il telefono o essere stato coinvolto in un incidente. Utilizzando un tono di emergenza, **chiede denaro per risolvere la situazione immediata**, ad esempio per pagare una multa, coprire spese mediche o rimediare a un problema urgente. La vittima, in situazione di forte stress psicologico, invia velocemente il denaro **senza verificare l'identità del mittente**. I pagamenti vengono spesso richiesti tramite bonifici o metodi difficili da rintracciare, come carte prepagate. Una volta ricevuti i soldi, l'impostore sparisce.

4. Offerte di lavoro fasulle

Si tratta di uno dei più comuni messaggi truffa su WhatsApp e consiste nell'offrire un lavoro ben pagato. Il malfattore richiede alla vittima di depositare soldi su una piattaforma di criptovalute prima di sparire con il denaro.
È una truffa simile al **money muling** ma che non vede il coinvolgimento in operazioni di riciclaggio, mira solo a **sottrarre denaro con promesse di impieghi inesistenti**.
La vittima viene contattata tramite messaggi truffa WhatsApp e viene richiesta per un lavoro apparentemente regolare e ben remunerato. Per iniziare, però, i truffatori richiedono alla vittima di **registrarsi presso un broker** o un exchange di criptovalute, e di effettuare un deposito di denaro, giustificandolo come necessario per avviare il lavoro o per accedere agli strumenti necessari per l'impiego. Una volta effettuato il pagamento, la vittima scopre che **il lavoro non esiste e i fondi sono irrecuperabili**. In alcuni casi, il truffatore continua a chiedere ulteriori pagamenti, adducendo scuse come tasse aggiuntive o commissioni necessarie per il prelievo dei presunti guadagni accumulati.

Ci sono dei segnali che indicano che hai ricevuto un messaggio sospetto o che il mittente non è affidabile. Presta attenzione a questi indizi:

- Errori ortografici o grammaticali
- Richiesta di toccare un link o di attivare nuove funzioni attraverso un link o scaricare un'app
- Richiesta di condividere informazioni personali, come dati della carta di credito e del conto corrente, data di nascita o password
- Richiesta di inoltrare un messaggio
- Richiesta di denaro o pagamento per poter usare WhatsApp
- Il truffatore finge di essere qualcuno che conosci

- Il messaggio è relativo alla lotteria, al gioco d'azzardo, a un lavoro, a un investimento o a un prestito
- La persona inizia a chattare con te per guadagnarsi la tua fiducia prima di chiedere informazioni personali

IN SINTESI:

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 del messaggio che hai ricevuto o non ne conosci l'autore, 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 confermare l'identità dell'altra persona.**

5. **Non condividere MAI le tue credenziali come password, pin o codici di sicurezza senza verificare prima la fonte della richiesta.**