COMUNE DI JESI

Comitato di Quartiere “SAN FRANCESCO”

Verbale n. 12 del 24/10/2025

Il giorno 24/10/2025 alle ore 21 presso la sede del Comitato di Quartiere SAN FRANCESCO, sita in Piazza San Francesco 1, a seguito della convocazione della Presidente Cerioni Maria Luisa si è svolta la seconda l’Assemblea Generale Pubblica per l’anno 2025, assemblea congiunta con il Comitato di Quartiere Coppi Giardini.

All’Assemblea per il nostro comitato risultano presenti i Signori:

CARICA	NOMINATIVO	Presente/Assente
Presidente	CERIONI MARIA LUISA	Presente
Vice Presidente	MANZOTTI CINZIA	Presente
Componente Segretario	MORETTI MAURO	Presente
Componente	GARZI DANIELE	Presente
Componente	CANAFOGLIA PAOLO	Presente
Componente	DUCA LAURA	Presente
Componente	BECCACECI ENZO	Presente
Componente	MONTECCHIANI GIORGIO	Presente
Componente	POLITA MIRKO	Assente

La tematica trattata in Assemblea è un problema che interessa tutti i cittadini, I PERICOLI DEL WEB.

Alle ore 21:15 la Presidente Cerioni Maria Luisa verificata la presenza dei cittadini intervenuti fa un saluto di benvenuto per il nostro comitato.

Anche la Presidente del comitato Coppi Giardini Rosita Giampieretti porge il proprio saluto ai presenti in sala. Le due presidenti del comitato ringraziano la CNA per il prezioso supporto.

Un saluto viene esplicitato anche dall’assessore Paola Lenti presente all’importante riunione che

ringrazia tutti i presenti che hanno saputo cogliere l’importanza di tale Assemblea.

La sopra citata tematica è trattata dalla dott.ssa Francesca Giuliani responsabile del servizio Privacy e Cybersecurity della CNA di Ancona che ci illustra, attraverso slaid.

La dott.ssa Giuliani ci fa presente che le truffe del web sono crimini informatici che sfruttano la manipolazione per rubare denaro o informazioni sensibili.

Il rischio di rimanere coinvolti in una truffa riguarda tutti e non va sottovalutato, anche perché spesso le frodi vengono messe in atto da veri "professionisti". I truffatori spesso fanno leva sulla buona fede delle persone e utilizzano diversi metodi per ingannare le possibili vittime come, ad esempio, fingere di chiamare per conto di enti pubblici.

Si può riassumere in generale quanto esposto dalla dott.ssa Giuliani come segue:

1. Riconoscere la provenienza di email, SMS e telefonate fraudolenti

La maggior parte delle truffe telematiche è veicolata da telefonate, email ed SMS che hanno tutta l'aria di provenire da enti conosciuti e fonti affidabili, spesso grandi aziende, banche e perfino enti pubblici. Quindi la prima cosa da fare è verificare la provenienza delle comunicazioni, in particolare di quelle che richiedono dati personali, credenziali, codici dispositivi o che invitano a cliccare su un link. Dobbiamo sempre verificare l'indirizzo di provenienza delle email e i numeri di telefono da cui provengono le telefonate e SMS.

Ad esempio, verificare che il numero di telefono appartenga effettivamente all'azienda cui dice di far parte l'interlocutore che abbiamo di fronte da cui dovrebbe provenire l'smsn. Controllare anche attentamente l'indirizzo del mittente delle email e il testo dei link che contengono: spesso i truffatori usano testi che differiscono di poco da quelli ufficiali delle aziende. Anche il testo di email e messaggi può darci indicazioni sulla loro natura fraudolenta, poiché spesso contengono errori di ortografia e di sintassi.

2. Non avere fretta

Molto spesso le truffe fanno leva sul senso di urgenza e sull'invito ad agire immediatamente. Ad esempio la comunicazione potrebbe avvertire di un servizio in scadenza, di un pagamento non andato a buon fine o della possibilità che un conto corrente venga bloccato e invita ad agire in fretta o addirittura immediatamente.

In qualsiasi contesto regolare si ha sempre a disposizione del tempo per effettuare il rinnovo di un servizio o per intervenire su un'operazione di pagamento. Perciò bisogna non agire d'impulso e prendere il tempo necessario per verificare, ad esempio attraverso una telefonata all'azienda che ci fornisce il servizio.

3. Fare attenzione alle proposte particolarmente vantaggiose o alle promesse di denaro o guadagni facili

Offerte a prezzi stracciati, prestiti stranamente vantaggiosi e proposte sospette relative al trading online potrebbero rivelarsi delle truffe. Dobbiamo verificare sempre la bontà dell'offerta paragonandola ad offerte simili e cercando informazioni sull'offerente.

4. Verificare le pagine web su cui si effettuano i propri acquisti

Nelle pagine web che propongono acquisti è sempre bene fare attenzione alla presenza di alcuni elementi di base, come ad esempio: l'indirizzo "https", la presenza del lucchetto nella barra di indirizzo (che indica che il sito è protetto da sistemi di sicurezza internazionali) e dei dati del venditore, come il numero di Partita IVA, la sede legale della società, i recapiti per il contatto, le condizioni generali di vendita, o un sistema di pagamento sicuro che riporti chiaramente i costi di spedizione. Ci ricorda la dott.ssa Giuliani inoltre che, sul sito dell'Agenzia delle Entrate, possiamo verificare i dati fiscali riportati nella pagina web.

5. Usare la massima cautela nella gestione di dati, informazioni e documenti personali

Se ci vengono richiesti di comunicare dati personali o sensibili o di inviare copia di documenti personali, dobbiamo porre la massima attenzione: inviare copia dei nostri documenti solo se necessario e in un contesto affidabile e accertarsi dell'identità dell'interlocutore.

6. Mantenere software e password sempre aggiornati

La dott.ssa Giuliani si è raccomandata che, oltre a modificare periodicamente le password, è necessario che i sistemi operativi e le applicazioni di PC e smartphone siano sempre aggiornati. In particolare, verificare che il browser che si utilizza sia aggiornato ed eliminare periodicamente i cookie e i file temporanei utilizzando gli appositi strumenti del browser.

7. Prestare attenzione alle truffe basate sull'intelligenza artificiale

L'uso crescente dell'intelligenza artificiale rende le frodi sempre più credibili e sofisticate. È possibile imbattersi in messaggi vocali o video apparentemente autentici, in cui viene riprodotta la voce o l'immagine di una persona nota o di un proprio contatto, con richieste ingannevoli di denaro o informazioni personali. La dott.ssa Giuliani ci fa presente di verificare sempre la fonte di comunicazioni inusuali, anche se sembrano provenire da persone conosciute, e di diffidare di richieste anomale connotate dal carattere di urgenza.

8. Conoscere lo spoofing e le nuove tecniche di phishing evoluto

Lo spoofing è una tecnica attraverso cui si falsifica l'identità del mittente, facendo apparire gli indirizzi e-mail o i numeri di telefono da cui provengono le comunicazioni come appartenenti a soggetti conosciuti o affidabili. Le tecniche di phishing più evolute permettono invece di replicare con grande precisione grafica e linguistica i siti ufficiali di enti, banche o servizi digitali. Dobbiamo quindi controllare sempre l'indirizzo web completo, evitare di cliccare su link sospetti e digitare direttamente l'URL nel browser. In caso di dubbio, dobbiamo contattare direttamente il presunto mittente tramite i canali ufficiali.

9. Diffidare di offerte di investimento da presunti esperti sui social

Sempre più spesso, le truffe legate al trading e agli investimenti viaggiano attraverso i social network, dove falsi esperti promettono guadagni elevati e in tempi brevi. Questi soggetti, che spesso si presentano con profili curati e testimonianze fittizie, invitano a versare denaro su piattaforme non autorizzate o a fornire i propri dati bancari. Prima di aderire a qualsiasi proposta di investimento, dobbiamo verificare che il promotore sia iscritto a registri ufficiali come quelli della Consob o dell'IVASS, e informarci sempre su eventuali segnalazioni di truffa.

La dott.ssa Giuliani fa presente che essere vittima di una truffa è un'evenienza che può capitare a chiunque. Se, nonostante tutte le precauzioni messe in atto, si è vittima di una truffa è sempre possibile attivarsi per denunciare quanto accaduto alle forze dell'ordine. Nel caso si tratti di una truffa avvenuta online, è opportuno fare riferimento alla Polizia Postale che ha competenza sui reati informatici. E' necessario raccogliere tutto il materiale che può provare quanto accaduto. Inoltre, se temiamo di essere rimasti vittima di una truffa bancaria, dobbiamo contattare il nostro Istituto di credito per bloccare le carte di pagamento e per verificare che non vi siano state disposizioni di pagamento fraudolente.

I cittadini presenti in sala sono intervenuti, compreso il nostro componente del comitato Enzo Beccaceci, per chiedere chiarimenti sulla tematica e i possibili rimedi che le autorità governative ed europee hanno in atto di prendere per evitare tali inconvenienti incresciosi.

Si conclude la serata con un caloroso applauso alla dott.ssa Francesca Giuliani.

La Presidente fa presente che il prossimo Consiglio Direttivo sarà il giorno 5 novembre 2025 alle ore 21 al quale possono partecipare tutti i cittadini.

La Presidente alle ore 23,30 dichiara terminata l'assemblea pubblica ringraziando di nuovo tutti i presenti.

Il presente verbale, debitamente sottoscritto, sarà scansionato e inviato in copia pdf alla PEC del Comune di Jesi.

IL/LA SEGRETARIO/A	**IL/LA PRESIDENTE**
.....	.....