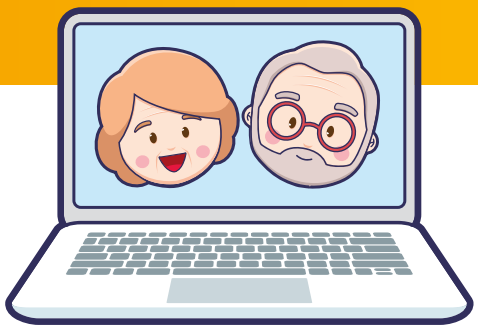


NONNITEC

nonni nel digitale

in partenariato:

Ministero del lavoro e delle politiche sociali
Direzione Generale del terzo settore e della responsabilità sociale delle imprese

Regione Abruzzo
Dipartimento Lavoro - Sociale
Servizio Programmazione Sociale - dpg022
Ufficio Terzo Settore

COMUNE DI
MOSCIANO SANT'ANGELO

Associazione Pro Loco Montone APS

"Uniti per la vita"

Volontari Protezione Civile Gran Sasso d'Italia

WWW.NONNITEC.IT

SOMMARIO

COMUNE DI MOSCIANO SANT'ANGELO

Desidero esprimere il mio sincero ringraziamento alla Pro Loco Montone per questa splendida iniziativa che, attraverso il progetto "NonniTec: nonni nel digitale" mira a ***includere la terza età nel mondo digitale****, una sfida e un'opportunità fondamentale per la nostra comunità.*

Viviamo in un'epoca in cui la tecnologia non è solo uno strumento di innovazione, ma un mezzo indispensabile per comunicare, accedere a servizi e informazioni, e migliorare la qualità della vita quotidiana. È quindi cruciale offrire ai nostri anziani la possibilità di acquisire le competenze necessarie per navigare con sicurezza e consapevolezza in un mondo sempre più interconnesso.

Grazie alla collaborazione dei circoli anziani, della Protezione Civile Gran Sasso d'Italia di Mosciano Sant'Angelo, e delle parrocchie del nostro territorio, questo progetto si pone come ***esempio virtuoso di sinergia tra associazioni, istituzioni e cittadini****.*

Credo fermamente che iniziative come questa non solo aiutino a contrastare il divario digitale, ma rappresentino anche un modo concreto per combattere la solitudine, rafforzare i legami intergenerazionali e promuovere una partecipazione attiva alla vita sociale.

Un plauso quindi alla Pro Loco Montone e a tutti i partner coinvolti per aver concepito un progetto di così grande rilevanza sociale, e un augurio di buon lavoro a tutti i partecipanti.

Mirko Rossi

Vicesindaco del Comune di Mosciano Sant'Angelo
con delega alle Tecnologie e Servizi Digitali

PRO LOCO MONTONE APS

È con grande entusiasmo che la Pro Loco Montone presenta il progetto "NonniTec: nonni nel digitale", questa iniziativa, nata dalla volontà di offrire strumenti concreti per la tutela e la sicurezza delle persone più vulnerabili della nostra comunità. La crescente diffusione di truffe, sia online che offline, rappresenta una minaccia reale che può colpire chiunque, ma che spesso vede come vittime privilegiate gli anziani. È per questo motivo che la ***Pro Loco Montone****, insieme ai preziosi partner quali la* ***Protezione Civile Gran Sasso d'Italia ODV e il Circolo Sportivo Anziani Invalidi Uniti per la Vita – Sezione di Sant'Alessandro APS****, ha deciso di promuovere un progetto di sensibilizzazione e prevenzione, in collaborazione con il* ***Comune di Mosciano Sant'Angelo****.*

*Questo vademecum nasce proprio per fornire informazioni chiare e pratiche, affinché ognuno di voi possa riconoscere ed evitare i raggiri più comuni. Grazie al finanziamento ottenuto nell'ambito dell'****Avviso pubblico per il finanziamento di iniziative e progetti di rilevanza regionale promossi da organizzazioni di volontariato, associazioni di promozione sociale e fondazioni del Terzo Settore, reso possibile dalle Risorse ADP 2022 – 2024 della Regione Abruzzo****, abbiamo potuto concretizzare un'iniziativa che ci auguriamo possa fare la differenza nella vita di molte persone.*

Ringrazio di cuore tutti i soggetti coinvolti nel progetto per il loro impegno e la loro dedizione. È solo attraverso la collaborazione tra istituzioni, associazioni e cittadini che possiamo costruire una comunità più sicura e consapevole. Vi invito a leggere con attenzione questo vademecum e a condividerlo con chiunque possa beneficiarne: ***la prevenzione è la nostra migliore difesa****.*

Eleonora Corona

Presidente della Pro Loco Montone

INTRODUZIONE

SCOPO E UTILITÀ DEL VADEMECUM

Questo vademecum nasce con l'intento di fornire una guida semplice e pratica per chi desidera avvicinarsi al mondo digitale in modo sicuro e consapevole. La tecnologia, sebbene possa sembrare distante e complessa, è oggi una componente essenziale della nostra quotidianità: dalle comunicazioni rapide e immediate, come le videochiamate con amici e parenti lontani, alla possibilità di accedere a informazioni, servizi sanitari e intrattenimento, il digitale offre infinite possibilità. È importante per questo conoscere in maniera approfondita i rischi e le insidie, che possono minare la sicurezza e la tranquillità di chi si avvicina a Internet e alle tecnologie.

Il nostro obiettivo è fornirti strumenti chiari per capire e sfruttare appieno il potenziale del digitale, difendendoti al contempo da pericoli come truffe online e offline. Con un approccio semplice e diretto, questo vademecum copre tutto ciò di cui hai bisogno: dall'alfabetizzazione digitale, per aiutarti a navigare in sicurezza, al riconoscimento delle truffe più comuni, fino ai consigli per instaurare un dialogo costruttivo con i più giovani della famiglia. Potrai così sentirti non solo più sicuro e consapevole, ma anche parte attiva di un mondo in continua evoluzione.

L'IMPORTANZA DI SENTIRSI AL PASSO CON IL MONDO DIGITALE

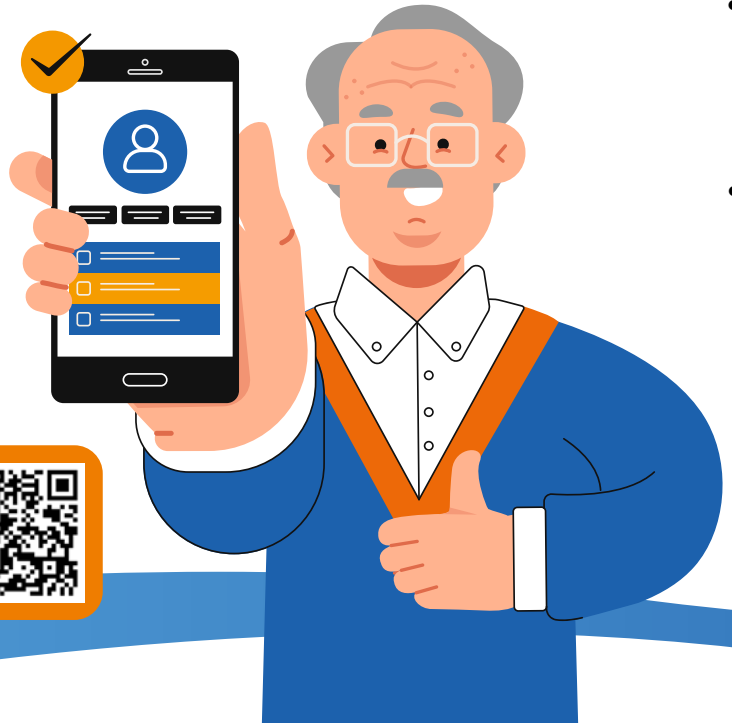
Essere al passo con il mondo digitale significa **mantenere viva la propria curiosità e desiderio di apprendere**. Il **digitale** può sembrare a volte un terreno difficile da esplorare, fatto di linguaggi nuovi e tecnologie complesse, ma in realtà è una **risorsa preziosa che consente di superare barriere**, comunicare con maggiore facilità e restare connessi con il mondo che ci circonda. **Viviamo in un'epoca in cui il cambiamento è rapido e continuo, e sentirsi parte di questa trasformazione non solo rafforza la nostra autonomia e sicurezza, ma favorisce il benessere emotivo e sociale.**

Imparare a utilizzare dispositivi come smartphone, computer o tablet, sapere come proteggere i propri dati e conoscere le basi della sicurezza online ci permette di affrontare con maggiore serenità le sfide quotidiane. Lo strumento digitale, inoltre,

può diventare **un ponte per rafforzare i rapporti intergenerazionali**: dialogare con i giovani, comprendere le loro passioni online e condividere saggezza ed esperienze personali può arricchire le relazioni familiari e aprire nuove strade di comprensione reciproca.

Ma il benessere non si ferma solo alla connessione sociale. L'accesso a risorse e strumenti digitali può migliorare la nostra salute fisica e mentale. Esistono applicazioni per il monitoraggio del benessere fisico, programmi di meditazione, libri digitali e corsi online su un'infinità di argomenti. Tutto questo stimola la mente, riduce lo stress e offre opportunità per mantenersi attivi. **Essere digitalmente inclusi significa vivere con maggiore autonomia, sapere come difendersi dai rischi e godere di tutti i benefici che il mondo moderno ci offre.**

Questo vademecum vuole essere il tuo compagno di viaggio in questo percorso di scoperta e crescita. Non si tratta solo di acquisire competenze tecniche, ma di scoprire come **il mondo digitale possa arricchire la tua vita, aumentare la tua sicurezza e permetterti di vivere il presente con una marcia in più**. Che tu sia un principiante o abbia già qualche esperienza, troverai qui spunti e consigli per affrontare il futuro con fiducia e curiosità.



CAPITOLO 1: ALFABETIZZAZIONE DIGITALE

NOZIONI DI BASE DEL DIGITALE

Internet rappresenta una delle più grandi innovazioni della storia umana, una rete globale che collega persone, dispositivi e informazioni. Per comprenderlo meglio, Internet potrebbe essere paragonato ad una rete stradale che collega città, negozi, biblioteche e piazze virtuali. Ogni sito web è una destinazione e ogni ricerca su un motore di ricerca come Google è il navigatore, che ti guida verso l'informazione o il servizio desiderato.
Ma come accedere a questa rete? Attraverso dispositivi come computer, smartphone e tablet.
Un passo fondamentale per iniziare a utilizzare questi dispositivi è comprendere il loro funzionamento di base. Ad esempio:

- **Computer:** al suo interno è presente un sistema operativo (Windows o macOS) che ti permette di accedere a programmi e file. Usare il mouse o il touchpad ti consente di spostarti tra le varie opzioni sullo schermo.
- **Smartphone:** sono dotati di sistemi operativi come Android e iOS sono progettati per essere intuitivi. Le applicazioni (o "app") sono rappresentate da icone che puoi toccare per aprire. Un'App, abbreviazione di "applicazione", è un programma che si può scaricare sul telefono o sul tablet per svolgere diverse attività. Le App possono servire, ad esempio, per comunicare con i propri cari, fare acquisti, leggere notizie, giocare o gestire promemoria. Esse sono progettate per essere semplici da usare, con comandi chiari

e pulsanti ben visibili, per aiutarti nella vita di tutti i giorni.

- **Tablet:** un dispositivo elettronico portatile con uno schermo touchscreen, che permette di navigare su Internet, leggere e inviare email, guardare video, fare videochiamate e utilizzare applicazioni di vario tipo. Ha le funzionalità di un computer, ma è più leggero e facile da usare, perché si controlla semplicemente toccando lo schermo con le dita. È ideale per chi vuole un dispositivo pratico da usare a casa o in viaggio, senza la complessità di un computer tradizionale.
- **Smart TV:** un televisore connesso a Internet che permette di accedere a contenuti online senza bisogno di dispositivi aggiuntivi. Oltre ai canali televisivi tradizionali, una Smart TV consente di guardare film e serie su piattaforme di streaming come Netflix, Prime Video e YouTube, navigare sul web, ascoltare musica e scaricare applicazioni.
- **Console di gioco**, come **PlayStation** o **Xbox**, sono progettate per giocare ai videogiochi su un televisore o uno schermo. Funzionano con giochi scaricabili o su disco e si controllano tramite un **joystick** o un **gamepad**, che permette di muoversi e interagire con il gioco. Alcune offrono anche il gioco online, per sfidare amici o altri giocatori da tutto il mondo.

È importante imparare a configurare i propri dispositivi. Al primo utilizzo, sarà necessario seguire una procedura guidata per impostare la lingua, il fuso orario e connettersi a una rete Wi-Fi. Queste impostazioni iniziali garantiscono che l'apparecchio sia pronto per essere usato.

NAVIGARE ONLINE IN SICUREZZA

Navigare su Internet può essere una straordinaria esperienza di scoperta, ma richiede anche una certa attenzione per evitare truffe e problemi di sicurezza. La prima regola è utilizzare browser affidabili, come Google Chrome o Firefox, che ti permettono di accedere a siti web ed integrano strumenti per proteggerti, come l'indicazione della sicurezza di un sito tramite un lucchetto accanto all'indirizzo web. Un sito sicuro inizia con "https://", dove la "s" indica che la connessione è protetta. Prima di inserire dati personali o sensibili, come il numero della carta di credito su un negozio online, controlla sempre che l'indirizzo inizi con "https://" e che il lucchetto sia presente. Se il sito appare sospetto o non sicuro, è meglio evitare di utilizzarlo.

CREARE PASSWORD SICURE

La gestione delle password è un altro elemento cruciale per proteggere i tuoi account. Una buona password dovrebbe essere:

- **Lunga almeno 8 caratteri**, ma preferibilmente più lunga.
- **Composta da lettere maiuscole e minuscole**, numeri e simboli speciali.
- **Unica per ogni account**. Evita di usare la stessa password per più siti o servizi.

Un buon metodo per creare una password efficace è quello della **frase facile da ricordare**, che rende la password più sicura e difficile da indovinare, ma allo stesso tempo facile da ricordare per te.

ESEMPIO PRATICO:

1. Scegli una frase che ti è familiare, ad esempio:
"Oggi il meteo promette bel tempo!"

2. Prendi le iniziali di ogni parola:
➡ oimpbt

3. Alterna maiuscole e minuscole per maggiore sicurezza:
➡ OiMpBt

4. Aggiungi il numero di lettere per ogni parola, ad esempio, "oggi" ha 4 lettere, "il" 2 lettere, "meteo" 5 lettere" ecc.
➡ OiMpBt425835

5. Aggiungi un simbolo speciale (es. !, ?, #) per aumentare la complessità:
➡ OiMpBt425835!

Ora hai una password lunga, complessa e difficile da indovinare, ma che per te è facile da ricordare perché deriva da una frase significativa.

Un vantaggio di questo metodo è che puoi segnare la frase originale su un foglietto, perché solo tu conosci il trucco per trasformarla nella tua password!

Per una maggiore protezione, puoi utilizzare un gestore di password, uno strumento che genera e salva in modo sicuro le tue credenziali.

L'autenticazione a due fattori (2FA), inoltre, è un metodo di sicurezza che aggiunge un ulteriore livello di protezione agli account online, essa, infatti, per effettuare l'accesso richiede due dei tre fattori, di seguito, per accedere a un account:

- **Qualcosa che sei** (es. riconoscimento facciale o impronta digitale)
- **Qualcosa che sai** (es. password, login)
- **Qualcosa che hai** (es. un codice inviato via SMS o generato da un'app su un dispositivo a cui hai facile accesso)

Questo metodo protegge l'account anche se la password viene rubata.

PROTEGGERE IL PROPRIO DISPOSITIVO

Mantenere il tuo dispositivo protetto è fondamentale per una navigazione sicura. Ecco come fare:

- **Installa un buon antivirus**: questo software ti aiuta a prevenire e rimuovere virus, malware e altre minacce digitali.
- **Aggiorna regolarmente il sistema operativo e le app**: gli aggiornamenti spesso includono correzioni di sicurezza che proteggono il tuo dispositivo da nuove minacce.
- **Evita di cliccare su link sospetti**: ricevere email, messaggi via SMS o WhatsApp con link è comune. Se non sei sicuro della loro provenienza, non cliccarli e nel dubbio, nel caso in cui tu conosca il mittente contattalo direttamente chiedendo chiarimenti.

ATTENZIONE A EMAIL E MESSAGGI!

Le truffe online spesso arrivano tramite email o messaggi. Questi possono sembrare provenire da aziende affidabili, ma po-

trebbero cercare di ingannarti. Fai attenzione a:

- **Mittenti sconosciuti o sospetti**
- **Messaggi che ti chiedono di inserire informazioni personali o bancarie**
- **Errori grammaticali o grafici** nei messaggi, spesso segno di una truffa

Se hai dubbi, non cliccare su link o allegati.

Ricorda: banche, Poste Italiane e altri enti ufficiali non chiedono mai di fornire dati sensibili tramite email, telefono o SMS. Nessuna comunicazione ufficiale richiederà di inserire il numero di conto corrente, il codice PIN, la password di accesso ai servizi online o i codici di sicurezza temporanei ricevuti via SMS. Anche la richiesta di informazioni personali riservate o credenziali bancarie attraverso questi mezzi deve essere considerata un segnale d'allarme.

CAPITOLO 2: COMUNICAZIONE DIGITALE

La comunicazione digitale ha trasformato il modo in cui interagiamo con gli altri. Piattaforme come le email, i social network e le app di messaggistica ci consentono di rimanere connessi con amici e familiari, ovunque si trovino.

EMAIL: COMUNICARE IN MODO FORMALE E SICURO

L'email (o posta elettronica) è uno dei metodi più comuni per inviare messaggi, documenti e foto in modo rapido. Creare un account email è il primo passo per entrare nel mondo digitale. Piattaforme come Gmail, Outlook e Yahoo offrono servizi gratuiti e facili da usare. Per configurare un account Gmail, ad esempio, basta visitare il sito ufficiale (https://workspace.google.com/intl/it/gmail/), fare clic su "Crea account" e seguire le istruzioni per inserire nome, cognome, password e altre informazioni di base.
Una volta creato il tuo account, puoi inviare un'email scrivendo l'indirizzo del destinatario, un oggetto (che riassuma il contenuto del messaggio) e il testo. Le email sono particolarmente utili per comunicazioni formali, come richieste di informazioni o invio di documenti ufficiali.
È importante prestare attenzione alla sicurezza, evita di aprire allegati o link provenienti da mittenti sconosciuti, poiché potrebbero contenere virus. Se ricevi un'email che ti sembra sospetta, controlla sempre il mittente e cerca eventuali errori grammaticali o grafici, segnali tipici di truffe online.

APP DI MESSAGGISTICA: IMMEDIATEZZA E SEMPLICITÀ

Le applicazioni di messaggistica, come WhatsApp e Telegram, sono strumenti ideali per comunicare in modo rapido e intuitivo. Permettono di inviare messaggi di testo, foto, video, messaggi vocali e persino documenti. Queste app sono gratuite e facili da configurare: basta scaricarle dallo store del tuo smartphone (Play Store per Android o App Store per iPhone), registrarti con il tuo numero di telefono e iniziare a comunicare.
Le app di messaggistica offrono anche funzioni avanzate, come la possibilità di creare gruppi per condividere messaggi con più persone contemporaneamente, ad esempio, si può creare un gruppo familiare per condividere aggiornamenti, foto e notizie. Per proteggere la tua privacy, assicurati di controllare le impostazioni dell'app. Puoi decidere chi può vedere il tuo stato, la tua foto profilo e il tuo ultimo accesso. Molte app, inoltre, come WhatsApp, utilizzano la crittografia end-to-end, che protegge i tuoi messaggi rendendoli leggibili solo a te e al destinatario; tuttavia, nonostante questa forma di tutela, evita sempre di condividere dati personali tramite messaggi.

Puoi, inoltre, proteggere il tuo account di WhtasApp attivando la **verifica in due passaggi**, una funzionalità di sicurezza che aggiunge un ulteriore livello di protezione. Attivandola, sarà necessario inserire un codice PIN ogni volta che si registra nuovamente l'account su un nuovo dispositivo, riducendo così il rischio di accessi non autorizzati.

Per attivare la verifica in due passaggi su WhatsApp, segui questi passaggi:

1. Apri WhatsApp sul tuo smartphone e accedi alle **Impostazioni**.
2. Seleziona la voce **Account**.
3. Tocca l'opzione **Verifica in due passaggi**.
4. Premi il pulsante **Attiva** per avvia la configurazione.
5. Inserisci un codice PIN a sei cifre che verrà richiesto periodicamente e ogni volta che si tenta di registrare l'account su un nuovo dispositivo.
6. Conferma il codice PIN digitandolo una seconda volta.
7. Inserisci un indirizzo email valido, che sarà utilizzato per recuperare il codice PIN nel caso in cui venga dimenticato. Questo passaggio è opzionale, ma fortemente consigliato per evitare di perdere l'accesso all'account.
8. Completata la configurazione, premi **Salva** o **Fine** per attivare la funzione.

Da questo momento, la verifica in due passaggi sarà attiva e ogni tentativo di accesso all'account da un nuovo dispositivo richiederà l'inserimento del codice PIN scelto. Per garantire la massima sicurezza, è importante non condividere il PIN con nessuno e annotarlo in un luogo sicuro.

SOCIAL NETWORK: CONNETTERSI E CONDIVIDERE

I social network, come Facebook e Instagram, sono ottimi per rimanere in contatto con amici e familiari e seguire gli aggiornamenti delle loro vite; per utilizzarli in sicurezza e tutelare le tue informazioni personali è fondamentale configurare corretta-

mente le impostazioni del tuo profilo. Per farlo, ad esempio su Facebook, segui questi passi semplici:

1. **Accedi alle impostazioni sulla privacy**: entra nel tuo profilo e clicca sull'icona del menu (spesso rappresentata da tre linee o un ingranaggio). Cerca la sezione dedicata alla privacy.
2. **Controlla chi può vedere i tuoi post**: nella sezione "Chi può vedere i contenuti che condividi?", scegli tra opzioni come "Solo amici" o "Solo io" per evitare che persone sconosciute accedano alle tue informazioni.
3. **Rivedi il tuo profilo pubblico**: Facebook ti permette di vedere come appare il tuo profilo agli estranei, in questo modo puoi assicurarti che nessuna informazione personale sia visibile.
4. **Gestisci i tag nelle foto e nei post**: nella sezione dedicata ai tag, attiva l'opzione che ti consente di approvare o evitare ogni tag prima che venga mostrato sul tuo profilo.
5. **Imposta restrizioni su richieste e messaggi**: puoi decidere chi può inviarti richieste di amicizia o messaggi, limitandolo, ad esempio, solo agli amici degli amici.
6. **Attiva le notifiche per accessi sospetti**: abilita l'opzione che ti avvisa se qualcuno tenta di accedere al tuo account da un dispositivo sconosciuto.

7. **Attiva l'autenticazione a due fattori**: attivando questa funzione ogni volta che tenti di accedere al tuo account da un nuovo dispositivo o browser, ti verrà richiesto un codice di verifica temporaneo. Questo codice viene inviato tramite SMS, email riducendo il rischio che qualcuno possa appropriarsi del tuo profilo anche se ha ottenuto la tua password.

Seguendo questi passaggi, puoi utilizzare i social network in modo più sicuro e controllare chi può vedere i tuoi contenuti. Ricorda di verificare regolarmente queste impostazioni, poiché le piattaforme possono aggiornare le loro regole e opzioni.

VIDEOCHIAMATE: VICINI ANCHE DA LONTANO

Le videochiamate sono uno degli strumenti più apprezzati per mantenere i rapporti con amici e familiari, soprattutto quando le distanze fisiche rendono difficile vedersi di persona. Piattaforme come WhatsApp Zoom, Skype, Google Meet e Microsoft Teams ti permettono di parlare e vedere i tuoi cari in tempo reale.

Per utilizzare queste applicazioni, è necessario scaricarle sul tuo dispositivo e registrarti con un'e-mail o un numero di telefono. Una volta configurata l'app, puoi avviare una videochiamata selezionando un contatto o invian-

do un link di invito. Nella piattaforma Zoom, ad esempio, puoi creare una riunione e condividere il link con i partecipanti, che potranno unirsi cliccando sul link stesso.
Le videochiamate sono utili non solo per comunicare con la famiglia, ma anche per partecipare a corsi online, riunioni o eventi virtuali. Per un'esperienza ottimale, assicurati di avere una connessione Internet stabile, scegli un ambiente tranquillo e ben illuminato e utilizza auricolari o cuffie per migliorare la qualità dell'audio.

APPLICAZIONI UTILI PER LA COMUNICAZIONE E LA GESTIONE DELLA VITA QUOTIDIANA

Oltre alle email, ai social e alle app di messaggistica, esistono molte altre applicazioni che possono semplificare la tua vita quotidiana:

- **Calendari e promemoria**: app come Google Calendar ti aiutano a organizzare appuntamenti, eventi e ricorrenze, inviandoti notifiche per non dimenticare nulla.
- **Mappe e navigatori**: Google Maps o Waze ti permettono di trovare percorsi, luoghi di interesse e indicazioni per arrivare a destinazione.
- **Traduttori**: app come Google Translate possono essere utili per tradurre frasi o parole in altre lingue.
- **App di salute**: molti smartphone includono app per monitorare l'attività fisica, la qualità del sonno o persino i parametri di salute, come la pressione o il battito cardiaco, se collegati a dispositivi specifici.

CAPITOLO 3:
TRUFFE COMUNI ONLINE E OFFLINE

INTRODUZIONE: LA REALTÀ DELLE TRUFFE

Le truffe, sia online che offline, sono diventate un problema sociale rilevante, colpendo in modo particolare le persone anziane. La loro diffusione è alimentata da due fattori principali: l'aumento della digitalizzazione e la capacità dei truffatori di adattarsi rapidamente a nuovi contesti. L'obiettivo dei truffatori è sempre lo stesso: **guadagnare la tua fiducia per ottenere denaro o informazioni personali.**

Il digitale ha introdotto un nuovo livello di complessità. Email, SMS e social network sono strumenti potentissimi per comunicare, ma vengono sfruttati anche da criminali per frodi su larga scala. Allo stesso tempo, le truffe tradizionali non sono scomparse: falsi tecnici, rappresentanti continuano a ingannare le persone vulnerabili.

Per affrontare questo fenomeno, è fondamentale apprendere i metodi usati dai truffatori, imparare a riconoscerli e adottare comportamenti prudenti.

TRUFFE ONLINE: UNA MINACCIA INVISIBILE

PHISHING: QUANDO IL TRUFFATORE TI SCRIVE

Il phishing è uno dei metodi più utilizzati dai criminali digitali. Si basa sull'invio di email fraudolente che imitano comunicazioni ufficiali.

Le email di phishing spesso contengono errori grammaticali, loghi sfocati o indirizzi email sospetti, anche se alcune sembrano estremamente convincenti. Per proteggerti, non cliccare mai su link sospetti e verifica sempre il mittente contattando direttamente l'ente.

SMISHING E VISHING: TRUFFE VIA SMS, WHATSAPP E TELEFONO

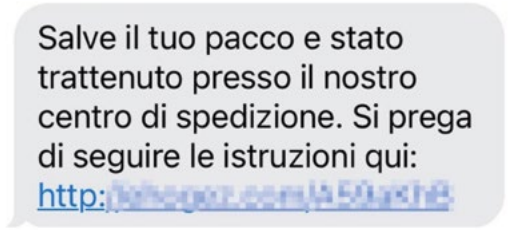
Il **smishing** è simile al phishing, ma utilizza messaggi SMS o via WhatsApp per attirarti nella trappola. Un esempio comune è un messaggio che ti informa di un "pacchetto in attesa" e ti chiede di cliccare su un link per sbloccarlo. Questo link potrebbe scaricare un malware sul tuo dispositivo o chiederti dati personali.

Il **vishing**, invece, avviene tramite telefonate. I truffatori si spacciano per operatori bancari o rappresentanti di aziende, creando storie convincenti per ottenere informazioni sensibili. Potrebbero dirti che il tuo conto è a rischio e convincerti a fornire il numero della tua carta o a fare un bonifico istantaneo.

Per difenderti:

- Non cliccare su link ricevuti via SMS.
- Non condividere mai dati personali o bancari al telefono.
- Se hai dubbi, chiama direttamente la banca o l'ente interessato usando i numeri ufficiali.

IL PACCO BLOCCATO



La truffa del pacco bloccato è un inganno molto diffuso che sfrutta l'aumento degli acquisti online e la dipendenza dalle consegne a domicilio. Immagina di ricevere un SMS o un'email che sembra arrivare da un corriere noto, come DHL, Poste Italiane o Bartolini. Nel messaggio, spesso formulato in modo convincente, ti viene comunicato che il tuo pacco è stato bloccato o che c'è un problema nella consegna. Il testo include un link con un invito a cliccarlo per risolvere la questione.

Una volta cliccato il link, vieni indirizzato a un sito web che sembra autentico ma è, in realtà, un sito fraudolento. Qui, ti viene chiesto di inserire informazioni personali, come indirizzo, numero di telefono o persino i dati della carta di credito, con la scusa di dover pagare una piccola tassa di sdoganamento o spese aggiuntive.

In realtà, il pacco non esiste e il sito è stato creato dai truffatori per rubare i tuoi dati personali o finanziari. Una volta ottenuti, i malintenzionati possono usarli per sottrarti denaro, clonare la tua carta di credito o compiere altre attività fraudolente.

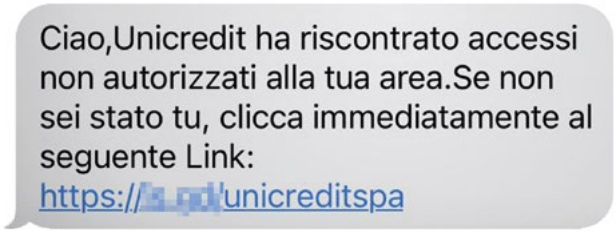
LA TRUFFA DEGLI INVESTIMENTI SU AMAZON

Le truffe legate ai falsi investimenti su Amazon sfruttano la notorietà e l'affidabilità del colosso dell'e-commerce per attirare ignari risparmiatori in schemi fraudolenti, promettendo guadagni facili e sicuri. I truffatori utilizzano annunci pubblicitari, email, social network e persino telefonate per convincerti a investire denaro in presunti

strumenti finanziari legati ad Amazon, che in realtà non esistono. Potresti ricevere un messaggio pubblicitario, una telefonata o un'e-mail che ti invita a partecipare a un programma esclusivo di investimenti su Amazon. Il messaggio afferma che Amazon offre ai piccoli investitori la possibilità di acquistare azioni o partecipare a un piano di guadagno passivo, con rendimenti garantiti e senza rischi.

Una volta che ti mostri interessato, vieni contattato da un presunto consulente finanziario, che ti chiede di versare una somma iniziale su una piattaforma di trading online. In molti casi, la piattaforma sembra autentica e mostra finti profitti per convincerti a investire ulteriori somme di denaro. Nel momento in cui cerchi di prelevare i tuoi presunti guadagni, scopri che il denaro è bloccato, che il sito non è più accessibile o che i truffatori sono spariti.

L'ACCESSO NON AUTORIZZATO AL CONTO



La truffa dell'accesso non autorizzato al conto è un inganno studiato per sottrarre i dati di accesso al tuo conto bancario e permettere ai truffatori di prendere il controllo delle tue finanze. Tramite un'email o un SMS che sembra provenire dalla tua banca ricevi un messaggio, molto spesso ben costruito con loghi ufficiali e un tono professionale che ti informa di un presunto problema urgente: ad esempio, un tentativo di accesso non autorizzato, una transazione sospetta o un blocco del conto.

Nel messaggio ti viene chiesto di agire subito per risolvere la questione, magari cliccando su un link per accedere al tuo conto o confermare i tuoi dati. Preso dalla fretta o dalla preoccupazione, clicchi sul link e ti ritrovi su un sito che sembra identico a quello della tua banca, ma in realtà è una copia creata dai truffatori. Qui ti chiedono di inserire username, password, o persino il codice OTP che ti è stato inviato via SMS.

Una volta che fornisci queste informazioni, i truffatori acquisiscono l'accesso diretto al tuo conto. Possono prelevare denaro, fare bonifici, o persino cambiare le tue credenziali per bloccarti fuori dal tuo account. A volte, la truffa include una telefonata da un falso operatore bancario che ti chiede ulteriori dettagli o ti convince a fornire codici di conferma.

La strategia dei truffatori si basa sul creare urgenza e spingerti ad agire senza riflettere troppo, facendo leva sulla paura di perdere i tuoi soldi o il controllo del conto.

IL PARENTE IN DIFFICOLTÀ

La truffa del parente in difficoltà è un raggiro subdolo che sfrutta i legami affettivi per ingannare le persone e ottenere denaro. Solitamente, i truffatori contattano la vittima tramite telefono, messaggio o email, fingendosi un parente, come un nipote o un cugino, in una situazione di emergenza. Raccontano di trovarsi in circostanze critiche, ad esempio un incidente stradale, un problema legale o un imprevisto all'estero, e chiedono aiuto economico immediato.

Il tono del messaggio è spesso drammatico e urgente, mirato a suscitare ansia e spingere la vittima ad agire senza pensarci troppo. I truffatori possono utilizzare dettagli personali ottenuti dai social media per rendere la storia più credibile. Per evitare ciò e proteggerti:

- Limita la visibilità dei tuoi post e delle tue informazioni personali sui social.
- Non accettare richieste di amicizia da sconosciuti.
- Segnala immediatamente profili sospetti alle piattaforme social.

Queste piccole azioni sono importanti in quanto i malviventi potrebbero menzionare il nome di un vero familiare o riferirsi a situazioni che sembrano plausibili. In alcuni casi, si spacciano per avvocati, medici o poliziotti, dicendo di agire per conto del presunto parente. La richiesta di denaro avviene solitamente attraverso bonifici, piattaforme di pagamento rapido o gift card, con l'obiettivo di rendere difficile il recupero delle somme inviate. La pressione emotiva gioca un ruolo centrale nella truffa, inducendo la vittima a reagire d'impulso.
Per difendersi, è fondamentale mantenere la calma e verificare sempre l'identità della persona che chiede aiuto. Chiamare direttamente il parente coinvolto, attraverso un numero di telefono conosciuto, è un passaggio importante per smascherare l'inganno. Anche evitare di fornire informazioni personali e diffidare di richieste insolite o troppo urgenti può aiutare a prevenire il rischio. Se si sospetta di essere vittime di questa truffa, è utile contattare immediatamente la banca o il servizio di pagamento utilizzato per cercare di bloccare il trasferimento, oltre a denunciare l'accaduto alle autorità competenti. Rimanere vigili e non cedere alla pressione emotiva sono i migliori strumenti per proteggersi da questo tipo di frode.

LA TRUFFA DI WHATSAPP

Una delle truffe più diffuse su WhatsApp è il furto dell'account tramite codice di verifica, un sistema che permette ai truffatori di prendere il controllo dell'app della vittima e usarla per ingannare amici e parenti. Questo raggiro sfrutta la procedura di verifica necessaria per accedere a WhatsApp su un nuovo dispositivo, facendo leva sulla fiducia tra contatti già presenti nella rubrica.
La truffa si sviluppa in più passaggi. Tutto inizia quando il malintenzionato tenta di registrare il tuo numero di telefono su un altro dispositivo. WhatsApp, per sicurezza, invia un codice di verifica a sei cifre via SMS al numero originale, ovvero il tuo. A questo punto, il truffatore, fingendosi un amico, un familiare o un servizio di assistenza, ti contatta su WhatsApp chiedendoti di inviargli quel codice.
Il messaggio potrebbe avere un tono rassicurante, come:
"Ciao, ho sbagliato a richiedere un codice di verifica per WhatsApp. Per favore, puoi mandarmelo? È urgente!"
Se la vittima condivide il codice, i truffatori lo utilizzano per completare la registrazione su un altro telefono, bloccando l'accesso all'account originale. Una volta ottenuto il controllo, possono usare il profilo WhatsApp per inviare messaggi ai contatti salvati, chiedendo denaro o informazioni sensibili.
Ad esempio, potrebbero scrivere a un tuo amico o parente:
"Ciao, ho un problema con il mio conto bancario e non posso fare pagamenti. Puoi prestarmi 500 euro? Ti rimborso domani."
Poiché il messaggio proviene da un numero conosciuto, molti cadono nella trappola e inviano il denaro senza sospettare nulla.

LE TRUFFE D'AMORE

Le truffe d'amore, note anche come "romance scam", sono inganni in cui i truffatori sfruttano i sentimenti delle vittime per manipolarle e ottenere denaro o informazioni personali. Questo tipo di truffa avviene spesso attraverso siti di incontri, social network o app di messaggistica, dove i truffatori creano falsi profili, utilizzando foto e informazioni che ispirano fiducia e attrattiva.

Il truffatore, dopo aver instaurato una connessione emotiva con la vittima, inizia a costruire un rapporto che sembra sincero e affettuoso. Possono parlare per settimane o mesi, scambiando messaggi quotidiani, facendo telefonate o persino videochiamate (spesso manipolate). L'obiettivo è guadagnare la fiducia della vittima e farla sentire coinvolta emotivamente.

Una volta stabilito il legame, il truffatore introduce una situazione problematica, come un'emergenza medica, una difficoltà economica o un problema con il visto per viaggiare. Racconta storie drammatiche, come essere bloccato in un paese straniero o dover pagare spese mediche per un parente malato. Chiede quindi denaro alla vittima, presentandolo come un aiuto temporaneo o come un gesto di amore.

La vittima, spinta dall'affetto e dalla fiducia, invia soldi, spesso tramite bonifici, ricariche prepagate o piattaforme come Western Union. Purtroppo, il truffatore sparisce una volta ricevuti i soldi, o continua a chiedere ulteriori somme inventando nuove scuse.

Per proteggersi da queste truffe, è importante diffidare di persone mai incontrate nella vita reale che chiedono denaro. Se qualcuno insiste nel chiedere soldi o racconta storie troppo drammatiche, è meglio interrompere il contatto. Ricordare che una vera relazione si basa sulla trasparenza e sulla fiducia reciproca è il modo migliore per evitare di cadere vittime di queste manipolazioni.

TRUFFE OFFLINE: IL PERICOLO DIETRO LA PORTA

FALSI TECNICI E RAPPRESENTANTI

Una delle truffe più comuni è quella dei falsi tecnici. Il truffatore si presenta come dipendente di un'azienda di servizi, come gas, luce o acqua, e chiede di entrare in casa per controlli tecnici. Una volta dentro, tenta di distrarti per rubare denaro o oggetti di valore.

Un'altra variante è il falso rappresentante di istituzioni pubbliche, come l'INPS o l'ASL. Queste persone possono chiedere denaro per "pagamenti arretrati" o fingere di dover verificare documenti ufficiali.

Per difenderti:

1. Non aprire mai la porta a sconosciuti senza verificare la loro identità. Chiedi un documento e controlla se ci sono veicoli ufficiali parcheggiati.
2. Non fornire mai denaro o documenti a chi si presenta senza preavviso.
3. In caso di dubbio, chiama l'ente o la società che dicono di rappresentare.

RAGGIRI PER STRADA

In strada, i truffatori possono avvicinarti fingendosi rappresentanti delle Forze dell'Ordine, venditori o membri di organizzazioni benefiche. Un esempio classico è il falso poliziotto che ti ferma, dicendo di voler controllare i tuoi documenti o gioielli.

Per proteggerti:

- Non fornire mai denaro o gioielli a sconosciuti.
- Se qualcuno si presenta come rappresentante delle Forze dell'Ordine, verifica attentamente la loro identità.

LA TRUFFA DELLO SPECCHIETTO

La truffa dello specchietto è un inganno estremamente diffuso sulle strade, spesso ai danni di automobilisti anziani o meno esperti. Il truffatore simula un incidente stradale, accusando la vittima di aver danneggiato il suo specchietto retrovisore e chiedendo un risarcimento immediato in denaro per evitare il coinvolgimento dell'assicurazione. Questa truffa sfrutta lo shock e il senso di colpa della persona coinvolta per spingerla a pagare senza verificare la reale dinamica dell'accaduto.

COME REAGIRE: STRATEGIE PRATICHE

Se sospetti di essere vittima di una truffa, segui questi passi:

1. **Interrompi immediatamente il contatto**: non continuare la conversazione e non cliccare su link sospetti.
2. **Verifica la situazione**: contatta direttamente l'ente, l'azienda o il familiare citato dal truffatore.
3. **Segnala l'accaduto**: chiama il 112 o recati presso la stazione dei carabinieri o di polizia più vicina per denunciare il tentativo di truffa.

Se hai già fornito denaro o informazioni sensibili:

- Contatta immediatamente la tua banca per bloccare il conto o la carta coinvolta.
- Informati su come proteggere i tuoi dati personali da un possibile uso fraudolento.

È fondamentale comprendere che essere vittima di una truffa non è motivo di vergogna, ma una situazione che può capitare a chiunque; denunciare prontamente l'accaduto alle autorità competenti è un passo cruciale per tutelare sé stessi, prevenire ulteriori danni e contribuire a proteggere altre persone da situazioni simili.

L'IMPORTANZA DELLA PREVENZIONE

La prevenzione è la miglior difesa contro le truffe. Condividi queste informazioni con amici e parenti, soprattutto con chi potrebbe essere più vulnerabile. Ricorda che i truffatori sfruttano spesso la fiducia e la mancanza di conoscenze tecnologiche, ma una buona informazione può fare la differenza.

Le Forze dell'Ordine lavorano quotidianamente per contrastare questi fenomeni, ma la tua collaborazione è fondamentale. Imparando a riconoscere i segnali di una truffa e agendo prontamente, puoi proteggere te stesso e chi ti è caro.

CONSIGLI PER INTERAGIRE CON I RAGAZZI/NIPOTI PER LA SICUREZZA ONLINE

COMPRENDERE IL LORO MONDO DIGITALE

Viviamo in un'epoca in cui il mondo digitale è parte integrante della vita quotidiana, specialmente per i ragazzi. Comprendere il loro universo online è il primo passo per instaurare un dialogo efficace sulla sicurezza. I giovani utilizzano smartphone, tablet e computer non solo per comunicare, ma anche per divertirsi, imparare e costruire relazioni. È importante che non si sentano giudicati o controllati, ma piuttosto supportati nel navigare in sicurezza.

I social media sono una parte centrale del loro mondo digitale. Per molti ragazzi, piattaforme come **Instagram**, **TikTok** e **WhatsApp** rappresentano luoghi dove esprimere sé stessi, interagire con amici e scoprire nuove tendenze. Allo stesso modo, app come **Discord**, **Twitch** e piattaforme di gaming online sono spazi virtuali dove condividono esperienze e passioni.

Instagram è usato per condividere foto e brevi video, seguire influencer e scoprire contenuti di tendenza. **TikTok**, invece, è il regno dei video brevi, creativi e spesso virali. Su **Discord** e **Twitch**, i ragazzi si riuniscono per chattare, giocare insieme o seguire streamer che condividono contenuti in diretta.

Comprendere come funzionano queste piattaforme è essenziale per affrontare eventuali rischi, come **il cyberbullismo, la condivisione di contenuti inappropriati o il contatto con sconosciuti**. Molte di queste app hanno impostazioni di privacy personalizzabili, che possono essere utilizzate per **proteggere i giovani da contenuti indesiderati o da interazioni potenzialmente pericolose**.

Coinvolgere i ragazzi nel processo di configurazione delle impostazioni di sicurezza sulle app può trasformarsi in un'esperienza educativa e condivisa. Potreste **controllare insieme chi può vedere i loro post, commentare o inviare messaggi**. Questo momento non deve essere percepito come controllo, ma come una collaborazione per assicurarsi che l'**esperienza digitale sia sicura e piacevole**.

Incoraggiare i giovani a parlare apertamente di eventuali situazioni spiacevoli o dubbi incontrati online è essenziale. Sentirsi ascoltati e compresi li aiuterà a rivolgersi a te in caso di problemi, sapendo che riceveranno supporto anziché giudizi. Il vero obiettivo non è vietare o limitare il loro accesso al mondo digitale, ma **equipaggiarli con gli strumenti e le conoscenze per muoversi in modo consapevole e sicuro**.

METTITI IN GIOCO!

PUZZLE DI PAROLE

Le parole sono nascoste orizzontali,verticali e diagonali

N	K	D	F	A	B	L	T	U	O	M	V	B	I
A	G	E	F	T	P	N	C	R	K	N	L	A	N
V	P	U	T	H	Q	P	K	V	O	M	D	C	F
I	R	L	P	A	G	O	P	A	D	L	B	K	O
G	I	P	A	W	E	B	C	A	M	I	L	U	R
A	V	N	F	Q	C	L	L	L	G	N	S	P	M
R	A	I	Y	M	G	C	P	G	O	S	T	F	A
E	C	C	P	R	N	L	U	O	K	T	R	A	T
L	Y	H	C	X	D	O	M	R	Z	A	E	C	I
F	J	M	H	O	P	U	V	I	H	G	A	E	C
A	A	Y	Q	C	U	D	U	T	Q	R	M	B	A
C	Q	H	R	W	M	N	Z	M	P	A	I	O	G
C	U	C	Q	F	U	R	T	O	C	M	N	O	Q
Z	B	I	O	M	E	T	R	I	C	O	G	K	K

ACCOUNT
APP
BIOMETRICO
FACEBOOK
INFORMATICA
NAVIGARE
PRIVACY
TROLL
ALGORITMO
BACKUP
CLOUD
FURTO
INSTAGRAM
PAGOPA
STREAMING
WEBCAM

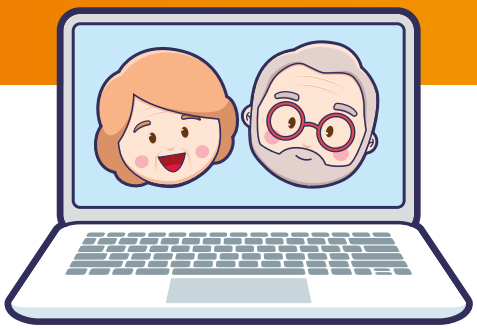
IL CRUCIVERBA

Verticali:

1. Motore di ricerca più famoso
2. Notizie false online
4. Social network famoso tra i più giovani
5. Metodo di comunicazione digitale
7. Truffa via email per rubare dati
11. Chiave segreta per accedere agli account

Orizzontali:

3. Esperto di informatica, a volte un criminale digitale
6. Rete globale di informazioni e connessioni
8. Valuta digitale, basata sulla tecnologia della blockchain
9. Truffa via SMS
10. App di messaggistica
12. Telefono con funzioni avanzate
13. Social network famoso
14. Identità digitale per i servizi online



NONNITEC

nonni nel digitale

Ministero del lavoro e delle politiche sociali
Direzione Generale del terzo settore e della responsabilità sociale delle imprese

REGIONE ABRUZZO
Dipartimento Lavoro - Sociale
Servizio Programmazione Sociale - DPG022
Ufficio Terzo Settore

COMUNE DI
MOSCIANO SANT'ANGELO

Associazione Pro Loco Montone APS

Finanziato nell'ambito dell'avviso pubblico per il finanziamento di iniziative e progetti di rilevanza regionale promossi da organizzazioni di volontariato, associazioni di promozione sociale e fondazioni del Terzo Settore per la realizzazione di attività di interesse generale di cui all'art. 5 del codice del Terzo Settore e d.m. 141/2022 - Risorse ADP 2022 - 2024 - Regione Abruzzo - CUP: C29I24000240008

in partenariato con:

"Uniti per la vita"

Volontari Protezione Civile Gran Sasso d'Italia

WWW.NONNITEC.IT