



ADICU aps

Associazione a Difesa dei Consumatori
e degli Utenti aps

LA TUA GUIDA PRATICA ALLA SICUREZZA ONLINE

PROTEGGI TE STESSO E I TUOI DISPOSITIVI

INIZIATIVE A VANTAGGIO DEI CONSUMATORI, ART. 4, CO. 1 DEL
DECRETO MINISTERIALE 6 MAGGIO 2022; ART. 4, COMMA 1, DEL
DECRETO MINISTERIALE DEL 31 LUGLIO 2024; DECRETO
DIRETTORIALE 29 NOVEMBRE 2024

DIGITALMENTIS

Iniziativa Competenze Digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024



Visita il nostro sito internet

www.adicu.it

INTRODUZIONE

BENVENUTO NEL MONDO DIGITALE

Benvenuto in questo manuale pratico, pensato per chiunque voglia navigare in Internet con maggiore sicurezza e consapevolezza. Non è necessario essere esperti di tecnologia: questa guida ti fornirà le conoscenze fondamentali per proteggere te stesso e i tuoi dispositivi nel vasto mondo digitale.

Pensa alla tua presenza online come a un "AVATAR": una rappresentazione digitale di te stesso. Proprio come nella vita di tutti i giorni proteggiamo la nostra persona, i nostri beni e la nostra privacy, è fondamentale imparare a proteggere il nostro AVATAR. Questo manuale ti insegnerà come farlo, passo dopo passo.

LE BASI: CHI È IL TUO "AVATAR" E DOVE VIVE?

Cos'è Internet?

Internet è una gigantesca rete che connette computer, smartphone e persone da ogni angolo del pianeta, superando i confini tradizionali. È una comunità globale che, se usata correttamente, ha un potenziale enorme.

Cosa dovrebbe essere Internet:

- Un modo per connettere gli esseri umani e arricchire le opportunità della vita.
- Uno strumento per allargare le nostre conoscenze e le nostre vedute.
- Un sistema di comunicazione mondiale per l'intera popolazione terrestre.
- Un mezzo per visitare luoghi lontani senza muoversi da casa.
- Uno strumento per abbattere le frontiere e avvicinare popoli e culture.



Un potente motore per creare e offrire nuovi servizi.

Allo stesso tempo, è fondamentale che Internet non diventi un inganno o una semplice alternativa alla vita reale, ma che resti uno strumento integrato positivamente nel nostro quotidiano.

L'AVATAR: La Tua Identità nel Mondo Virtuale

Il tuo AVATAR è la tua identità digitale. Oggi, la vita reale e quella virtuale non sono più separate, ma si fondono in un'unica esperienza. Le nostre azioni online hanno conseguenze concrete e viceversa. Il concetto chiave da comprendere è questo:

Siamo costretti a usare mediatori differenti: il corpo nella vita reale e l'AVATAR nella realtà virtuale, che è la rappresentazione digitale della persona reale.

Lasciare il nostro AVATAR indifeso significa esporre la nostra persona a rischi reali, come truffe, furti d'identità e violazioni della privacy.

Prima di avventurarci nel mondo digitale, è essenziale assicurarsi che i "luoghi" da cui il nostro AVATAR si connette siano sicuri. Questi luoghi sono i nostri dispositivi: computer, smartphone e tablet.

LA PRIMA DIFESA: PROTEGGERE I TUOI DISPOSITIVI

Il Computer: La Tua Casa Digitale

Un computer connesso a Internet ma non protetto è come una casa con porte e finestre spalancate. Chiunque può entrare e rubare informazioni preziose. Per mettere in sicurezza la tua "*casa digitale*", segui queste 5 azioni fondamentali:

1. **Attivare i sistemi di sicurezza:** È il primo passo, fondamentale per creare una barriera di base. La maggior parte dei sistemi operativi include già strumenti di protezione che vanno semplicemente attivati.
2. **Usare un Firewall:** Agisce come un "*buttafuori*" digitale, filtrando le comunicazioni in entrata e in uscita dal tuo PC e bloccando i tentativi di accesso non autorizzati.

3. **Installare e aggiornare un Antivirus:** Un buon antivirus rileva e rimuove software dannosi (virus, spyware). È cruciale mantenerlo costantemente aggiornato per riconoscere le minacce più recenti.
4. **Fare attenzione ai siti web:** Se il tuo PC o il tuo browser ti avvisano che un sito non è attendibile, fidati. È meglio uscire subito dalla pagina per non correre rischi.
5. **Connettersi con un Router:** Un router di buona qualità agisce come uno scudo. Gli attacchi informatici vengono spesso diretti al router invece che al singolo PC, offrendoti così una protezione indiretta.

Smartphone e Tablet: La Sicurezza in Tasca

Anche i dispositivi che portiamo sempre con noi contengono un'enorme quantità di dati personali e richiedono la massima attenzione. Ecco i rischi principali e come difendersi.

Rischio Principale	Come Proteggersi
Furto o smarrimento	Imposta sempre un codice PIN , una password o un sistema di sblocco biometrico (impronta/volto). Annota e conserva in un luogo sicuro il codice IMEI del dispositivo: è indispensabile per richiederne il blocco all'operatore telefonico e alle Forze dell'Ordine.
Abbonamenti non richiesti	Prevenzione: Fai attenzione ai banner ingannevoli che compaiono durante l'uso di app o la navigazione. Installa applicazioni solo da fonti attendibili e mantienile sempre aggiornate. Azione Correttiva: Se attivi involontariamente un servizio a pagamento, segui questi passaggi: 1. Contatta subito il tuo operatore per disattivare il servizio. 2. Chiedi il rimborso. 3. Se necessario, rivolgiti a un'associazione di consumatori.



Un Consiglio Fondamentale: Gestire i Dati Sensibili

Il consiglio più importante riguarda la gestione dei tuoi dati più preziosi.

Il modo migliore per proteggere l'identità è eliminare all'origine tutti i dati sensibili. La tecnologia offre soluzioni come il cloud, dove si possono salvare i propri file in memorie non residenti nell'apparato (protette da login e password)...

Servizi come **Google Drive** o **Dropbox** ti permettono di archiviare documenti, foto e file importanti in uno spazio online sicuro, accessibile da qualsiasi dispositivo, senza doverli conservare sulla memoria fisica del tuo PC o smartphone, dove sarebbero più vulnerabili in caso di furto o attacco informatico.

Una volta messi in sicurezza i nostri dispositivi, è il momento di concentrarci su uno degli strumenti di comunicazione più utilizzati e, purtroppo, più vulnerabili: la posta elettronica.

OCCHIO ALLA POSTA: RICONOSCERE E GESTIRE LE EMAIL PERICOLOSE

Proteggere il Tuo Account Email

La posta elettronica è uno dei veicoli principali per la diffusione di virus e per la realizzazione di truffe online. Segui queste tre regole d'oro per proteggere il tuo account:

- **Usa una password complessa** (con lettere, numeri e simboli) e ricordati di cambiarla spesso.
- **Non aprire mai allegati o link** provenienti da mittenti che non conosci o da indirizzi email sospetti.
- **Utilizza filtri antispam** e controlla periodicamente la cartella della posta indesiderata per recuperare eventuali messaggi legittimi finiti lì per errore.

Il Phishing: La Truffa più Diffusa

Il **phishing** è una tecnica fraudolenta usata dai criminali informatici per "pescare" (dall'inglese **fishing**) i tuoi dati sensibili, come password, numeri di carte di credito o credenziali di accesso alla banca. Di solito avviene tramite email che sembrano provenire da fonti attendibili.

Ecco le 4 caratteristiche tipiche di un'email di phishing:

- **Richiesta di credenziali:** Ti spingono a cliccare su un link che porta a un sito web falso, identico a quello originale (della tua banca, delle poste, ecc.), dove ti viene chiesto di inserire i tuoi dati.
- **Tono intimidatorio:** Usano un linguaggio che genera ansia o urgenza ("*Il tuo conto sta per essere bloccato!*", "*Verifica subito i tuoi dati per non perdere l'accesso*").
- **Mancanza di personalizzazione:** Spesso iniziano con saluti generici come "*Gentile Cliente*" invece di usare il tuo nome e cognome.
- **Errori di ortografia:** Contengono quasi sempre errori grammaticali, di battitura o di traduzione, un segnale di scarsa professionalità.

Come Difendersi dal Phishing: Riepilogo

Se ricevi un'email sospetta, segui questa semplice lista di controllo.

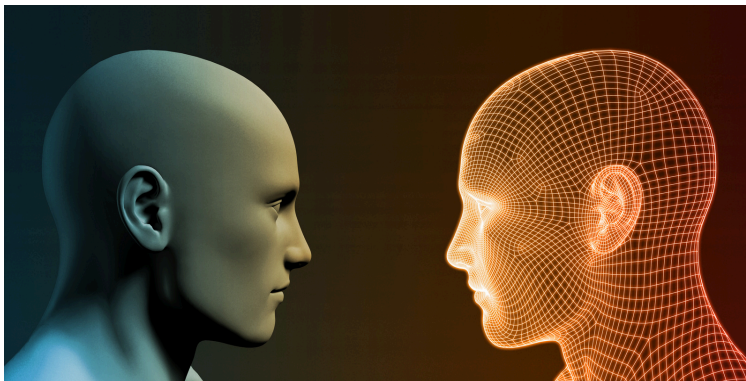
Cosa NON fare:

- [] NON rispondere mai a email che chiedono dati personali, password o numeri di carte di credito.
- [] NON cliccare sui link contenuti nel messaggio.
- [] NON fornire mai i tuoi dati su pagine web raggiunte tramite link sospetti.

Cosa FARE:

- [] In caso di dubbio, contatta direttamente la tua banca o l'istituto interessato tramite i loro canali ufficiali (sito web o numero di telefono).
- [] Se sei caduto nella trappola, informa subito la banca per bloccare le operazioni e segnala l'accaduto alla Polizia di Stato.

Oltre alla posta elettronica, i rischi si estendono a tutta la nostra attività online. Vediamo ora come navigare sul web e sui social network in modo più consapevole e sicuro.



NAVIGARE CON PRUDENZA: SOCIAL NETWORK E WEB SICURO

Scegliere e Aggiornare il Browser

Il browser (come Chrome, Firefox, Safari) è il programma che usi per navigare su Internet. È la tua "automobile" per esplorare il web. Per viaggiare in sicurezza, è fondamentale che sia sempre aggiornato:

- **Usa sempre l'ultima versione disponibile.**
- **Attiva gli aggiornamenti automatici.**

Gli aggiornamenti non solo introducono nuove funzioni, ma correggono anche le vulnerabilità di sicurezza che i criminali potrebbero sfruttare per attaccare il tuo dispositivo.

I Social Network: Condividere con Intelligenza

Sui social network, il rischio principale spesso non viene da attacchi esterni, ma dalla condivisione volontaria di troppe informazioni personali. Ricorda che ogni dato che pubblichi può essere visto, copiato e usato da altri.

Ecco 5 regole fondamentali per usare i social network in modo sicuro:

1. **Controlla le Impostazioni sulla Privacy:** Prenditi del tempo per esplorare le impostazioni del tuo profilo. Limita la visibilità dei tuoi post e delle tue informazioni personali solo a una cerchia ristretta di amici di cui ti fidi.
2. **Seleziona gli Amici con Cura:** Non accettare richieste di amicizia da persone che non conosci nella vita reale. Un profilo può essere falso e nascondere cattive intenzioni.
3. **Pensa Prima di Pubblicare:** Prima di condividere una foto, un video o un pensiero, chiediti: "Mi sentirei a mio agio se questa informazione diventasse pubblica?". Ricorda che tutto ciò che metti online può essere salvato e redistribuito da altri, anche se in futuro dovessi cancellarlo.
4. **Usa una Password Sicura:** Proteggi il tuo account con una password robusta e cambiala periodicamente. Non usare mai la stessa password per più servizi.
5. **Controlla cosa Pubblicano gli Altri su di Te:** Presta attenzione a foto o post in cui vieni taggato. Se un contenuto ti mette a disagio o viola la tua privacy, chiedi immediatamente a chi l'ha pubblicato di rimuoverlo.

Ora che abbiamo visto le regole generali per la navigazione, concentriamoci su due ambienti online specifici che richiedono accorgimenti particolari: le chat e i negozi virtuali.

AMBIENTI SPECIFICI: REGOLE D'ORO PER CHAT E SHOPPING ONLINE

Le Chat Line: Un Territorio Insidioso

Le chat line (da non confondere con le app di messaggistica come WhatsApp) sono ambienti online dove l'anonimato è la regola. Questo le rende un territorio particolarmente rischioso, popolato da "**FINTI AVATAR**", ovvero persone che si nascondono dietro false identità.

Per proteggerti, segui questi 3 consigli fondamentali:

- **NON diffondere mai informazioni personali**, dati sensibili, fotografie o video.
- **NON fidarti mai dell'identità degli altri utenti**. È impossibile sapere con certezza chi si nasconde dietro uno schermo.
- **NON organizzare mai incontri reali** con persone conosciute in chat senza aver preso le massime precauzioni (informare qualcuno, scegliere un luogo pubblico, farsi accompagnare).

È fondamentale sottolineare che questi ambienti sono particolarmente pericolosi per i minori. La chat è un luogo in cui i "giovani AVATAR" non dovrebbero mai trovarsi, a causa dell'alto rischio di incontrare malintenzionati con scopi illeciti.

Shopping Online (E-commerce): Acquistare in Sicurezza

Fare acquisti online è comodo e veloce, ma è importante saper riconoscere i siti affidabili per evitare truffe. Prima di inserire i tuoi dati di pagamento, usa questa checklist:

- [] **Verifica la connessione sicura**: Controlla che l'indirizzo del sito inizi con https e che nella barra degli indirizzi sia presente il simbolo del lucchetto. Questo garantisce che i tuoi dati vengano trasmessi in modo crittografato.
- [] **Evita computer condivisi**: Non inserire mai i dati della tua carta di credito se stai usando un computer pubblico (es. in un internet café o in una biblioteca).

- [] **Leggi le condizioni di contratto:** Assicurati che il sito specifichi chiaramente le politiche di vendita, come il diritto di recesso (la possibilità di restituire il prodotto entro 14 giorni).
- [] **Controlla i dati dell'azienda:** Un venditore serio indica sempre i propri dati, come la sede legale e la partita IVA.
- [] **Diffida da prezzi troppo bassi:** Offerte che sembrano troppo belle per essere vere sono spesso il segnale di una truffa.

Infine, è fondamentale dedicare un'attenzione speciale alla protezione degli utenti più vulnerabili del mondo digitale: i giovani e i minori.

UN OCCHIO DI RIGUARDO: PROTEGGERE I "GIOVANI AVATAR"

Cos'è il Cyberbullismo

Il cyberbullismo è l'uso delle tecnologie digitali (smartphone, social network, chat) per intimidire, molestare, mettere in imbarazzo o escludere deliberatamente altre persone. A differenza del bullismo tradizionale, può avvenire 24 ore su 24 e raggiungere un pubblico vastissimo in pochi istanti.

Alcuni esempi di cyberbullismo includono:

- Invio di messaggi o email minacciosi.
- Pubblicazione di foto o video imbarazzanti senza il consenso della persona interessata.
- Diffusione di pettegolezzi e calunnie online.
- Creazione di profili falsi per danneggiare la reputazione di qualcuno (furto d'identità).

Consigli per i Genitori

Proteggere i minori online richiede un mix di accorgimenti tecnologici e, soprattutto, un forte ruolo educativo.

Accorgimenti Tecnologici	Ruolo Educativo e Regole Semplici
<p>Usa le impostazioni del browser e del router di casa per bloccare l'accesso a siti web con contenuti inappropriati. Inserendo un sito nella lista nera del router, questo sarà inaccessibile da tutti i dispositivi connessi alla rete domestica (PC, tablet, smartphone).</p>	<p>Insegna ai tuoi figli queste regole fondamentali per navigare in sicurezza: <ul style="list-style-type: none"> Non fornire mai dati personali (nome, indirizzo, numero di telefono) a sconosciuti online. Non inviare mai fotografie o video a persone conosciute solo su Internet. Non fissare mai incontri con persone conosciute online. Segnalare subito a un genitore o un insegnante ogni sito, messaggio o richiesta che li fa sentire a disagio o spaventati. </p>

Se Sei Vittima di Molestie

Se sei un ragazzo o una ragazza e stai subendo molestie online, la cosa più importante da sapere è che non sei solo e non è colpa tua. Non nasconderti e non soffrire in silenzio. La prima cosa da fare è **parlarne subito con un adulto di cui ti fidi**: i tuoi genitori, un insegnante o un altro parente. Segnalare questi episodi è l'unico modo per fermarli.

Per segnalazioni ufficiali, è possibile contattare la Polizia delle Comunicazioni scrivendo a polizia.comunicazioni@interno.it o visitando il sito www.commissariatodips.it.

RIEPILOGO FINALE LE 8 REGOLE D'ORO DA NON DIMENTICARE

Per concludere, abbiamo raccolto le regole più importanti da tenere sempre a mente. Se dovessi ricordare solo otto cose da questa guida, fai in modo che siano queste:

1. **Mantieni il PC ben protetto:** Usa sempre un firewall, un antivirus aggiornato e attiva gli aggiornamenti automatici per il sistema operativo e i browser.
2. **Custodisci le tue informazioni personali:** Prima di inserire dati, controlla la presenza di https e del lucchetto. Usa password lunghe, complesse e diverse per ogni sito.
3. **Pensa prima di cliccare!:** Non aprire allegati o link sospetti, anche se sembrano provenire da persone che conosci. In caso di dubbio, verifica in altro modo.
4. **Non fornire informazioni via e-mail:** Nessuna banca o istituzione seria ti chiederà mai dati personali o password tramite email.
5. **Attenzione ai falsi!:** Diffida di messaggi allarmistici, offerte imperdibili o richieste di aiuto. Spesso sono trappole.
6. **Sui social network con prudenza:** Controlla attentamente le impostazioni sulla privacy e limita la visibilità delle tue informazioni personali.
7. **Pensa bene a quello che pubblichi su Internet:** Ricorda che tutto ciò che metti online può rimanere per sempre e essere visto da chiunque. Non pubblicare nulla di cui potresti pentirti.

Rispetta la netiquette Comportati online con la stessa educazione e rispetto che useresti nella vita reale.

GLOSSARIO

LE PAROLE DELLA SICUREZZA

- **AVATAR:** La rappresentazione digitale di una persona reale nel mondo virtuale di Internet.
- **Browser:** Il programma utilizzato per navigare su Internet (es. Google Chrome, Mozilla Firefox, Apple Safari).
- **Malware:** Un termine generico che indica qualsiasi software creato con lo scopo di causare danni a un computer (include virus, spyware, ecc.).
- **Phishing:** Una truffa online che mira a rubare dati sensibili (come password o numeri di carte di credito) inducendo la vittima a inserirli su un sito web falso.
- **Router:** Un dispositivo che instrada i dati tra le reti. In casa, distribuisce la connessione Internet ai vari dispositivi e agisce come una prima linea di difesa.
- **Spyware:** Un tipo di malware che si installa di nascosto su un dispositivo per raccogliere informazioni sulle abitudini dell'utente e trasmetterle a terzi.
- **Virus:** Un programma dannoso che si diffonde da un computer all'altro, spesso tramite allegati email o download, per danneggiare file e sistemi.



DIGITALMENTIS



Progetto “Digitalmentis 2” è rivolto alle Regioni per lo sviluppo delle competenze digitali dei consumatori adulti e vulnerabili di cui all’Avviso pubblico del Ministero delle Imprese e del Made in Italy (MIMIT), ai sensi dell’art. 148, Legge 388/2000 - Iniziative a vantaggio dei consumatori, art. 4, co. 1 del decreto ministeriale 6 maggio 2022; art. 4, comma 1, del decreto ministeriale del 31 luglio 2024; decreto direttoriale 29 novembre 2024.

Con la nuova Agenda Digitale si apre una nuova stagione che proietta la Regione Lazio direttamente nel futuro.

Tra gli **obiettivi principali** dell’Agenda Digitale da raggiungere entro il **2026** troviamo: colmare il gap digitale, rendendo digitalmente abile almeno il 70% della popolazione; raddoppiare la popolazione in possesso di competenze digitali avanzate; incrementare del 50% la quota delle micro, piccole e medie imprese che utilizzano specialisti ICT; raggiungere almeno il 65% di popolazione che utilizza servizi pubblici digitali; elevare all’80% la percentuale di popolazione che utilizza Internet.



ADICU aps

Ente Terzo Settore

ADICU – Associazione per la difesa dei consumatori e degli utenti – nasce da una precedente realtà associativa, costituita sin dal 2009 e vanta un bagaglio di esperienza nel settore consumeristico.

Lo scopo di ADICU aps è di rappresentare, supportare, assistere e tutelare a 360° i consumatori e gli utenti.

Sin dall'epoca, l'attuale Adicu, attraverso una rete diversificata di iniziative, si è sempre contraddistinta perseguendo **obiettivi di solidarietà** e **promozione sociale**, attività di sostegno, **formazione** e **informazione** promuovendo campagne sia a livello nazionale che locale.

L'attività svolta dall'associazione riguarda i seguenti settori: assicurazioni, sicurezza stradale, risparmio energetico, trasporti, credito e risparmio, poste, telecomunicazioni e nuove tecnologie (tv digitale, banda larga, internet), contratti, vendite fuori e dentro i locali commerciali, turismo, commercio, alimentazione, fisco e tributi,

Adicu, altresì, si rivolge e pone al centro del proprio agire **il consumatore** ed opera, favorendo la **conciliazione** tra consumatori ed aziende e **le buone pratiche** quali strumenti di difesa, mettendo a disposizione il proprio bagaglio di conoscenze e figure professionali preparate nell'approntare una risposta rapida ed efficiente alle problematiche.

Oggi **Adicu** è Associazione autonoma con propri associati e con una composita organizzazione articolata in vari sportelli su tutto il territorio nazionale; è iscritta nel **Registro Nazionale delle APS** presso il Ministero del Lavoro e delle Politiche Sociali ed è un **Associazione riconosciuta** in base alla Legge, 7 dicembre 2000, n. 383.

Per informazioni e contatti

ADICU aps

Via Val Varaita 8 - Roma - Tel.: 06.88642693 - Cell.: 393.9130788
email: segreteria@adicu.it - pec.: adicu@pec.it - sito internet: www.adicu.it
Orari di ricevimento: Martedì e Mercoledì dalle ore 15.30 alle ore 19.30