Federconsumatori
MARCHE APS - ETS

LE PRECAUZIONI PER UN USO CORRETTO DEL DIGITALE

TURISMO

Attenzione alle truffe, link sospetti

Con l'avvicinarsi delle vacanze, aumentano anche i tentativi di truffa online legati al turismo. Molti utenti, alla ricerca di offerte vantaggiose su voli, hotel o pacchetti vacanza, rischiano di cadere vittime di siti fraudolenti o link sospetti inviati via email o messaggistica.

Come riconoscere i link sospetti:

- Controllare sempre l'indirizzo web (URL): diffidare di siti con nomi strani, errori ortografici o estensioni non comuni.
- Non cliccare su link ricevuti da mittenti sconosciuti o non verificabili.
- Verificare che il sito abbia un certificato di sicurezza (https://).

Consigli utili per evitare le truffe:

- Prenotare solo su piattaforme ufficiali o largamente conosciute.
- Leggere le recensioni e confrontare le offerte.
- Diffidare di offerte troppo vantaggiose o con richieste di pagamento non tracciabili.

La prudenza è fondamentale per evitare spiacevoli sorprese e godersi una vacanza in tutta tranquillità.

TELEMARKETING

Come proteggerti dalle chiamate moleste

Negli ultimi anni, il telemarketing è diventato una presenza sempre più frequente (e fastidiosa) nelle nostre vite. Chiamate a tutte le ore, numeri sconosciuti e offerte mai richieste: ma è possibile difendersi?

Ecco cosa puoi fare:

1. Iscriviti al Registro Pubblico delle Opposizioni (RPO)

È gratuito e ti permette di non ricevere più chiamate promozionali. Puoi registrare sia numeri fissi che cellulari.

2. Non fornire mai il tuo consenso con leggerezza

Spesso acconsentiamo all'uso dei dati personali senza accorgercene (es. online o nei concorsi). Leggi sempre bene prima di accettare.

3. Segnala gli abusi al Garante della Privacy

Se vieni contattato nonostante il rifiuto esplicito, puoi fare una segnalazione formale.

Curiosità:
Dal 2022, anche i cellulari possono essere registrati al RPO. Inoltre, i call center devono mostrare il numero da cui chiamano: se lo nascondono, sono fuori legge.

Hai ricevuto una chiamata sospetta?
Ti consigliamo di consultare il sito ufficiale del Garante della Privacy o segnalarla subito.

Registrati al Registro delle Opposizioni »
https://registrodelleopposizioni.it
Numero verde 800957766 (da fisso)
06 42986411(da mobile)
Email compilando il modulo scaricabile dal sito e inviandolo.

ACCESSO AI SERVIZI SANITARI NELLA REGIONE MARCHE

1. Fascicolo Sanitario Elettronico (FSE)

Il Fascicolo Sanitario Elettronico (FSE) è uno strumento digitale che raccoglie i tuoi documenti e dati sanitari, consentendoti di: Consultare referti, lettere di dimissione, prescrizioni e altri documenti clinici.
Prenotare visite ed esami.
Gestire il consenso alla condivisione dei dati.
Pagare le prestazioni sanitarie online.
Per accedere al FSE, è necessario autenticarsi tramite:

- SPID (Sistema Pubblico di Identità Digitale).
- Carta d'Identità Elettronica (CIE).
- Carta Nazionale dei Servizi (CNS).

Puoi accedere al FSE attraverso il portale ufficiale della Regione Marche: fse.sanita.marche.it.

2. App SaluteMarche

L'applicazione **SaluteMarche** ti permette di:

- Prenotare visite ed esami sanitari online.
- Pagare le prestazioni in modo semplice e veloce.

L'app è disponibile per smartphone e tablet. Maggiori informazioni sono disponibili sul sito ufficiale: Asur Marche.

Come accedere ai Servizi Sanitari della Regione Marche con SPID

Gentile cittadino,
da oggi accedere ai servizi sanitari digitali della Regione Marche è ancora più semplice e sicuro grazie all'utilizzo dello **SPID** (Sistema Pubblico di Identità Digitale).
SPID consente di identificarti in modo certo e sicuro per usufruire di diversi servizi online, comodamente da casa o tramite smartphone.

Ecco cosa puoi fare accedendo con SPID ai servizi sanitari regionali:

- Consultare il tuo **Fascicolo Sanitario Elettronico (FSE)**
- Scaricare **referti medici, esami di laboratorio e radiografie**
- Prenotare, modificare o cancellare **visite specialistiche e prestazioni ambulatoriali**
- Richiedere il **medico di base** o il **pediatra di libera scelta**

- Accedere al **servizio di esenzione ticket**
- Verificare lo stato delle **prenotazioni CUP**

Come accedere:

1. Vai al portale della Regione Marche: https://www.regione.marche.it

2. Clicca su “Servizi online” o vai direttamente su https://servizi.marche.it

3. Seleziona “Accedi con SPID”

4. Scegli il tuo provider SPID (es. PosteID, Aruba, TIM, etc.)

5. Inserisci le credenziali e accedi in totale sicurezza

Non hai ancora SPID?
Puoi ottenerlo gratuitamente
da uno dei provider accreditati.
Consulta la guida su https://www.spid.gov.it
oppure vieni nelle nostre sedi.

ACQUISTI SU FACEBOOK

Cosa sapere per evitare truffe

Facebook Marketplace e i gruppi di vendita sono ormai luoghi comuni per acquistare oggetti nuovi o usati. Ma attenzione: dietro offerte allettanti possono nascondersi truffe. Ecco alcuni consigli utili per acquistare in sicurezza

1. Controlla il profilo del venditore

Verifica che abbia foto reali, amici e attività recente. I profili falsi o creati da poco sono spesso usati per truffe.

2. Non inviare mai denaro in anticipo

Evita bonifici o ricariche PostePay. Preferisci pagamenti sicuri come PayPal (con la modalità “beni e servizi”) o lo scambio a mano.

3. Chiedi sempre foto reali e dettagliate del prodotto

Diffida da immagini troppo patinate o già viste su altri siti. Chiedi anche una breve descrizione.

4. Fissa l'incontro in un luogo pubblico e frequentato

Se possibile, scegli zone sorvegliate o ben illuminate, e informa qualcuno dell'appuntamento.

5. Segnala comportamenti sospetti a Facebook

Se hai dubbi su un utente o un annuncio, usa la funzione “Segnala” per proteggere te e gli altri utenti.

Consiglio extra:

Non condividere mai documenti, codice fiscale o coordinate bancarie tramite Messenger. Nessun venditore serio ne ha bisogno

Comprare su Facebook può essere comodo e conveniente, ma la prudenza è fondamentale.
Segui questi semplici consigli per evitare brutte sorprese.

Tutela del Consumatore nei Contratti a Distanza

COSA SAPERE

Con la crescente diffusione degli acquisti online e dei servizi digitali, i **contratti a distanza** sono diventati sempre più comuni. Tuttavia, è fondamentale conoscere i propri diritti e adottare alcune **precauzioni** per evitare truffe o situazioni svantaggiose

Cosa sono i contratti a distanza?

I contratti a distanza sono accordi stipulati tra professionista e consumatore **senza la presenza fisica simultanea** delle parti, attraverso internet, telefono o posta.

Precauzioni fondamentali:

1. **Informazioni chiare prima dell'acquisto**

   Il venditore deve fornire informazioni complete su prezzo, caratteristiche del prodotto/servizio, modalità di pagamento, diritto di recesso e contatti.

2. Diritto di recesso

Il consumatore ha generalmente **14 giorni di tempo** per recedere dal contratto senza penalità e senza dover fornire motivazioni.

3. Attenzione alle clausole nascoste

Leggi sempre le **condizioni generali di contratto**, in particolare le sezioni su rinnovi automatici, penali, o limitazioni di responsabilità.

4. Pagamenti sicuri

Utilizza solo **canali di pagamento tracciabili** e sicuri (es. carta di credito, PayPal). Evita bonifici a sconosciuti o anticipi sospetti.

5. Verifica l'identità del venditore

Controlla che siano presenti **dati identificativi** completi (P.IVA, indirizzo, contatti). I siti affidabili mostrano anche recensioni e politiche di assistenza chiare.

6. Documentazione

Conserva copie delle **email, conferme d'ordine e condizioni contrattuali**. Possono essere utili in caso di contestazioni.

La comodità dei contratti a distanza non deve farci abbassare la guardia. Una **corretta informazione** e una **dovuta attenzione** sono le migliori difese del consumatore.

Precauzioni nelle comunicazioni con la Pubblica Amministrazione

Con la crescente digitalizzazione dei rapporti con la Pubblica Amministrazione (PA), è fondamentale adottare comportamenti attenti e consapevoli per garantire la correttezza delle comunicazioni e la tutela dei propri diritti.

Ecco alcune precauzioni essenziali da osservare:

1. Utilizzo della PEC

La Posta Elettronica Certificata (PEC) è lo strumento privilegiato per le comunicazioni ufficiali. Assicuratevi che l'indirizzo PEC sia attivo, correttamente registrato e monitorato con regolarità.

2. Verifica dei destinatari

Prima dell'invio, controllare attentamente gli indirizzi di destinazione. L'invio a un indirizzo errato può comportare l'inefficacia della comunicazione.

3. Rispetto dei termini

I termini fissati dalla normativa o dalle amministrazioni (es. presentazione di istanze, risposte a comunicazioni) sono perentori. Rispettarli è essenziale per evitare decadenze o sanzioni.

4. Formati e allegati

Seguire le indicazioni tecniche fornite dalle PA, soprattutto riguardo ai formati dei documenti (PDF, XML, ecc.) e alle dimensioni massime degli allegati.

5. Conservazione delle comunicazioni

Archiviare in modo ordinato tutte le comunicazioni inviate e ricevute, incluse le ricevute di accettazione e consegna delle PEC.

6. Controlli di autenticità

In caso di dubbi su una comunicazione ricevuta, è opportuno verificarne la provenienza tramite i

canali ufficiali (siti istituzionali, elenchi pubblici PEC, ecc.).

7. Assistenza professionale

In caso di comunicazioni complesse o procedimenti delicati, è consigliabile rivolgersi a un consulente o legale di fiducia.

La correttezza nella forma e nei contenuti delle comunicazioni con la PA è un elemento cruciale per il buon esito di qualsiasi procedura. Adottare precauzioni concrete riduce il rischio di errori, omissioni o contenziosi.

Per ulteriori informazioni o per ricevere assistenza specifica, le nostre sedi sono a disposizione.

Operazioni bancarie on line

Nel mondo sempre più digitale, effettuare operazioni bancarie online è diventato comodo e veloce. Tuttavia, è importante adottare alcune precauzioni per proteggere i propri dati e risparmi.

Ecco alcuni consigli utili:

1. Usa solo app e siti ufficiali

Effettua operazioni bancarie esclusivamente tramite l'app ufficiale della tua banca o il suo sito web (verifica che l'indirizzo inizi con "https").

2. Attiva l'autenticazione a due fattori (2FA)

Questa misura di sicurezza aggiuntiva rende più difficile l'accesso da parte di malintenzionati.

3. Non condividere mai le tue credenziali

Nessuna banca ti chiederà mai PIN o password via email, SMS o telefono. Diffida da qualsiasi richiesta in tal senso.

4. Attenzione alle reti Wi-Fi pubbliche

Evita di accedere al tuo conto da reti Wi-Fi pubbliche o non protette. Usa una connessione sicura o una VPN.

5. Aggiorna regolarmente i tuoi dispositivi

Mantieni aggiornato il sistema operativo e le app per beneficiare delle ultime patch di sicurezza.

6. Controlla regolarmente i movimenti

Segnala subito alla tua banca eventuali movimenti sospetti o non autorizzati.

7. Usa password forti e uniche

Evita password ovvie o riutilizzate. Valuta l'uso di un gestore di password affidabile.

La tua sicurezza è la nostra priorità. Seguendo questi semplici accorgimenti, puoi effettuare le tue operazioni digitali con maggiore serenità.

Federconsumatori
MARCHE APS - ETS

Via I Maggio, 142/c - Ancona Tel. 071.2866977
E-mail: **regione@federconsumatorimarche.it**
Presidente: **Giancarlo Collina**

ANCONA – *Sede Provinciale*
Via I Maggio, 142/c Ancona – Tel. **071.2866977**
E-mail: **s.cesaro@federconsumatorimarche.it**
Presidente: *Serena Cesaro*

ASCOLI PICENO – *Sede Provinciale*
Via C. Rozzi, 13/F Ascoli Piceno – Tel. **0736.343957**
E-mail: **ascolipiceno@federconsumatorimarche.it**
Presidente: *Nicolò Norcini Pala*

FERMO – *Sede Provinciale*
Via dell'Annunziata, 1 Fermo – Tel. **0734.220808**
E-mail: **fermo@federconsumatorimarche.it**
Presidente: *Romina Iullitti*

MACERATA – *Sede Provinciale*
Via G. di Vittorio, 2/4 Macerata – Tel. **0733.245711**
E-mail: **macerata@federconsumatorimarche.it**
Presidente: *Lorenzo Longo*

PESARO – *Sede Provinciale*
Via Gagarin, 179 Pesaro – Tel. **0721.67941**
E-mail: **pesaro.federconsumatori@marche.it**
Presidente: *Alessandro Pertoldi*

Finanziato nell'ambito del programma della Regione Marche con fondi MIMIT - DM 31/07/2024 e DD 14/02/2025.