

PagoPA e Pagamenti Digitali

Praticità, sicurezza e trasparenza per tutti

Cosa sono i Pagamenti Digitali

I pagamenti digitali sono transazioni di denaro elettronico che sostituiscono contanti e assegni, utilizzando metodi come carte di credito e debito, bonifici, app di pagamento (come PayPal), portafogli mobili (Apple Pay, Google Pay) e pagamenti contactless

Quali vantaggi nell'utilizzo

Velocità e comodità: permettono di effettuare transazioni in qualsiasi momento e luogo;

Sicurezza: Utilizzo di tecnologie avanzate per proteggere le transazioni

Tracciabilità: ogni operazione lascia una traccia digitale

Sicurezza nei pagamenti digitali

- SCA (Strong Customer Authentication): autenticazione forte prevista da PSD2.
- Connessioni HTTPS (sicure).
- App e siti ufficiali.
- Password robuste e uniche.

Principali riferimenti normativi

- Direttiva (UE) 2015/2366 – PSD2 (Payment Services Directive 2): regola i servizi di pagamento elettronico.
- D.Lgs. 218/2017: recepisce la PSD2 (Payment Service Directive 2) in Italia.
- D.Lgs. 82/2005 – CAD (Codice dell'Amministrazione Digitale): art. 5 impone i pagamenti elettronici.
- D.Lgs. 217/2017: obbligo di PagoPA per la Pubblica Amministrazione.

Cos'è PagoPA

- Piattaforma digitale pubblica per pagamenti verso la Pubblica Amministrazione.
- Semplifica e garantisce pagamenti sicuri e tracciabili.
- Obbligatoria per gli enti pubblici (art. 5 CAD).



A cosa serve PagoPA

- Il sistema PagoPA serve per versare tributi, imposte, rette, bolli auto, ticket sanitari, multe e qualsiasi altro tipo di pagamento dovuto a:
- Comuni, Regioni, ASL;
- Scuole e Università;
- Agenzia delle Entrate e altri enti nazionali;
- Società a partecipazione pubblica e altri soggetti che forniscono servizi al cittadino

Come funziona PagoPA

- Ricevi un avviso con codice IUUV (Identificativo Unico di Versamento) o QR Code.
- Accedi a canali autorizzati: home banking, app, sito dell'ente.
- Controlla i dati e autorizza.
- Ricevi una ricevuta telematica valida legalmente.

Vantaggi per i cittadini

Pagamenti tracciabili e sicuri: ogni pagamento è gestito tramite canali sicuri e tracciato con certezza, garantendo la corretta acquisizione da parte dell'ente creditore.

Scelta tra più canali e banche: il cittadino può scegliere il PSP e lo strumento di pagamento (conto corrente, carta di credito, ecc.) che preferisce, conoscendo in anticipo i costi di commissione applicati dai vari operatori.

Riduzione di errori e frodi

Trasparenza e velocità

Errori comuni da evitare

- Usare bonifico tradizionale invece di PagoPA.
- Inserire codice IUV (Identificativo Univoco di Versamento) errato.
- Usare link o siti non ufficiali.
- Non salvare la ricevuta.

Problemi e soluzioni

- Pagamento non registrato → contattare ente e inviare ricevuta.
- Doppio pagamento → richiedere rimborso.
- Importo errato → avvisare ente e PSP (Payment Service Provider).
- Commissioni alte → confrontare diversi PSP

Problemi e soluzioni

1. **Phishing / Smishing:** truffa informatica che induce le vittime a fornire informazioni sensibili, come credenziali di accesso o dati finanziari tramite email, messaggi o siti web falsi.

2. **Vishing:** combinazione delle parole voice e phishing, riguarda una truffa che si avvale anche del contatto telefonico, per indurre la vittima a condividere informazioni personali, finanziarie o di sicurezza, ovvero a trasferire denaro

Problemi e soluzioni

3. **Spoofing:** inteso come tipologia di attacco che consente ad un attore malevolo di nascondere la propria identità, per risultare affidabile alla vittima designata e ottenere accesso a informazioni riservate e dati sensibili.

4. **Man in the browser:** installazione di uno spyware sul pc del cliente.

Problemi e soluzioni

5. **key logging:** il cliente riceve dal truffatore una mail contenente un allegato, che - una volta aperto - installa automaticamente sul suo pc un programma che consente al truffatore di captare i dati inseriti dal cliente o link sospetti.
6. **Falsi avvisi di pagamento.**
7. **App o portali falsi.**
8. **Canali non ufficiali o link sospetti.**

Come difendersi

- Non cliccare link sospetti.
- Controllare che l'URL inizi con https://.
- Verificare la fonte dell'avviso.
- Usare solo app ufficiali.
- Non condividere OTP (One Time Password), PIN o password.
- Segnalare a banca o Polizia Postale.

Vademecum pratico

- **Prima del pagamento:** controlla l'Identificativo Univoco di Versamento, beneficiario, importo, logo PagoPA.
- **Durante:** verifica dati e autorizza solo se corretti.
- **Dopo:** conserva la ricevuta e controlla la registrazione.

Quadro Normativo

- CAD (D.Lgs. 82/2005): regola la digitalizzazione della PA.
- D.Lgs. 217/2017: obbliga le PA a usare PagoPA.
- PSD2 (Direttiva UE 2015/2366): sicurezza e trasparenza.
- D.Lgs. 218/2017: attua la PSD2 in Italia.
- Linee guida PagoPA S.p.A. 2023: standard tecnici e operativi.

Consigli finali

- Usa sempre canali ufficiali.
- Leggi con attenzione i dati prima di confermare.
- Conserva la ricevuta.
- Diffida di messaggi urgenti o con errori.
- Mantieniti informato sulle novità.

Conclusione

- PagoPA e i pagamenti digitali rendono la vita più semplice e trasparente.
- La sicurezza nasce dalla consapevolezza.
- Un cittadino informato è un cittadino protetto.

Grazie per l'attenzione!

CONTATTI

U.Di.Con. REGIONALE PIEMONTE APS

Via San Donato 58 - 10144 Torino

Tel 011.2075267

WhatsApp 3515882443

E-mail: regionepiemonte@udicon.org

Sito: udiconpiemonte.org