GIORNATA FORMATIVA
il giorno **mercoledì 8 maggio 2024** dalle ore 10,00
Sede Civitella Casanova (PE)
via Roma 33 presso la **SALA ALESSANDRO**

_____ / _____

INPS
Come accedere con le modalità telematiche previste e gestire il proprio account digitale (Spid, SSN, CIE

Per accedere e gestire il tuo account digitale sul portale **INPS** utilizzando le modalità telematiche previste, puoi scegliere tra diversi metodi di autenticazione: **SPID**, **CIE** (Carta di Identità Elettronica) o **CNS** (Tessera Sanitaria/Carta Nazionale dei Servizi). Di seguito ti spiego come usare ciascuna di queste modalità per accedere al portale INPS e gestire il tuo profilo.

1. Accesso tramite SPID (Sistema Pubblico di Identità Digitale):

- **Passo 1**: Vai al sito ufficiale dell'INPS (www.inps.it) e clicca su **"Entra in MyINPS"**.
- **Passo 2**: Seleziona l'opzione **"SPID"** tra le modalità di accesso disponibili.
- **Passo 3**: Scegli il tuo Identity Provider (come Poste, Aruba, InfoCert, ecc.) e inserisci le tue credenziali SPID (nome utente e password).
- **Passo 4**: Inserisci il codice OTP (One-Time Password) se richiesto, per confermare l'accesso. Questo dipende dal livello di sicurezza del tuo SPID (Livello 2 o 3).
- **Gestione dell'account**: Una volta effettuato l'accesso, potrai gestire il tuo profilo personale, verificare contributi, richiedere prestazioni, consultare lo stato delle pratiche e accedere a vari servizi digitali offerti dall'INPS.

2. Accesso tramite CIE (Carta di Identità Elettronica):

- **Passo 1**: Accedi al portale INPS e clicca su **"Entra in MyINPS"**.
- **Passo 2**: Seleziona l'opzione **"CIE"**.
- **Passo 3**: Collega il **lettore di smart card** al computer oppure utilizza il tuo **smartphone con NFC** (Near Field Communication).
- **Passo 4**: Se utilizzi un lettore smart card, inserisci la CIE e il PIN della carta. Se usi lo smartphone, scarica l'app **CieID**, avvicina la carta al telefono e segui le istruzioni per completare l'accesso.

- **Gestione dell'account**: Dopo l'accesso con la CIE, puoi gestire il tuo account digitale INPS e usufruire degli stessi servizi accessibili tramite SPID.

3. Accesso tramite CNS (Carta Nazionale dei Servizi):

- **Passo 1**: Collega il **lettore di smart card** al tuo computer e inserisci la tua **tessera sanitaria** con chip.
- **Passo 2**: Vai sul sito INPS, clicca su **"Entra in MyINPS"** e seleziona l'opzione **"CNS"**.
- **Passo 3**: Inserisci il **PIN** della tessera sanitaria e segui le istruzioni per autenticarti.
- **Gestione dell'account**: Una volta autenticato, puoi accedere al tuo profilo INPS e gestire i servizi disponibili.

Servizi disponibili su MyINPS:

Indipendentemente dal metodo di autenticazione scelto, accedendo a **MyINPS** potrai:

- Verificare i tuoi **contributi pensionistici**.
- Consultare il **cedolino della pensione**.
- Richiedere la **disoccupazione NASpI**, il **reddito di cittadinanza**, e altri servizi di assistenza sociale.
- Scaricare e inviare documenti per prestazioni sociali e fiscali.
- Prenotare un appuntamento presso le sedi INPS o ottenere assistenza online.

Conclusione:

SPID, CIE, e CNS sono modalità sicure per accedere e gestire i servizi INPS online. SPID è il metodo più popolare per la sua semplicità, mentre la CIE e la CNS richiedono l'uso di lettori di smart card o smartphone con NFC

_____ / _____

Gestione in sicurezza del proprio conto bancario

Per gestire in sicurezza il proprio conto bancario, è essenziale seguire una serie di pratiche volte a proteggere le tue informazioni finanziarie e ridurre i rischi di frodi o accessi non autorizzati. Ecco alcune delle principali strategie di sicurezza:

1. Utilizzare password complesse e sicure

- **Crea una password forte**: Usa una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Evita parole comuni o informazioni personali (come nomi o date di nascita).
- **Cambia la password periodicamente**: Questo riduce il rischio che un eventuale accesso non autorizzato rimanga attivo nel tempo.
- **Autenticazione a due fattori (2FA)**: Attiva l'autenticazione a due fattori se disponibile. Questo aggiunge un ulteriore livello di sicurezza richiedendo un codice temporaneo inviato al telefono o generato da un'app (come Google Authenticator).

2. Verifica costantemente l'attività del conto

- **Controlla regolarmente gli estratti conto**: Monitora le transazioni per individuare eventuali spese sospette o non autorizzate. La maggior parte delle banche offre la possibilità di impostare notifiche automatiche via SMS o email per ogni transazione effettuata.
- **Confronta con le tue spese**: Ogni mese, verifica le transazioni con le tue ricevute e spese per assicurarti che tutto sia corretto.

3. Proteggere i dispositivi

- **Aggiorna software e antivirus**: Mantieni aggiornati il sistema operativo e il software antivirus per proteggere il tuo dispositivo da malware e virus che potrebbero rubare le tue credenziali bancarie.
- **Evita reti Wi-Fi pubbliche non sicure**: Non effettuare operazioni bancarie su reti Wi-Fi pubbliche, come quelle di caffè o aeroporti, poiché queste reti sono spesso poco protette e possono essere bersagli facili per gli hacker. Se necessario, utilizza una **VPN (Virtual Private Network)**.

4. Evitare phishing e truffe online

- **Non cliccare su link sospetti**: Le truffe di phishing sono progettate per indurti a inserire le tue credenziali su falsi siti bancari. Non cliccare mai su link presenti in email o messaggi sospetti che richiedono di accedere al tuo conto.
- **Verifica sempre l'indirizzo del sito**: Quando accedi al sito della tua banca, verifica che l'URL inizi con **https://** e che ci sia un'icona di un lucchetto accanto alla barra degli indirizzi, che indica una connessione sicura.

5. Usare solo app bancarie ufficiali

- Scarica l'app bancaria **solo dagli store ufficiali** (Google Play Store o Apple App Store). App non ufficiali possono contenere malware progettati per rubare le tue informazioni.
- **Disabilita l'accesso automatico**: Evita di mantenere aperto l'accesso automatico all'app della tua banca e imposta un blocco tramite PIN o dati biometrici (impronte digitali, riconoscimento facciale).

6. Attiva notifiche di sicurezza

- Imposta notifiche o avvisi per ogni operazione finanziaria significativa (prelievi, trasferimenti, acquisti). Questi avvisi ti consentono di reagire rapidamente in caso di attività sospette.

7. Sicurezza fisica

- **Proteggi le tue carte**: Non condividere mai il PIN della tua carta di credito o debito, e assicurati di coprire il tastierino quando lo inserisci nei bancomat o nei POS.
- **Sostituzione immediata in caso di furto**: Se sospetti che la tua carta sia stata rubata o clonata, blocca immediatamente la carta tramite il servizio clienti della tua banca.

8. Utilizzare carte virtuali per acquisti online

- Alcune banche offrono carte di credito o debito virtuali che puoi utilizzare esclusivamente per acquisti online, limitando il rischio di esposizione dei dati della tua carta principale.

9. Limiti di spesa e prelievo

- Imposta limiti di spesa giornalieri o mensili per le tue carte di credito o debito. Questo riduce il danno potenziale in caso di furto o accesso non autorizzato.

10. Backup dei dati e tracciabilità

- Conserva un backup sicuro delle informazioni importanti, come estratti conto e documenti fiscali, ma **non salvare mai le tue password** su dispositivi non sicuri o in file non protetti.

Seguendo queste pratiche, puoi ridurre significativamente i rischi associati alla gestione del tuo conto bancario online e proteggere le tue finanze da accessi non autorizzati e frodi.

BANCHE E PRIVACY

Le **banche** hanno un ruolo fondamentale nella gestione della privacy dei dati personali dei clienti, poiché trattano informazioni sensibili come i dati finanziari e personali. La protezione della **privacy bancaria** è regolamentata da leggi nazionali e sovranazionali, tra cui il **Regolamento Generale sulla Protezione dei Dati (GDPR)** in Europa, che impone stringenti norme per il trattamento dei dati personali.

Aspetti principali della privacy in banca:

1. Protezione dei dati personali

Le banche devono garantire che i dati personali siano trattati in modo sicuro e trasparente. Questo include:

- **Consenso informato**: Le banche devono raccogliere i dati personali solo con il consenso informato del cliente e devono fornire informazioni chiare su come verranno utilizzati.
- **Minimizzazione dei dati**: Possono raccogliere solo i dati necessari per gli scopi dichiarati (come l'apertura di un conto o l'emissione di un prestito).
- **Conservazione limitata**: I dati personali devono essere conservati solo per il tempo strettamente necessario e poi eliminati in modo sicuro.

2. Trasparenza e diritto all'informazione

I clienti hanno il diritto di sapere come i propri dati vengono utilizzati e conservati. Le banche devono informare in maniera chiara circa:

- Lo scopo della raccolta dei dati.
- Chi può accedere ai dati (ad esempio, se i dati saranno condivisi con terzi, come agenzie di recupero crediti o altre istituzioni finanziarie).
- I diritti dell'utente, tra cui il diritto di accesso, rettifica, cancellazione e opposizione al trattamento dei propri dati.

3. Sicurezza delle informazioni

Le banche sono tenute a proteggere i dati personali attraverso misure tecniche e organizzative adeguate, tra cui:

- **Crittografia dei dati**: I dati sensibili devono essere criptati per evitare accessi non autorizzati.
- **Controllo degli accessi**: Le banche devono garantire che solo il personale autorizzato possa accedere ai dati personali.
- **Monitoraggio delle violazioni**: Devono avere sistemi per individuare e rispondere rapidamente a eventuali violazioni della sicurezza dei dati.

4. Diritti degli utenti

I clienti delle banche, in linea con il GDPR, hanno il diritto di:

- **Accesso ai dati**: Verificare quali dati personali sono in possesso della banca.
- **Rettifica dei dati**: Correggere eventuali errori o inesattezze.
- **Cancellazione (Diritto all'oblio)**: Chiedere che i propri dati vengano eliminati in determinate circostanze.
- **Portabilità dei dati**: Richiedere che i propri dati siano trasferiti a un altro fornitore di servizi finanziari.
- **Revoca del consenso**: In qualsiasi momento, possono revocare il consenso per il trattamento dei propri dati.

5. Condivisione dei dati con terze parti

Le banche possono condividere i dati dei clienti solo con il consenso esplicito o quando è necessario per eseguire servizi legittimi (come la gestione di pagamenti o la concessione di mutui). In questi casi, le banche devono garantire che anche i terzi rispettino le stesse norme di protezione dei dati.

6. Open Banking e GDPR

L'introduzione dell'**open banking** ha aumentato la condivisione dei dati tra le banche e terze parti (come le fintech), ma sempre nel rispetto delle norme del GDPR. L'utente deve dare il proprio consenso esplicito alla condivisione dei dati con questi servizi.

Conclusione:

La gestione della privacy nelle banche è strettamente regolamentata per proteggere i dati personali dei clienti, con norme che coprono tutto, dalla raccolta dei dati all'accesso, alla condivisione e alla conservazione. I clienti devono essere consapevoli dei loro diritti e delle misure di protezione adottate dalle banche per garantire la sicurezza delle informazioni.