Home banking, cos'è e come funziona

Comune di Modena

Modena Città Sicura

Polizia Locale Comune Modena

Palestra Digitale Innovation Lab

MODI modalitàdifferenti

“La prevenzione rende sicuri: azioni integrate per il contrasto di truffe e raggiri ai danni della popolazione anziana”

Finanziato dal Fondo Unico di Giustizia del Ministero degli Interni.

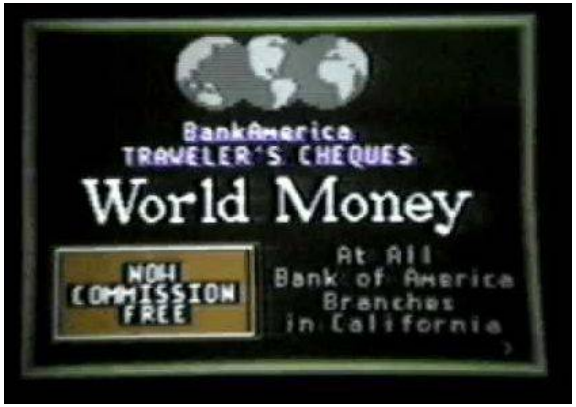
Cos’è l’Home Banking

Chiamato anche **internet banking**, è un servizio che permette a chi ha un conto corrente di poter condurre tutte le operazioni bancarie tramite internet, senza bisogno di recarsi fisicamente presso propria banca.

Cos'è l'Home Banking

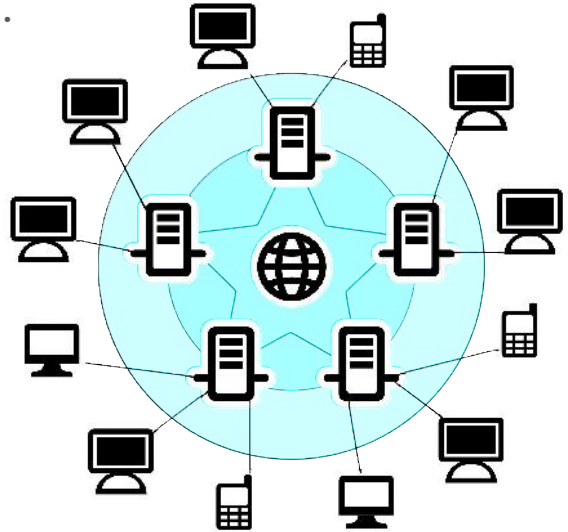
- **Anni '80** ➡ primo esperimento: toni audio su linea telefonica tramite un tastierino numerico
- **Anni '90** ➡ diffusione delle connessioni internet: interattività con la banca grazie ai Videotex
- **Oggi** ➡ uno dei servizi immancabili dell'offerta bancaria

Videotex



Cosa serve?

Per poter usufruire dell’home banking è sufficiente avere una connessione internet ed un PC o uno smartphone.



Banche virtuali

L'home banking è un servizio adottato inizialmente dalle banche tradizionali e ha permesso successivamente la nascita di banche 100% online.

L'abbattimento delle infrastrutture fisiche legate all'internet banking ha creato benefici tanto per i clienti quanto per le banche stesse.

Banche virtuali

- N26
- Revolut
- IWBank
- CheBanca!
- Webank
- Hype

Vantaggi

- Tutte le operazioni a portata di click
- Risparmio di tempo e spese per il tragitto
- Alleggerimento del carico lavorativo delle banche
- È utilizzabile ovunque, anche all'estero
- Ha costi di gestione del conto nettamente inferiori
- È disponibile in qualsiasi momento, 24 ore su 24
- È veloce

Svantaggi

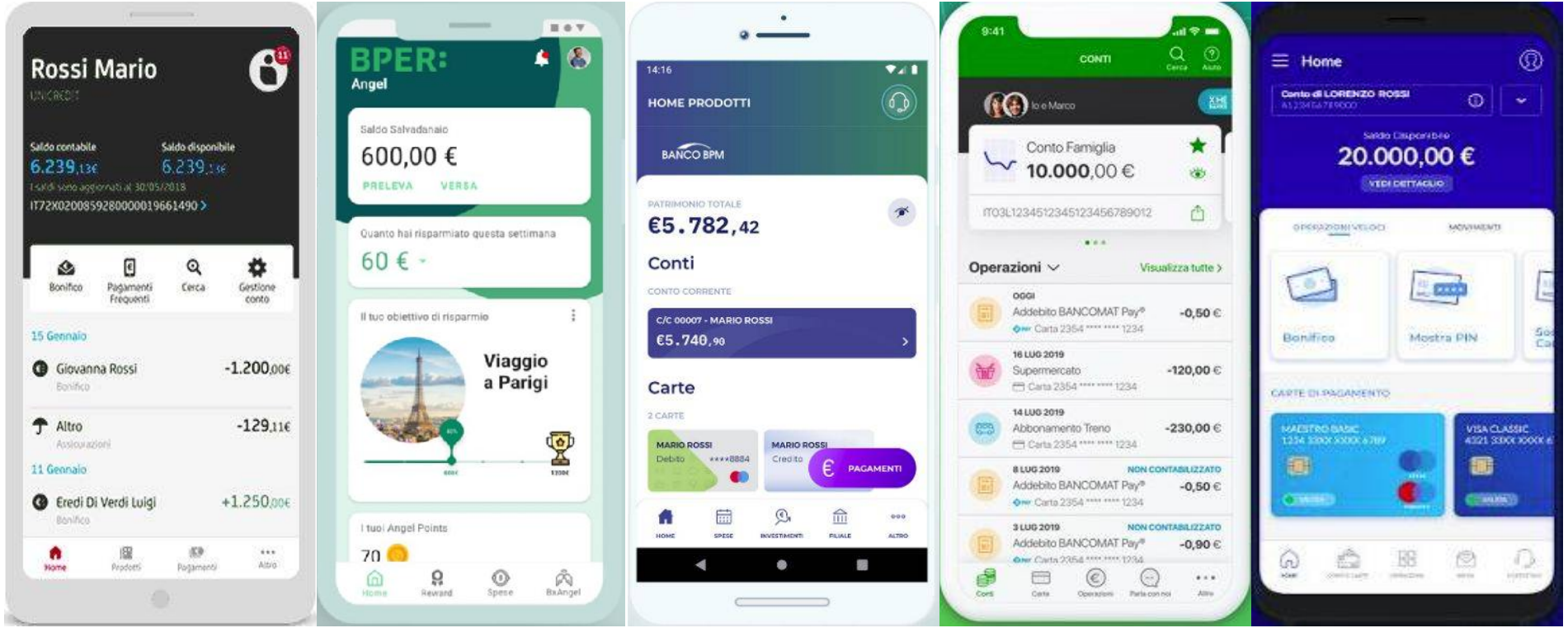
- La sicurezza
- L’assenza del bancomat
- La mancanza della sede fisica
- La connessione a internet

App o sito web?

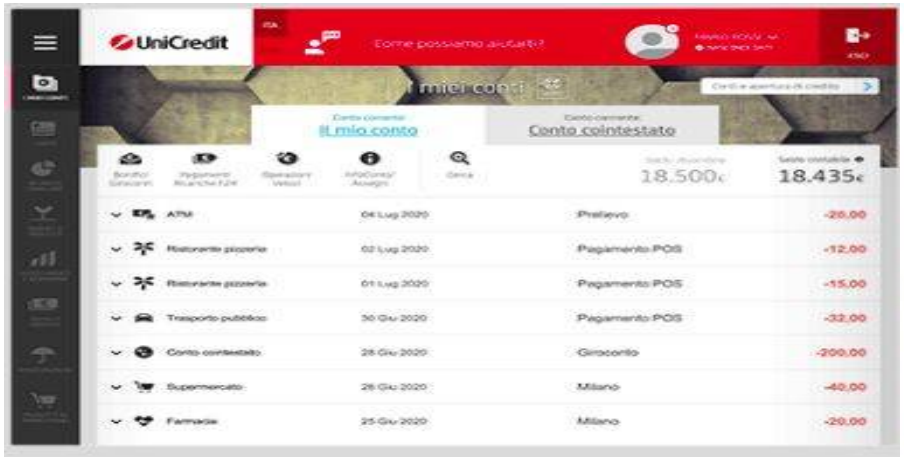
- Il sito è più funzionale
- L'app è più pratica

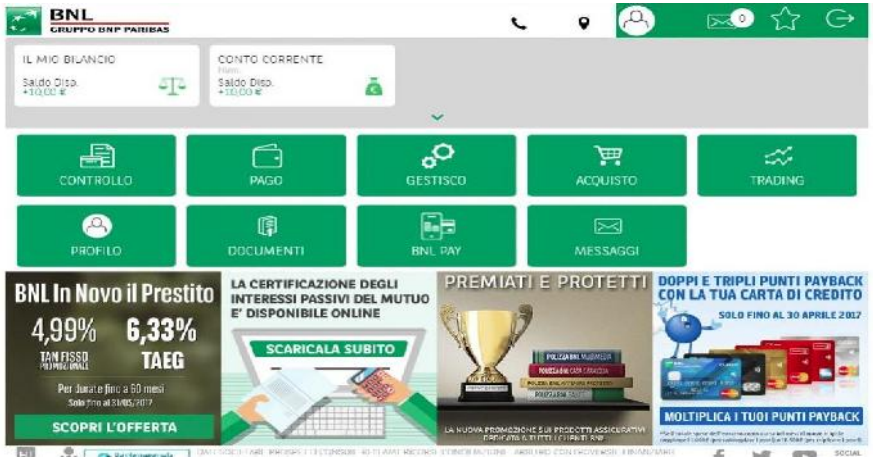
Non tutte le app di mobile banking sono uguali e non tutte offrono gli stessi servizi: solitamente sono meno complete rispetto alle piattaforme di home banking alle quali accediamo da pc, ma comunque sono utilissime per compiere tutte le operazioni più semplici e veloci.

App

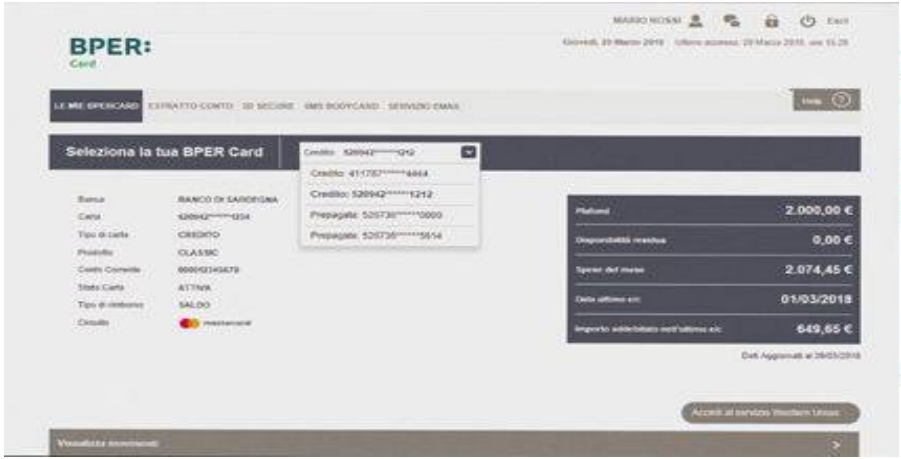

Rossi Mario
Saldo contabile
6.239,13€
Saldo disponibile
6.239,13€
IT72X0200859280000019661490
Bonifico
Pagamenti Frequenti
Cerca
Gestione conto
15 Gennaio
Giovanna Rossi
-1.200,00€
Bonifico
Altro
-129,11€
Assicurazioni
11 Gennaio
Eredi Di Verdi Luigi
+1.250,00€
Bonifico
Home
Prodotti
Pagamenti
Altro
BPER:
Angel
Saldo Salvadanaio
600,00 €
PRELEVA
VERSA
Quanto hai risparmiato questa settimana
60 €
Il tuo obiettivo di risparmio
Viaggio a Parigi
I tuoi Angel Points
70
Home
Reward
Spese
BxAngel
14:16
HOME PRODOTTI
BANCO BPM
PATRIMONIO TOTALE
€5.782,42
Conti
CONTO CORRENTE
C/C 00007 - MARIO ROSSI
€5.740,90
Carte
2 CARTE
MARIO ROSSI
Debito
****8884
MARIO ROSSI
Credito
PAGAMENTI
HOME
SPESE
INVESTIMENTI
FILIALE
ALTRO
9:41
CONTI
Cerca
Aiuto
Io e Marco
Conto Famiglia
10.000,00 €
IT03L1234512345123456789012
Operazioni
Visualizza tutte
OGGI
Addebito BANCOMAT Pay®
-0,50 €
Carta 2354 **** **** 1234
16 LUG 2019
Supermercato
-120,00 €
Carta 2354 **** **** 1234
14 LUG 2019
Abbonamento Treno
-230,00 €
Carta 2354 **** **** 1234
8 LUG 2019
NON CONTABILIZZATO
Addebito BANCOMAT Pay®
-0,50 €
Carta 2354 **** **** 1234
3 LUG 2019
NON CONTABILIZZATO
Addebito BANCOMAT Pay®
-0,90 €
Carta 2354 **** **** 1234
Conti
Carte
Operazioni
Parla con noi
Altro
Home
Conto di LORENZO ROSSI
Saldo Disponibile
20.000,00 €
VEDI DETTAGLIO
OPERAZIONI VELOCI
MOVIMENTI
Bonifico
Mostra PIN
CARTE DI PAGAMENTO
MAESTRO BASIC
VISA CLASSIC

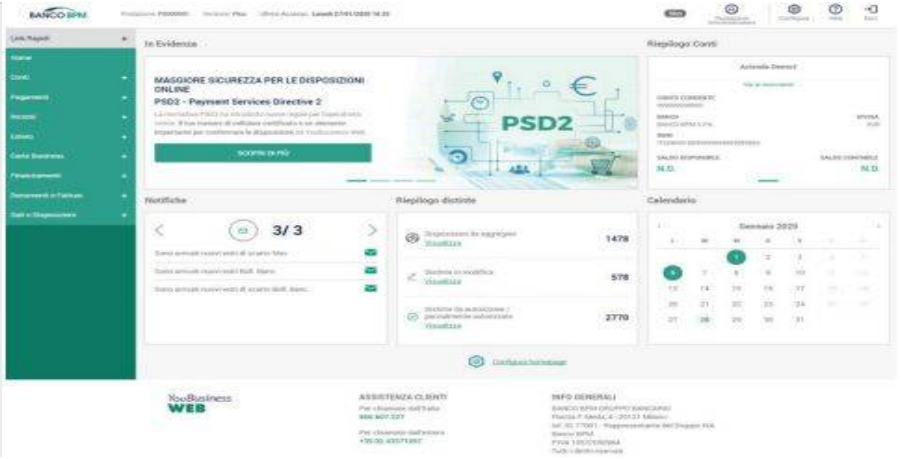
Sito web


UniCredit
Come possiamo aiutarti?
I miei conti
Il mio conto
Conto cointestato
18.500€
18.435€
ATM
Ristorante pizzeria
Ristorante pizzeria
Trasporto pubblico
Conto contestato
Supermercato
Farmacia


BNL
GRUPPO BNP PARIBAS
IL MIO BILANCIO
CONTO CORRENTE
CONTROLLO
PAGO
GESTISCO
ACQUISTO
TRADING
PROFILO
DOCUMENTI
BNL PAY
MESSAGGI
BNL In Novo il Prestito
4,99%
6,33%
TAEG
SCOPRI L'OFFERTA
LA CERTIFICAZIONE DEGLI INTERESSI PASSIVI DEL MUTUO E' DISPONIBILE ONLINE
SCARICALA SUBITO
PREMIATI E PROTETTI
DOPPI E TRIPLI PUNTI PAYBACK CON LA TUA CARTA DI CREDITO
SOLO FINO AL 30 APRILE 2017
MOLTIPLICA I TUOI PUNTI PAYBACK

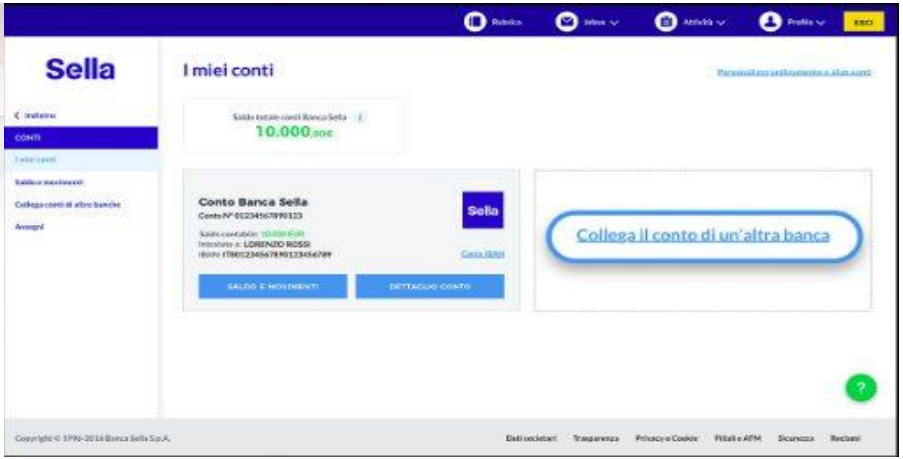
Sito web


BPER:
Card
Seleziona la tua BPER Card
2.000,00 €
0,00 €
2.074,45 €
01/03/2018
649,65 €


In Evidenza
MAGGIORE SICUREZZA PER LE DISPOSIZIONI ONLINE
PSD2 - Payment Services Directive 2
PSD2
Riepilogo Conti
Notifiche
3/ 3
Riepilogo distinte
1478
578
2770
Calendario
YouBusiness WEB
ASSISTENZA CLIENTI
INFO GENERALI

Sito web


INTESA SANPAOLO
Cerca nel sito
Home
CONTI E SALVADANAIO
I MIEI CONTI
Conto 1000/000
Conto
Conto
Conto minore
DETTAGLIO CONTO
Ultimi 30 Giorni
Ultimi 60 Giorni
Ultimi 90 Giorni
RICERCA AVANZATA
Uscite
Saldo disponibile
Entrate
Tutte le operazioni
SCARICA PDF | SCARICA EXCEL
Movimenti degli ultimi 30 giorni


Sella
I miei conti
10.000,00€
Conto Banca Sella
Sella
Collega il conto di un'altra banca
SALDO E MOVIMENTI
DETTAGLIO CONTO

Servizi offerti

- Gestione carte
- Bonifici
- Pagamenti rapidi
- Bollette, tasse, abbonamenti
- Salvadanaio
- Investimenti
- Categorie con grafici, budget, entrate e uscite
- Prenotazione appuntamento in banca

Servizi offerti

- Visualizzi i tuoi conti o quelli cointestati
- Controlli l'andamento della tua capacità di risparmio
- Funzioni “Recupera dati” e “Rubrica” per i bonifici
- Pagamento Bollettini inquadrando QR code o codice a barre
- Paghi i tributi, incluso il bollo auto con il CBill-Pago PA
- Saldo, movimenti e credito disponibile in una sola vista
- Ricarica prepagata o credito del cellulare
- Simulazioni di finanziamento

Come accedere in sicurezza?

- Vpn
- WiFi di casa
- 3g,4g,5g
- Navigazione Anonima

- WiFi Pubblici
- Hot Spot

Da ricordare!

- Le banche non chiedono mai informazioni personali (come data di nascita, indirizzo di posta elettronica, numero di telefono o di conto corrente) tramite sms, e-mail o telefono.
- Cambiare spesso la password di accesso, almeno una volta al mese.
- Attivare metodi di autenticazione aggiuntivi, a due fattori (2FA).
- Non accedere mai al proprio conto su Wi Fi di luoghi pubblici.
- Ricordarsi di fare il Log Out dal conto.

Autenticazione forte (2018)

*La direttiva europea PSD2 (2015/2366/UE) ha recentemente introdotto il tema dell'**autenticazione forte del cliente**, in inglese Strong Customer Authentication o semplicemente **SCA**.*

*La Strong Customer Authentication impone che **tutte le operazioni di pagamento elettronico,** e alcune altre operazioni a distanza che comportino un rischio di frode, **vengano confermate e autorizzate combinando due o più fattori di autenticazione**, scelti tra qualcosa che solo chi effettua l'operazione **conosce** (ad esempio un PIN o una password), qualcosa che solo chi effettua l'operazione **possiede** (un'app su un dispositivo mobile o una chiave che genera codici OTP), oppure un elemento di inerenza, cioè qualcosa che **contraddistingue univocamente l'utente** (l'impronta digitale, la geometria del volto, o un'altra caratteristica biometrica).*

*I fattori scelti devono essere reciprocamente **indipendenti**, in modo che la violazione di uno dei fattori non comprometta l'affidabilità degli altri.*

Metodi di autenticazione

- SMS di conferma
- Notifica Push
- Chiavetta OTP (One Time Password)
- Applicazioni OTP
- Accesso Biometrico tramite sensore di impronte digitali
- Riconoscimento del volto
- Password Sicure
- Autenticazione a doppio Fattore (2FA)

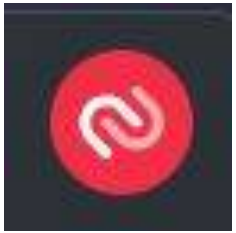
Chiavetta con il token

- Mobile token: si tratta di uno strumento che genera automaticamente OTP (One Time Password), cioè password valide per un solo utilizzo.

Le OTP possono essere utilizzate come unico fattore di autenticazione, o in aggiunta ad un altro fattore, come può essere la password dell'utente o un PIN in modo da realizzare una autenticazione a due fattori.

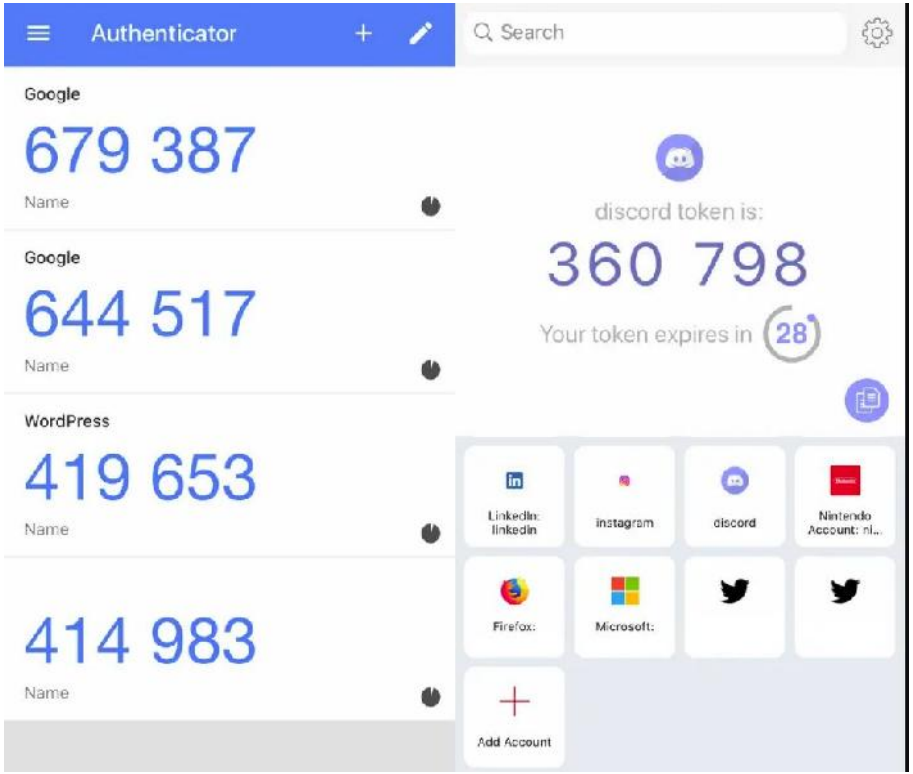
App con il token OTP

Sugli smartphone, le OTP possono anche essere consegnate direttamente tramite l'app stessa della banca, o addirittura con app di autenticazione dedicate come Authy, Duo, Microsoft Authenticator e Google Authenticator.



App con il token OTP

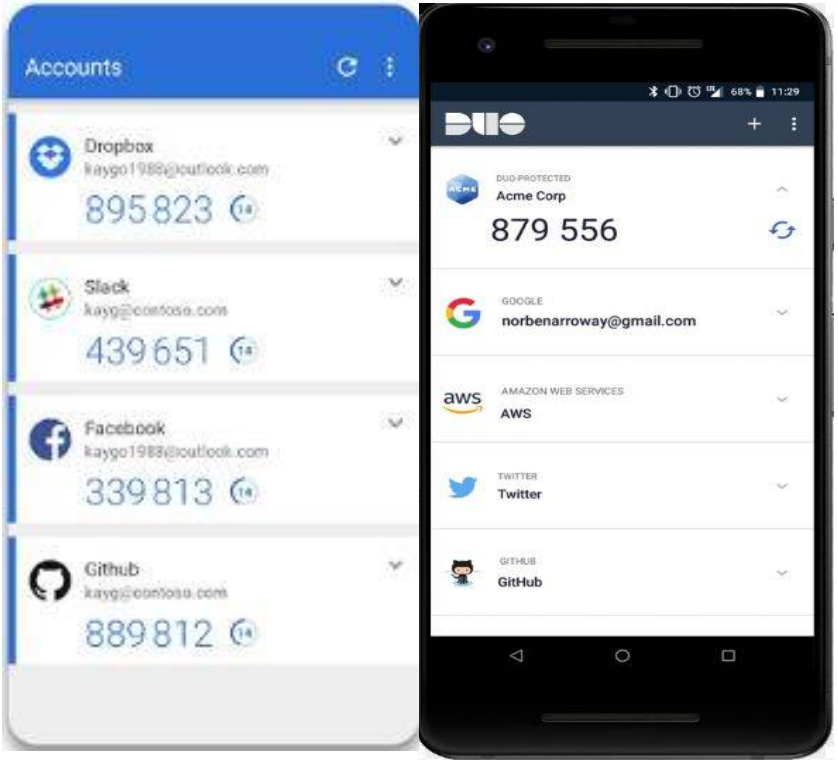
Google Authenticator



Authy

App con il token OTP

Microsoft Authenticator

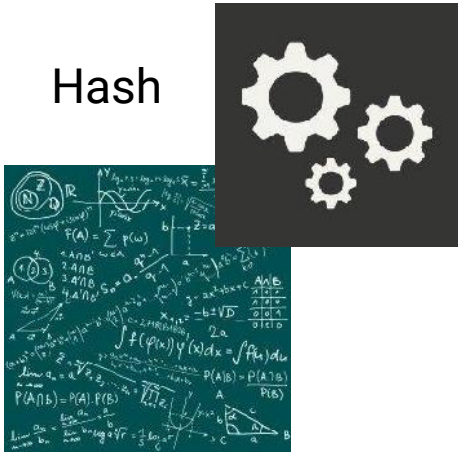


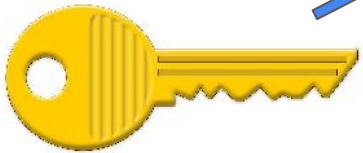
Duo

Come funziona l'OTP?

Fattore Tempo

Hash





Chiave univoca

OTP

Password sicura

- Usa sempre una password univoca per ogni account. Il rischio è di subire una violazione su tutti i siti in una volta sola.
- Quando crei una password non usare informazioni che ti rendano personalmente identificabile: nomi, compleanni e indirizzi sono facili da ricordare, ma anche da trovare online.
- Assicurati che le tue password contengano almeno 12 caratteri e che comprendano lettere, numeri e caratteri speciali.
- Aiutati a ricordarle utilizzando frasi o di canzoni o del tuo film preferito. Aggiungi caratteri a caso, ma sempre utilizzando modelli difficili.

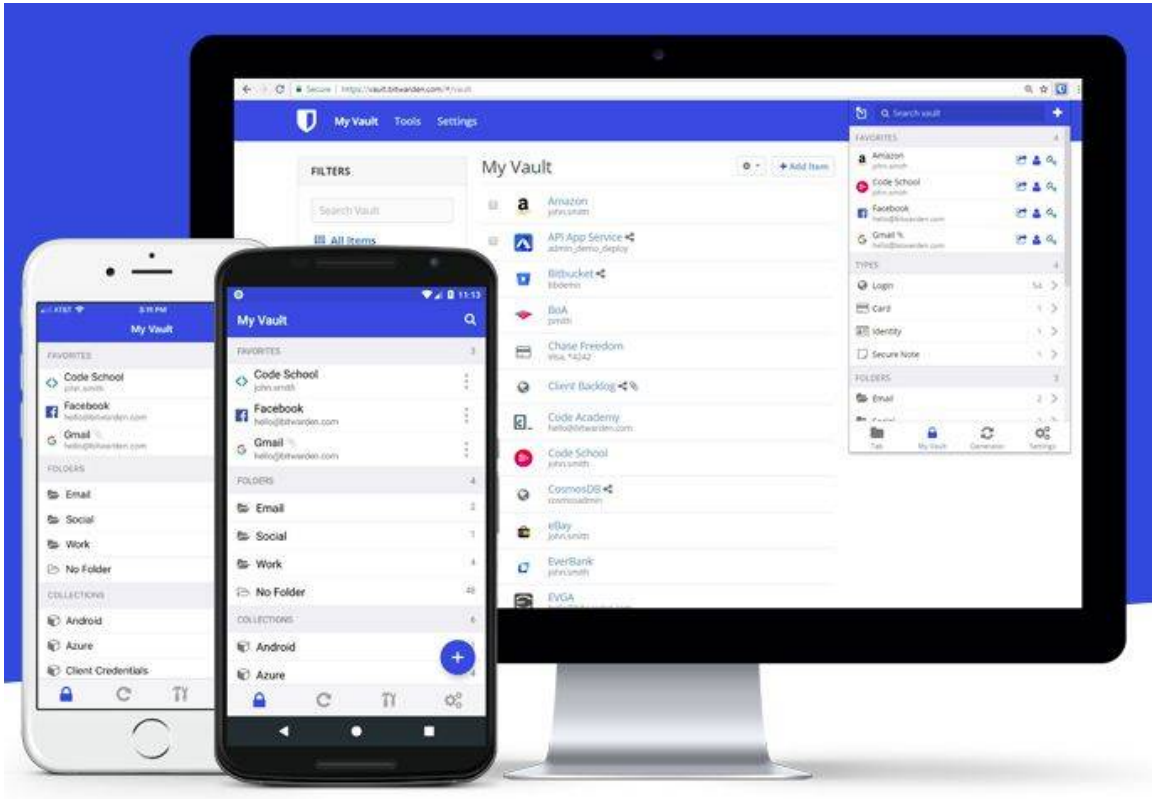
Password sicura

- Evita password deboli, di uso comune come ciao1234 o password1. Ecco alcuni esempi di una password forte: S&2x4S12nLS1*, JANa@sx3l2&s$, 49915w5$oYmH.
- Modifica le password, quando è opportuno, ad esempio dopo averle condivise con qualcuno, se è stata violata o se dall’ultima volta che hai cambiato le password è trascorso più di un anno.
- Non condividere mai le password via email o SMS.
- Usa un gestore di password per salvare le tue password.

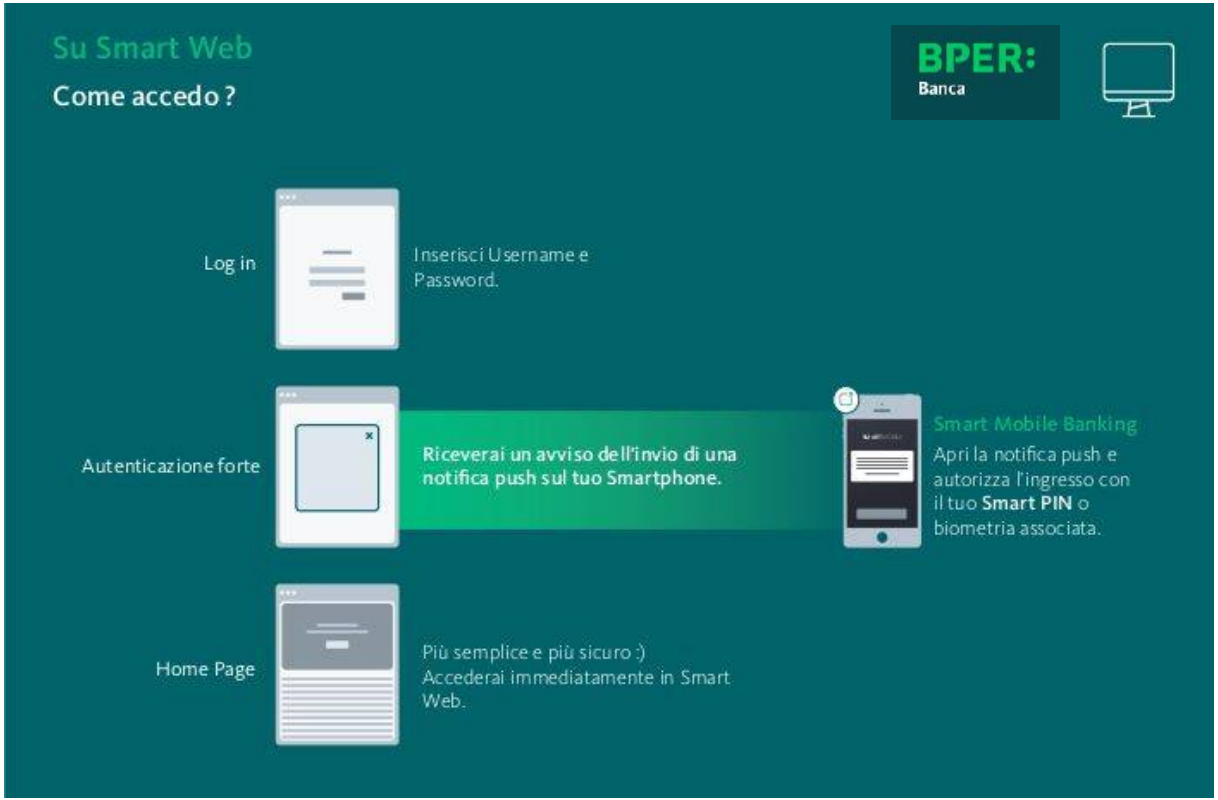
Archivi per le password

- Last Pass
- Bit Warden
- 1Password
- Nord Pass
- Kee Pass
- Dash Lane
- Roboform
- Keeper
- Sticky Password

Archivi per le password



Esempio di Autenticazione



Esempio di Autenticazione

Esempio di Autenticazione

Esempio di Autenticazione

Esempio di Autenticazione

Esempio di Autenticazione

Glossario

Codice utente
è un codice numerico a 8 cifre necessario a identificare ogni cliente.
Puoi sempre recuperare il tuo codice utente qui.

Alias
è una parola che puoi personalizzare e che può sostituire il tuo codice utente in fase di login (è più facile da ricordare!). Puoi crearlo o modificarlo all'interno di Smart Web > Sicurezza > Gestione Alias

Password
è un codice numerico di almeno 8 cifre che, insieme al codice utente/alias, è necessario per autenticarsi sui canali Smart. Puoi sempre modificare la tua password qui.

Smart PIN
è un codice numerico a 5 cifre che ti servirà per autenticarti all'interno dei canali Smart. Puoi sempre modificarlo all'interno dell'app Smart Mobile Banking.

Esempio di Autenticazione

Biometria

può essere associata al tuo Smart PIN, e comprende l'impronta digitale o il riconoscimento facciale. Puoi sempre modificare questa impostazione all'interno dell'app Smart Mobile Banking

Codice OTP

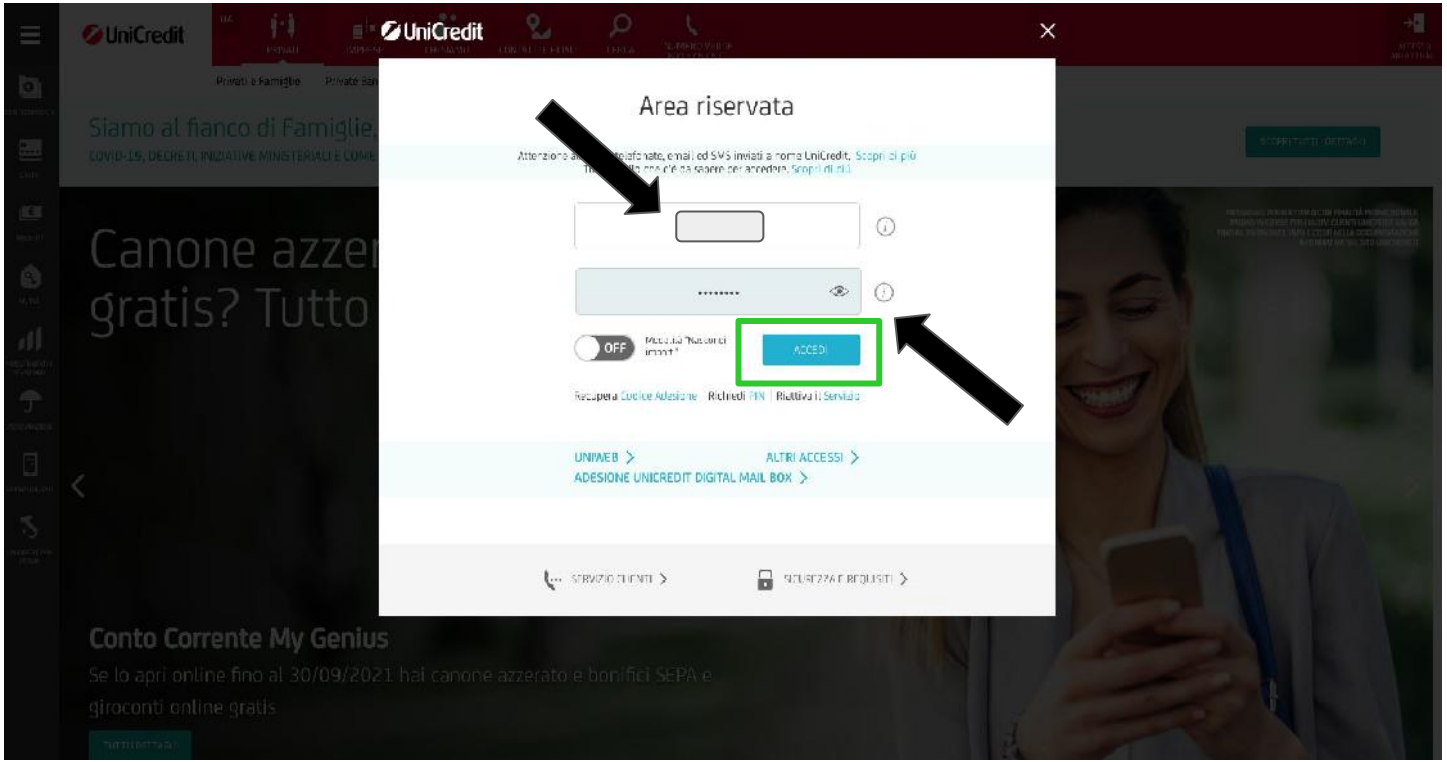
è un codice di 6 cifre che richiedi sui canali Smart della banca e che ricevi tramite SMS. Fino all'aggiornamento sarà necessario per effettuare accesso e operazioni, successivamente potrai utilizzare Smart PIN.
Nel caso in cui non dovessi ricevere le notifiche push sul tuo smartphone oppure in assenza di connessione internet, potrai generare un OTP anche dall'app Smart Mobile Banking.

Codice di sicurezza (codice per lo sblocco dell'utenza)

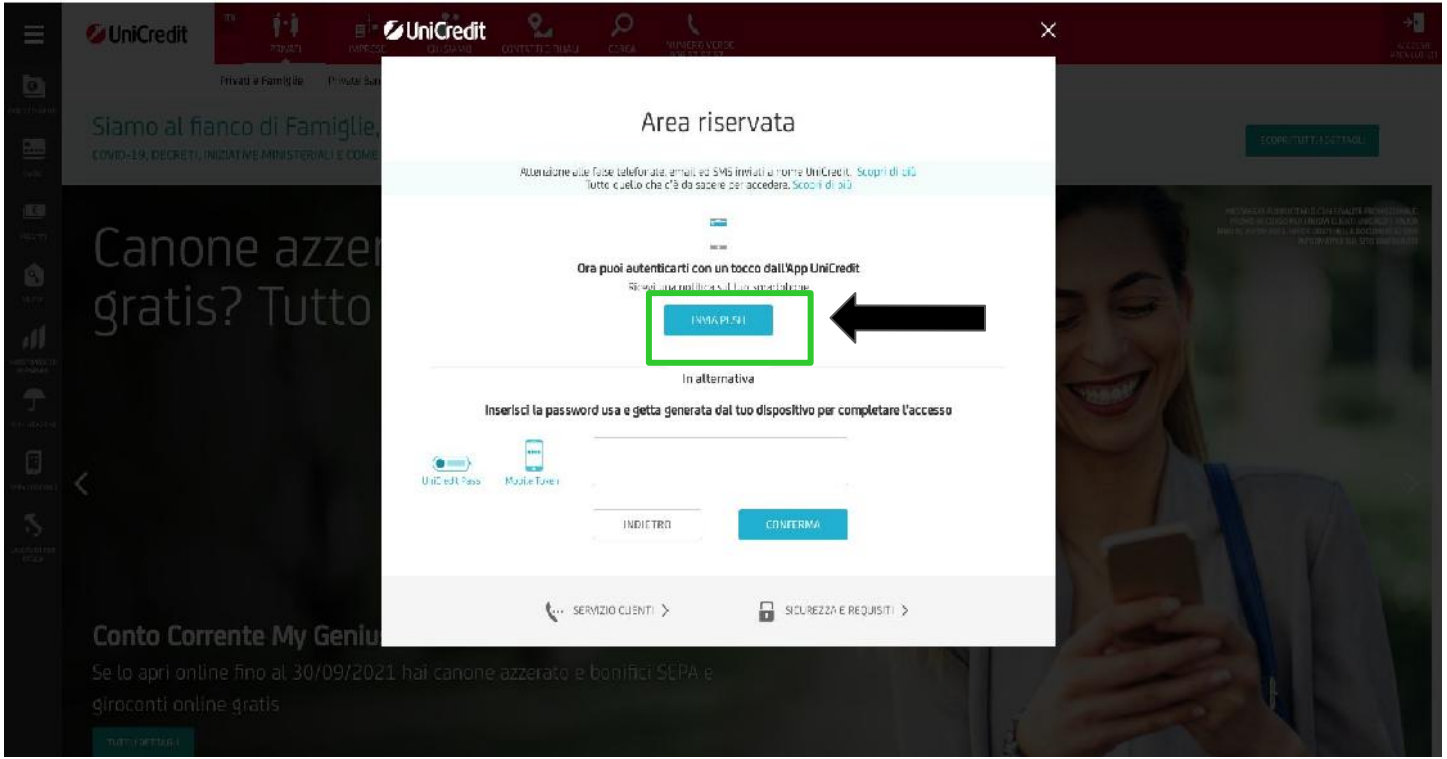
è un codice di 20 caratteri che ti permette, in caso di necessità, di sbloccare la tua utenza. Lo trovi nella busta che ti è stata consegnata in filiale quando hai sottoscritto la tua utenza Smart Web.

Esempio di Autenticazione

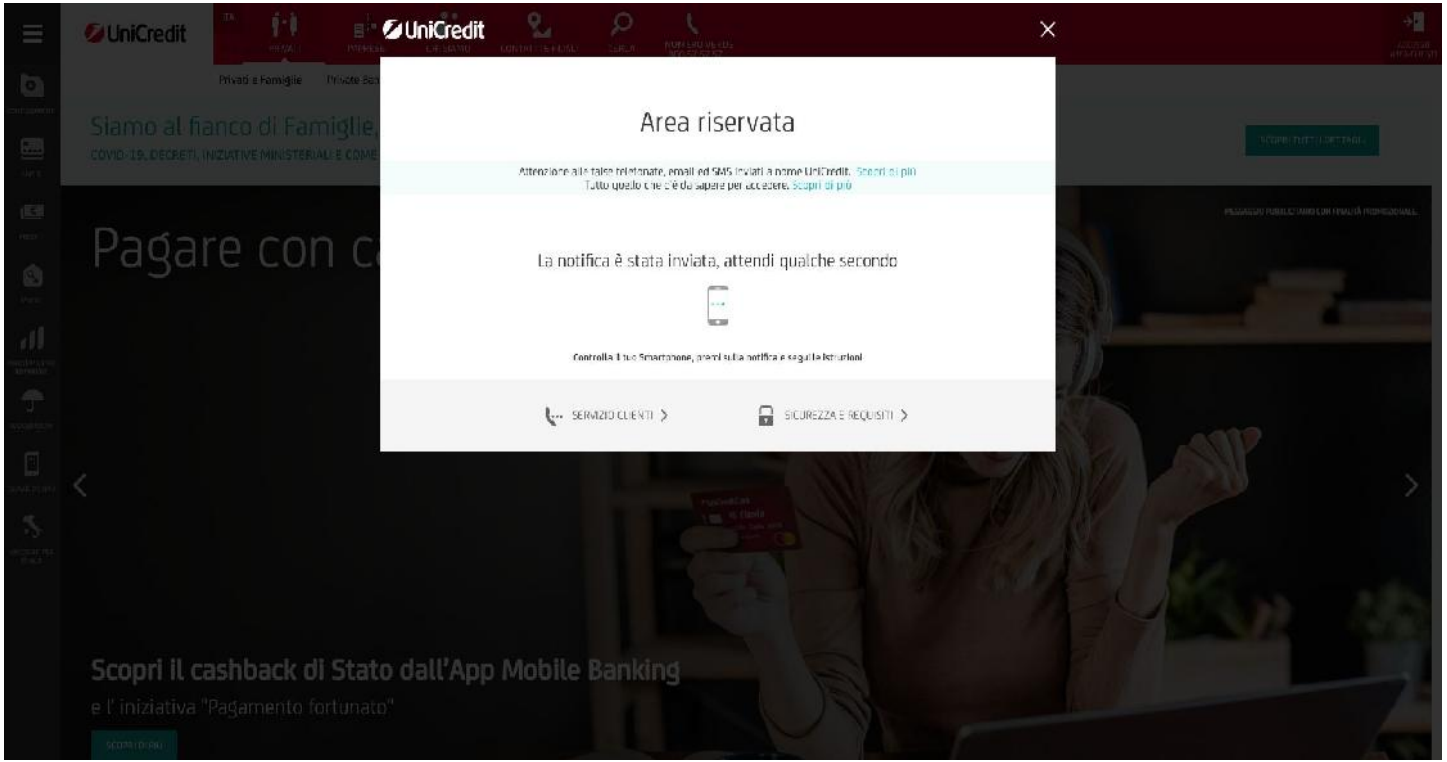
Esempio di Autenticazione



Esempio di Autenticazione



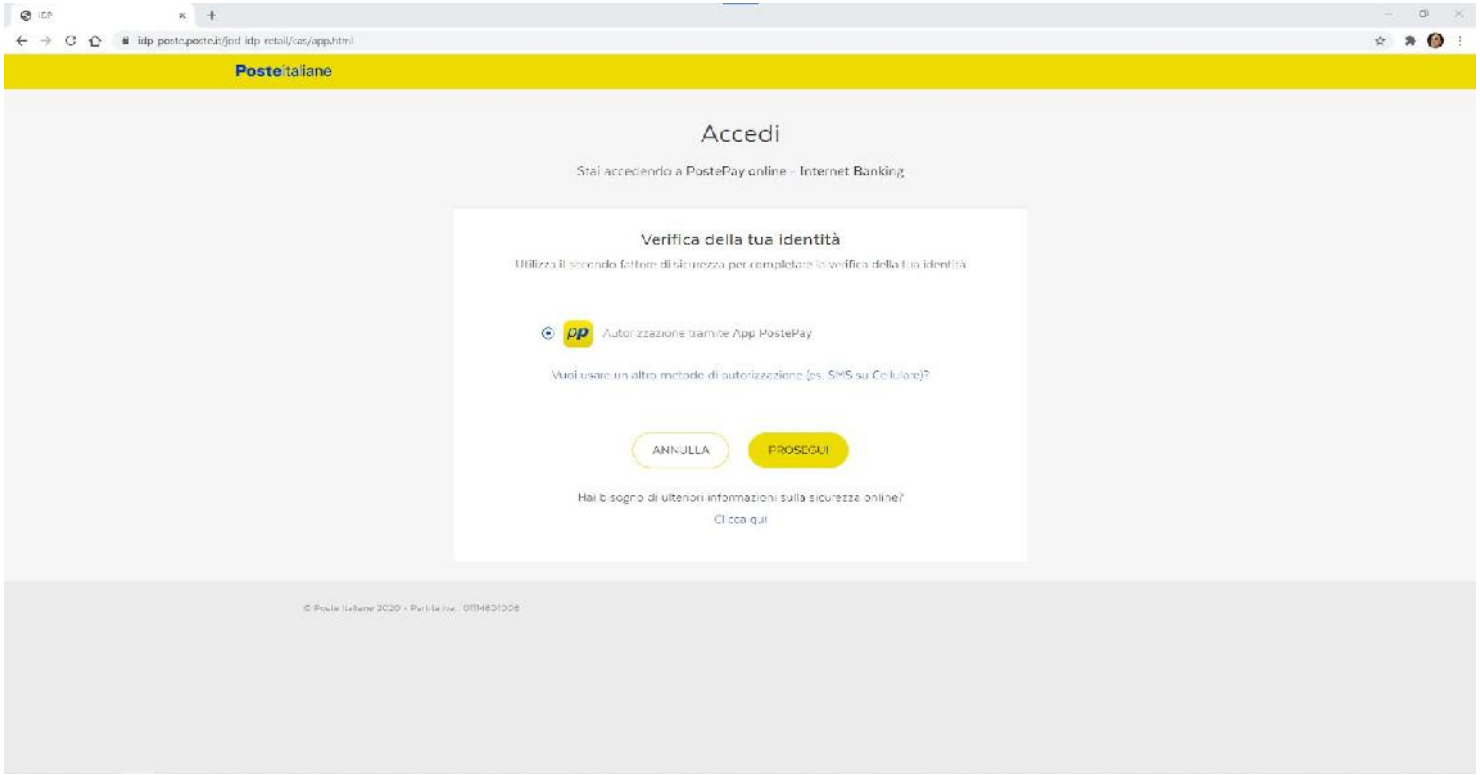
Esempio di Autenticazione



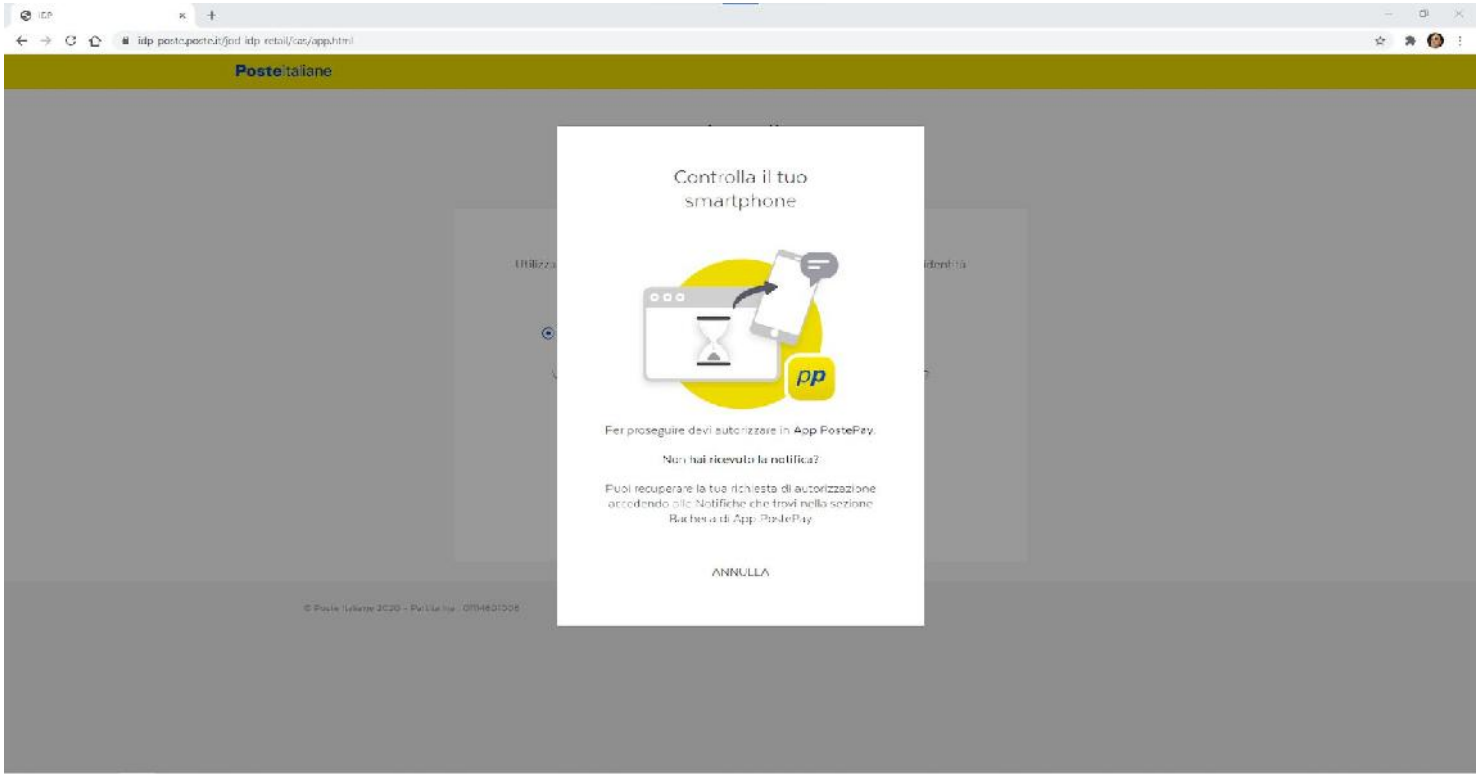
Esempio di Autenticazione

Esempio di Autenticazione (2FA)

Esempio di Autenticazione (2FA)



Esempio di Autenticazione (2FA)



Esempio di Autenticazione (2FA)

Tecniche di attacco (Man in the Middle)

Pc o Smartphone

Normale connessione (WiFi Pubblico)

Web

Tecniche di attacco (Man in the Middle)

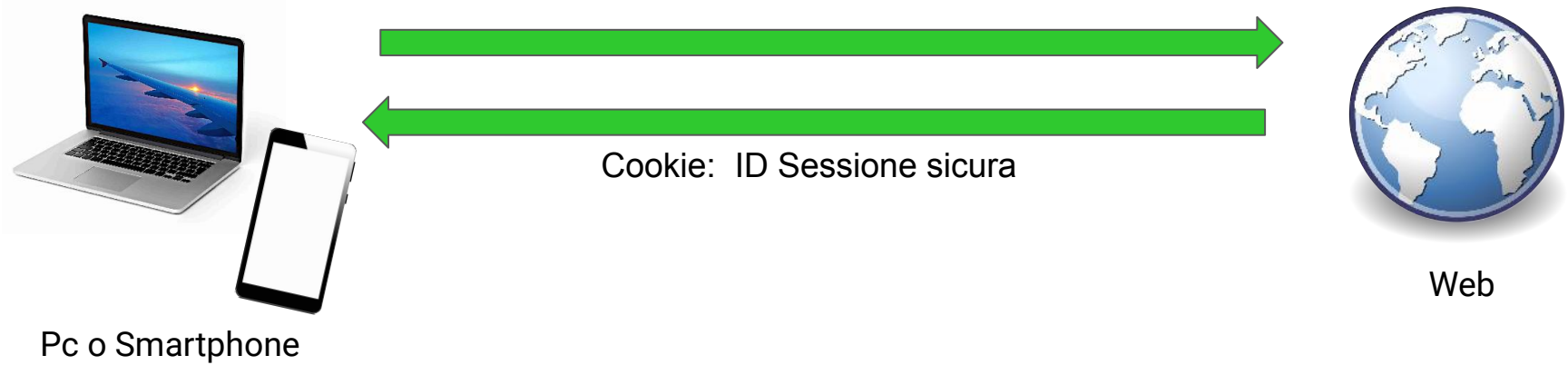
Tecniche di attacco (App Corrotte)

Tecniche di attacco (Cookie Poisoning)

Il "cookie" è un semplice file di testo che viene scaricato dal PC o smartphone per archiviare informazioni legate alla navigazione di un determinato sito.

I Cookie vengono scaricati dal Server Web che ospita il sito sui browser (Internet Explorer, Mozilla Firefox, Google Chrome, etc…). Tali file risiedono quindi nel dispositivo dell'utente e vengono utilizzati/letti durante le visite successive al sito.

Tecniche di attacco (Cookie Poisoning)



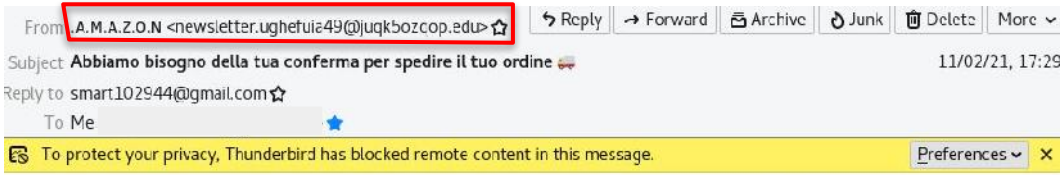
Tecniche di attacco (Cookie Poisoning)

Tecniche di attacco (Phishing)

Il phishing è una truffa che sfrutta l'ingegneria sociale attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Il termine phishing è una variante di fishing ("pescare" in lingua inglese) e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente.

Tecniche di attacco (Phishing)



Tecniche di attacco (Phishing)

Gentile cliente,

Nell'ambito di un progetto di verifica dei dati anagrafici forniti durante la sottoscrizione dei servizi di Poste Italiane e stata riscontrata una incongruenza relativa ai dati anagrafici in oggetto da Lei forniti all momento della sottoscrizione contrattuale.
L'inserimento dei dati alterati puo costituire motivo di interruzione del servizio secondo gli art. 135 e 137/c da Lei accettati al momento della sottoscrizione, oltre a costituire reato penalmente perseguibile secondo il C.P.P art. 415 del 2009 relativo alla legge contro il riciclaggio e la trasparenza dei dati forniti in auto certificazione.
Per ovviare al problema e necessaria la verifica e l'aggiornamento dei dati relativi all'anagrafica dell'Intestatario dei servizi Postali.
Effettuare l'aggiornamento dei dati cliccando sul seguente collegamento sicuro:

https://bancopostaonline.poste.it/bpol/formslogin.asp

Se la nostra richiesta viene ignorata, non avremo altra scelta che bloccare temporaneamente il suo account.

La ringraziamo per aver scelto i nostri servizi.

Distinti Saluti
Posteitaliane

Posteitaliane

Tecniche di attacco (Phishing)

Da: Tim <support@citytec.com>
Oggetto: "One for two"
A:

Data: Lunedì 16 febbraio 2015, 15:06

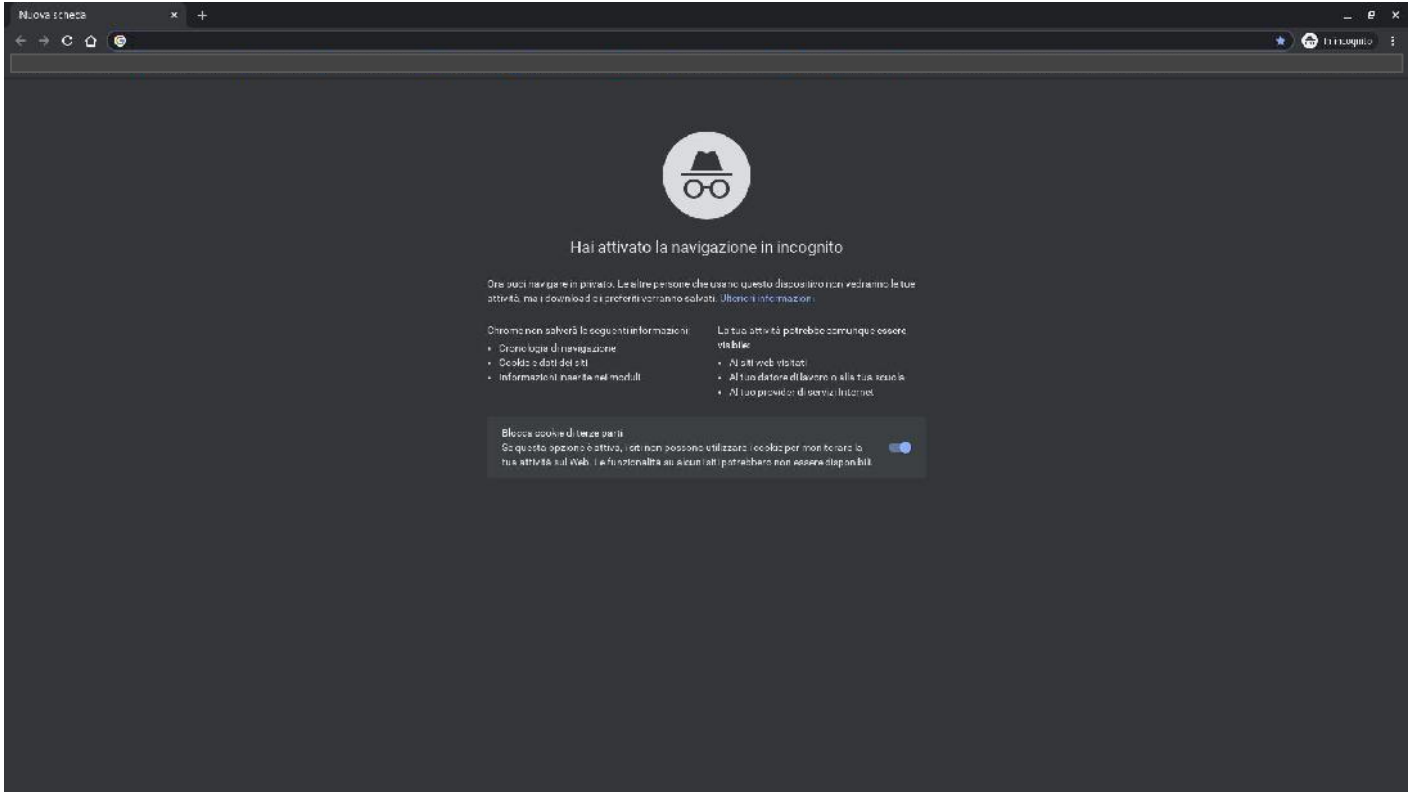
Gentile Cliente,
TIM ti regala un'offerta che nessuno ti da.
Se ricarichi oggi direttamente online ti regaliamo 50 Euro omaggio sulla tua sim card.

Per aderire all'offerta Clicca sul link che segue
Ricarica adesso

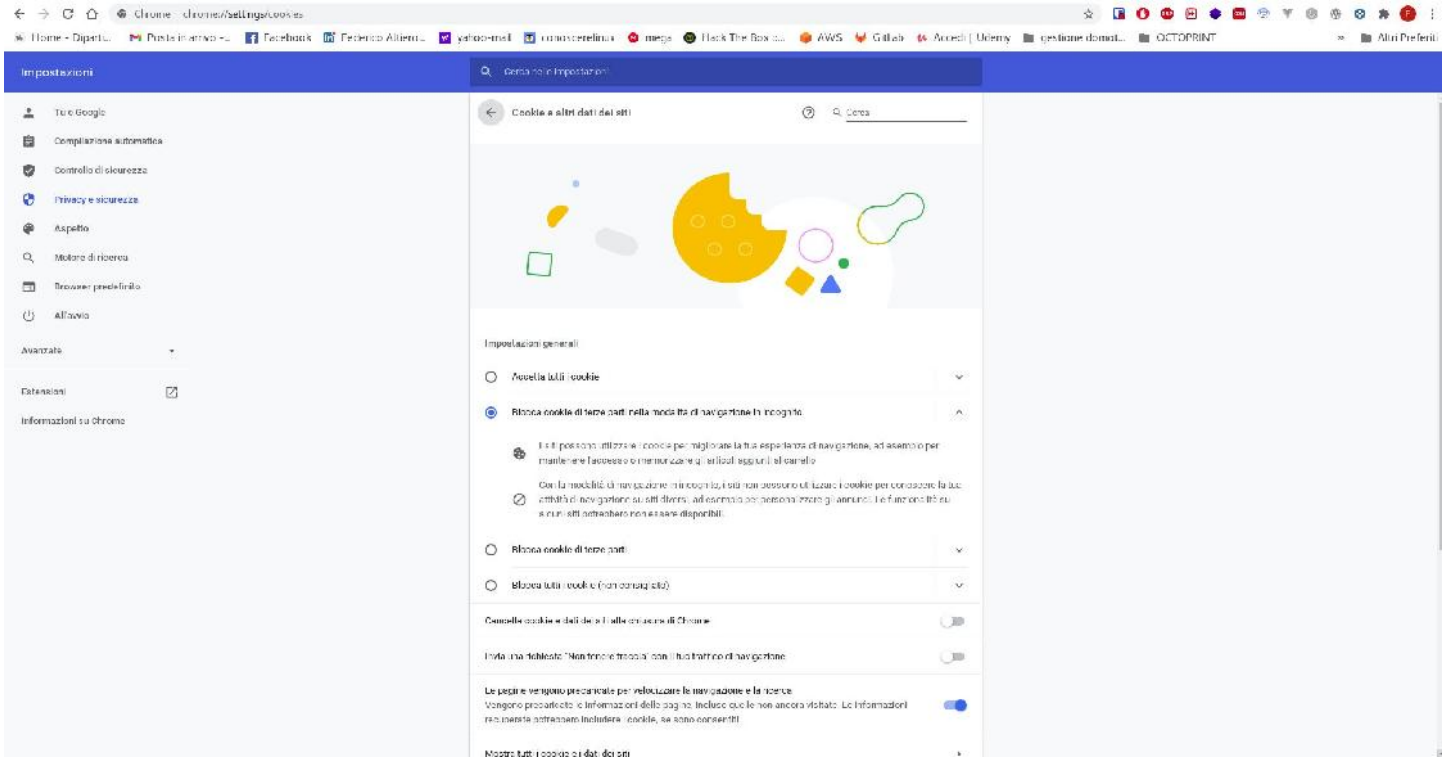
Grazie per aver scelto la Ricarica Online di tim.it.

Servizio Clienti tim.it
Questa email viene inviata automaticamente, ti preghiamo quindi di non rispondere a questo indirizzo.

Navigazione in incognito



Blocco dei Cookies



Utilizzo di VPN

Pc o Smartphone

Connessione via Tunnel sicuro (VPN)

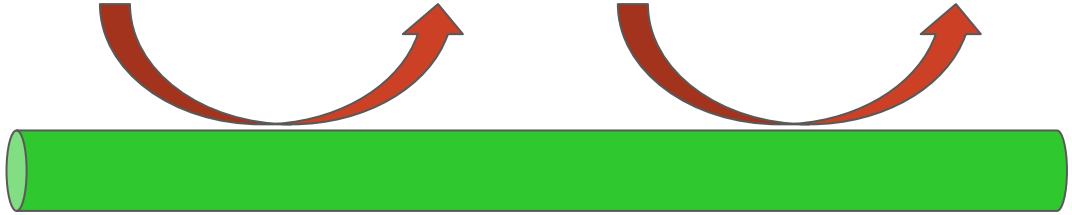
Web

Utilizzo di VPN

Malintenzionato

Internet Provider

Pc o Smartphone



Connessione via Tunnel sicuro (VPN)

Web

Utilizzo di VPN

CyberGhost

MULLVAD VPN

NordVPN®

Surfshark®

ProtonVPN

Sicurezza del telefono

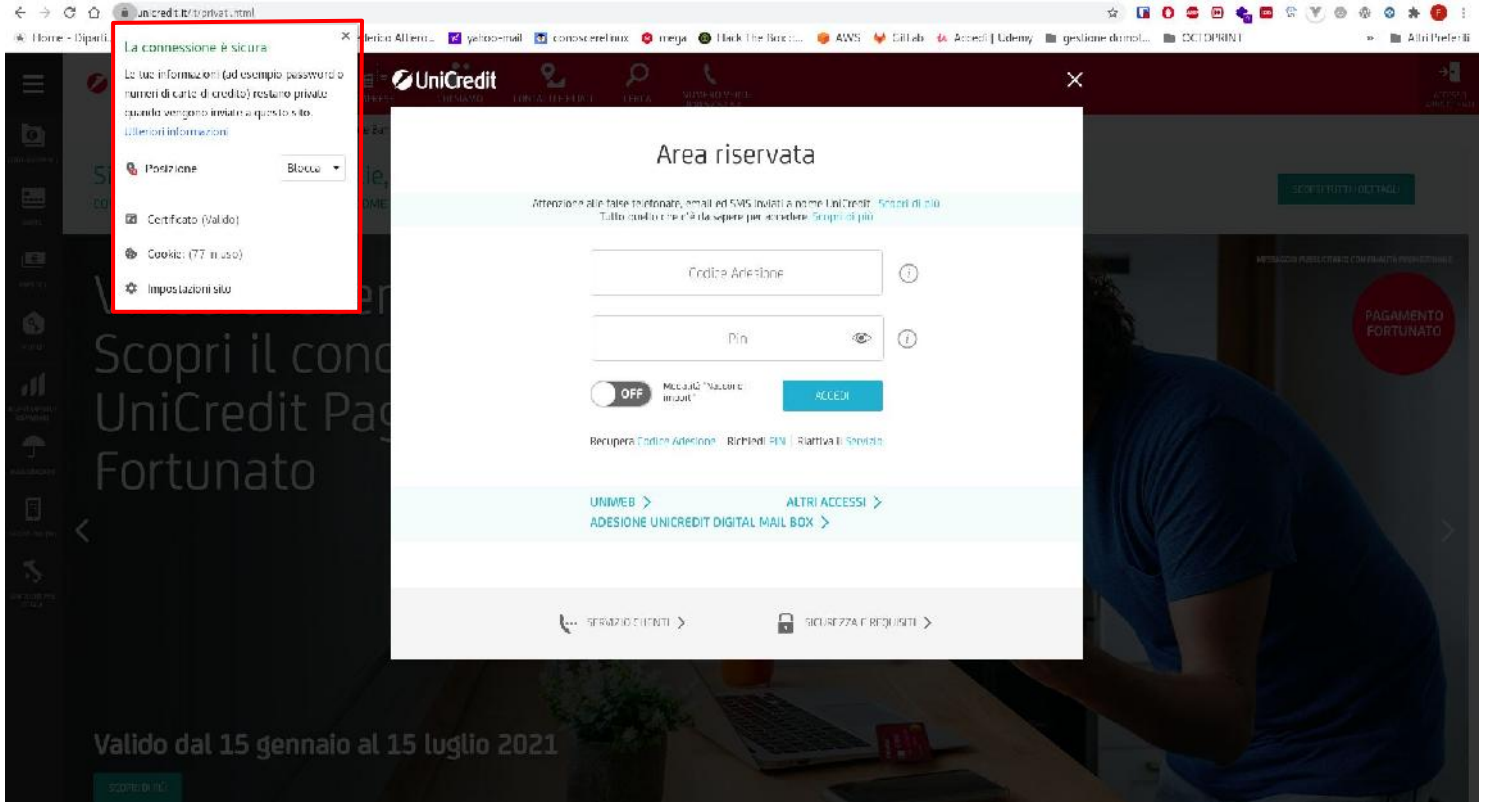
- Non connettere mai il telefono ad un Wifi pubblico o ad un Hotspot per accedere al proprio conto.
- Scaricare un antivirus sul cellulare.
- Abilitare come fattore di autenticazione il rilevamento biometrico

Sicurezza del PC

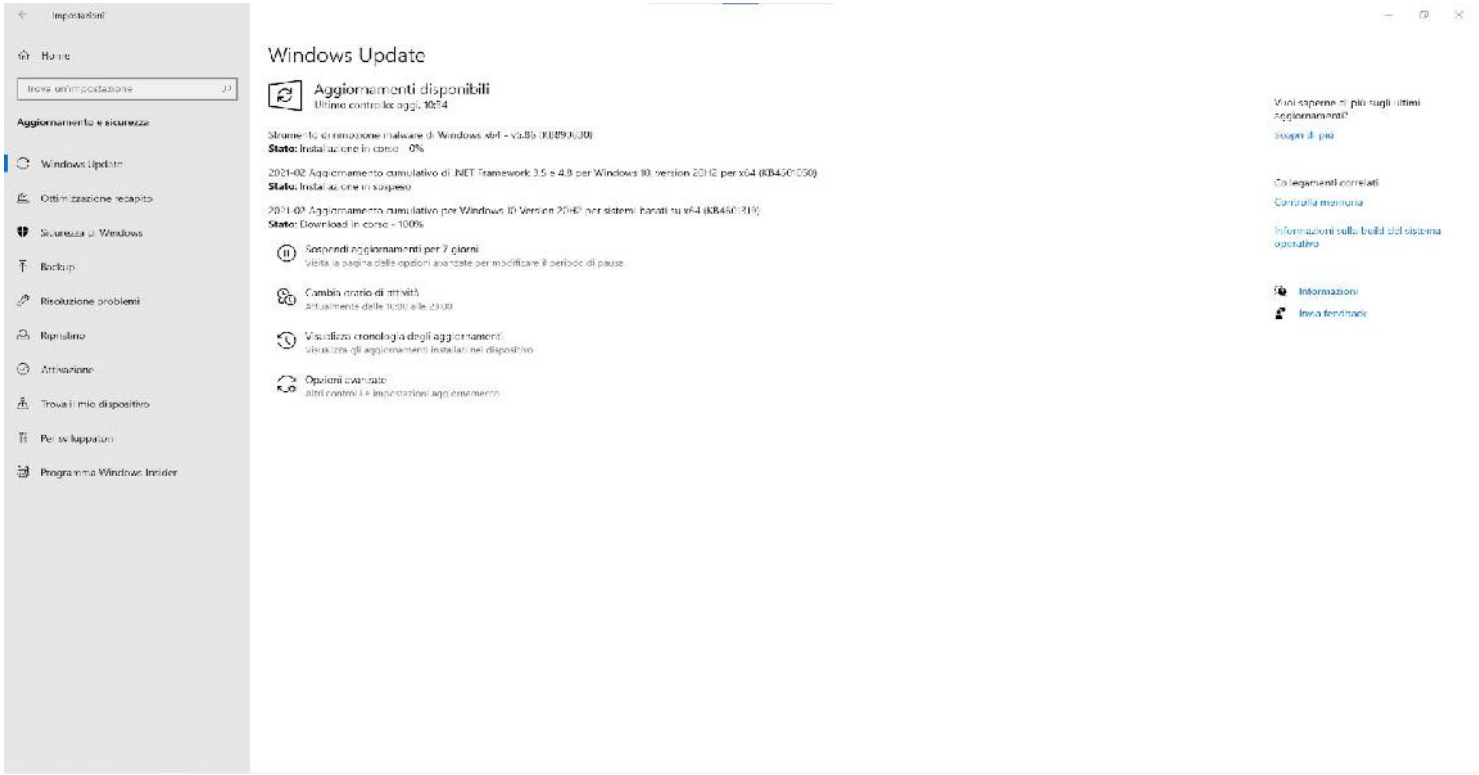
- Se ci connettiamo al conto tramite il PC assicurarsi di aver fatto gli opportuni aggiornamenti, di avere un antivirus attivo e che il sito della banca non sia un sito contraffatto.

- Mai connettersi al proprio conto su PC altrui.

Sicurezza del PC



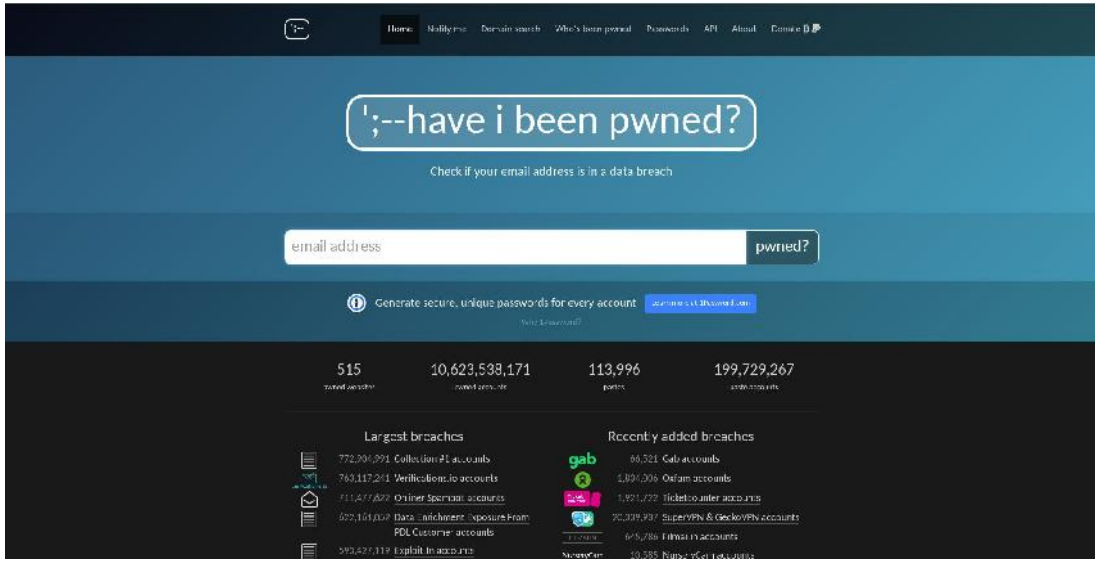
Sicurezza del PC



Il mio account è vulnerabile?

Per scoprire se ci hanno violato un'account possiamo andare su HaveiBeenPwned

https://haveibeenpwned.com/



Paypal

Se si desidera pagare online si consiglia di associare le carte prepagate del proprio conto ad un conto paypal.

PayPal è un’azienda molto grande che gestisce la sicurezza dei pagamenti e la protezione degli utenti attraverso 3 soluzioni di sicurezza avanzate:

- Crittografia del sito e degli acquisti.
- Sistema di Protezione degli acquisti.
- Sistema di Protezione antifrode.

CONTATTI

https://www.associazionemodi.it/

@modiaps

Il Fondo di risarcimento rientra tra le diverse iniziative del Comune di Modena realizzate per la prevenzione dei reati e per l'aiuto alle vittime, anche in collaborazione con le Forze di Polizia nell'ambito di un protocollo d'intesa finalizzato a migliorare i servizi di aiuto alle vittime

FONDO PER IL RISARCIMENTO ALLE VITTIME

(estratto dal regolamento approvato con D.G 676/2020)

Risarcire spese sostenute per:

1) riparazioni di danni materiali arrecati alla propria abitazione, domicilio o residenza (porta ingresso, portafinestra, finestra), e/o a sue pertinenze, a seguito di effrazioni per furto o tentato furto o sostituzioni in caso di danni irreparabili.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 300,00.

2) sostituzione della serratura e rifacimento delle chiavi della propia abitazione, domicilio o residenza, e/o sue pertinenze, qualora a seguito di furto, scippo o borseggio sia avvenuto anche il furto delle chiavi.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 200,00.

3) sostituzione della serratura o del vetro dei finestrini dell'autoveicolo a seguito di furto o tentato furto su autoveicolo e riproduzione delle chiavi dell'autoveicolo a seguito di furto.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 150,00.

4) duplicazione dei seguenti documenti personali rubati carta d'identità, patente di guida, passaporto, permesso/carta di soggiorno.
Risarcimento: 100% delle spese sostenute per il rifacimento della carta d'identità e della patente di guida;
Risarcimento: 70% delle spese sostenute per il rifacimento del permesso/carta di soggiorno e del passaporto.

5) duplicazione di documenti o targhe relativi ad autoveicoli o a ciclomotori, a seguito di furto, intestati alla vittima.
Risarcimento: 100% delle spese amministrative sostenute.

Non è possibile presentare richiesta di risarcimento:
- per spese intestate a soggetto con partita iva;
- per più di una volta consecutiva nello stesso anno solare;
- se si è presentata analoga domanda presso altri enti.

Il risarcimento è **escluso** in caso di risarcimento totale da parte di compagnia assicurativa.
Il risarcimento è **parziale** in caso di risarcimento parziale o franchigia da parte di compagnia assicurativa.

I MODULI DI DOMANDA

Disponibili presso: Sportelli **"Non da Soli"**; Ufficio Legalità e Sicurezze.

Scaricabili dal sito:
www.comune.modena.it/politichedellesicurezze/non-da-soli

LA DOMANDA DI RISARCIMENTO

Deve essere presentate entro 60 giorni dalla data di denuncia del reato.

DOCUMENTAZIONE

- domanda compilata su modulo preposto;
- denuncia di reato ad un organo di Polizia;
- documento di riconoscimento personale;
- ricevute fiscali e/o fatture intestate alla vittima o a familiari e/o conviventi, con relativa quietanza, bonifico o contabile di pagamento, scontrini fiscali con la descrizione dei beni/servizi acquistati;
- polizza assicurativa e relativa quietanza di pagamento della polizza in caso di furto/tentato furto su autoveicolo e di furto, scippo o borseggio di chiavi dell'autoveicolo;
- polizza assicurativa di tipo privato o condominiale in caso di riparazioni di danni materiali arrecati all'abitazione a seguito di effrazioni per furto o tentato furto;
- dichiarazione del tecnico della ditta nel caso di sostituzione completa della porta di ingresso dell'abitazione, o di sue pertinenze, che attesti il caso di danno non riparabile, in alternativa documentazione fotografica;
- in caso di risarcimento assicurativo: attestazione dell'assicurazione con dettaglio dei beni soggetti a risarcimento.

MODALITÀ DI PRESENTAZIONE

- via PEC o mail Ufficio Legalità e Sicurezze **modenasicura@cert.comune.modena.it**
- via mail Sportelli Non da Soli
- via fax Ufficio Legalità e Sicurezze al nr. 059 2032109
- di persona previo appuntamento presso Ufficio Legalità e Sicurezze

ULTERIORI INFORMAZIONI E REGOLAMENTO

Disponibili presso l'Ufficio Legalità e Sicurezze, il Posto Integrato di Polizia, gli sportelli del servizio **"Non da Soli"**, l'Urp di Piazza Grande e sul sito:
www.comune.modena.it/politichedellesicurezze/non-da-soli

GLI SPORTELLI NON DA SOLI

S. Faustino, Madonnina
via Leonardo da Vinci, 158 - 41126 Modena
nondasoli.sfaustino@comune.modena.it

Buon Pastore, S. Agnese
via Panni, 202 - 41125 Modena
anzianibuonpastore@libero.it

Crocetta, San Lazzaro, Modena Est
P.zza Liberazione,13 - 41122 Modena
nondasoli.modenaest@comune.modena.it

Informazioni:
Ufficio Legalità e Sicurezze
via Scudari, 20 - 41121 Modena
☎ 059 2032502 - 2032963
fax 059 2032109

www.comune.modena.it/politichedellesicurezze/non-da-soli
mosicura@comune.modena.it
PEC modenasicura@cert.comune.modena.it

In collaborazione con:

Prefettura di Modena

Questura di Modena

Arma dei Carabinieri

Guardia di Finanza

Comitato Cittadini Modena Est
Centro Sociale Anziani e Orti Buon Pastore
Centro Sociale Anziani e Orti S. Faustino

Aggiornato dicembre 2020

Comune di Modena
Polizia Locale
CITTÀ SICURA

- **Non teniamo denaro o oggetti preziosi** in cassetti o armadi a portata di mano.
- **Durante gli interventi manutentivi** (idraulico, elettricista,...) **facciamo in modo che una persona di fiducia rimanga in casa con noi.**
- **Non buttiamo nella spazzatura le fatture delle utenze (bollette).**
- **Se utilizziamo internet**, diffidiamo di chiunque chieda i nostri dati e credenziali personali (ad es. per sbloccare carte, bancomat, per verificare se il nostro conto corrente sia stato impropriamente utilizzato, ecc.)
  Non comunichiamo mai i nostri dati bancari.
  Non rispondiamo a e-mail o telefonate contenenti indicazioni Coronavirus.
  Per le notizie e le informazioni sul Coronavirus facciamo solo ed esclusivamente riferimento alle fonti istituzionali facendo riferimento ai siti ufficiali (Ministero della Salute, Istituto Superiore della Sanità, Commissariato di Polizia di Stato, Protezione Civile, Croce Rossa). Evitiamo di diffondere informazioni e notizie tramite messaggi di testo o audio provenienti da fonti diverse.

Se ci sentiamo minacciati o vittime di un reato, telefoniamo al numero unico 112 (Polizia di Stato e Arma dei Carabinieri) o al pronto intervento della Polizia Locale 059 20314

Iniziativa a cura del Ufficio Legalità e sicurezze realizzata nell'ambito del progetto "La prevenzione rende sicuri: azioni integrate per il contrasto di truffe e raggiri ai danni della popolazione anziana" finanziato dal Fondo Unico di Giustizia del Ministero degli Interni, con la collaborazione di:

- Sportelli di aiuto alle Vittime di Reato "Non da Soli"
- Sportello S.O.S. Truffa & C.
- Associazioni dei Consumatori

Comune di Modena
Ufficio Legalità e Sicurezze
Via Scudari, 20 - Modena
tel. 059 2032502-2032963
fax 059 2032109
mosicura@comune.modena.it
www.comune.modena.it/politichedellesicurezze

LA PREVENZIONE RENDE SICURI

CAMPAGNA per la SICUREZZA delle PERSONE ANZIANE

Consigli utili per difendersi dai malintenzionati

Comune di Modena

Polizia Locale

In banca, in posta, nei negozi, al mercato

- **Facciamo accreditare la pensione** sul conto corrente o sul libretto di risparmio e paghiamo le utenze tramite addebito sul conto corrente (domiciliazione utenze).
- **Non rechiamoci in banca o in posta** in orari di punta; se possibile, chiediamo ad un parente o conoscente di di accompagnarci.
- **Quando utilizziamo il bancomat:** accertiamoci che nessuno possa vedere il codice pin. Preleviamo l'importo minimo necessario e riponiamo immediatamente la somma.
- **Non teniamo il codice pin in evidenza.**
- **Non distraiamoci** mentre paghiamo o maneggiamo il denaro.
- **Non parliamo di operazioni di deposito o prelievo,** soprattutto se nelle vicinanze ci sono sconosciuti che ci ascoltano.
- **Non lasciamoci avvicinare da estranei** quando usciamo dalla banca o dalla posta, anche se si presentano come persone dipendenti e con una scusa chiedono di controllare il nostro denaro.
- **Quando facciamo la spesa** non lasciamo mai borse o borselli incustoditi sul carrello. Dopo aver fatto la spesa, mentre carichiamo le buste sull'auto, non lasciamo la borsa incustodita sui sedili. **Chiudiamo a chiave l'auto** quando andiamo a riporre il carrello.

In autobus, bicicletta o in automobile

- **Sull'autobus**, non ci lasciamo avvicinare da sconosciuti. Qualche malintenzionato potrebbe sfilarci il portafoglio da le tasche posteriori o dalla borsa. Teniamo la borsa a tracolla e lo zaino davanti.
- **In bicicletta,** non mettiamo mai la borsa sul manubrio, nel cestino o nei portapacchi, ma indossiamola a tracolla.
- **Chiudiamo sempre a chiave l'auto**, anche se ci allontaniamo per pochi istanti, e non lasciamo mai all'interno oggetti che possono attirare l'attenzione come borse, giacche, oggetti di valore.
- **Facciamo attenzione a chi si rende disponibile** a darci una mano per aiutarci (gomma bucata) o ci contesta un danno subito (specchietto rotto, danno alla carrozzeria), nel dubbio chiamiamo le Forze di Polizia.
- Portiamo con noi **solo il denaro indispensabile.**

Quando camminiamo per strada

- Sui marciapiedi, **teniamo la borsa o il borsello a tracolla e dal lato interno,** camminando vicino al muro per scoraggiare eventuali malintenzionati.
- **Evitiamo la folla** perché i borseggiatori possono approfittare del contatto fisico per derubarci.
- **Non ascoltiamo** chi ci avvicina chiedendoci di pagare un debito contratto da un parente (figlio, nipote) e non consegniamo per nessun motivo denaro: chiamiamo immediatamente **il numero di emergenza 112** e chiediamo aiuto ai passanti.
- **Se abbiamo il sospetto** di essere seguiti entriamo nel negozio più vicino.
- **Non accettiamo** di vedere cataloghi di articoli vari.
- **Non firmiamo** mai nulla.
- **Non comunichiamo** i nostri dati personali.

Quando siamo a casa

- **Se una persona sconosciuta** vuole salire in ascensore con noi, diciamo che aspettiamo una persona e ci accertiamo della motivazione della sua presenza.
- **Non lasciamo i bambini** liberi di aprire la porta.
- **Quando rientriamo** a casa stiamo attenti che nessuno ci segua, chiudiamo la porta e non lasciamo la chiave nella serratura. Inseriamo il chiavistello se la nostra porta ne è fornita.
- **Non apriamo agli sconosciuti.** Gli operatori di acqua, luce, gas, telefonia o degli Enti pubblici sono riconoscibili da un tesserino ben visibile e preannunciano il loro arrivo. Non siamo obbligati ad aprire. I consumi possono essere comunicati successivamente con l'aiuto di un parente o amico.
  Non apriamo a chi vuole venderci vaccini o farmaci specifici per prevenire o curare il coronavirus in quanto non sono ancora in commercio e non vengono distribuiti a casa senza preavviso.
- **Se non siamo sicuri della loro identità,** non apriamo neppure a chi si presenta in divisa delle Forze di Polizia. **Nel dubbio contattiamo il numero di emergenza 112.**
  Allo stesso modo non apriamo a chi si presenta come infermiere, incaricato di ASL o di Pubblica Amministrazione per somministrare il tampone per il Coronavirus se non siamo stati in ma preavvisati.
- **Non facciamo entrare in casa persone** che dicono di essere state mandate dall'amministratore di condominio, dal vicino, da un parente, dalla banca o che dicono di dovere entrare per risolvere problemi vari (perdita d'acqua, controllo banconote ecc.).
- **Non apriamo a chi si presenta per eseguire** disinfestazioni da coronavirus delle abitazioni o dei condomini.

→