Sicurezza online

Consigli e strumenti per proteggere i tuoi dati

BANCA EUROMOBILIARE

Private banking dal 1973

GUIDA OPERATIVA

Sicurezza online

Consigli e strumenti per proteggere i tuoi dati

LA TUA SICUREZZA PER NOI È IMPORTANTE

Benvenuto nell'area dedicata alla sicurezza online, qui troverai tanti consigli utili per imparare a proteggere i tuoi dati e conoscere tutti gli strumenti adottati da Banca Euromobiliare per garantirti la massima sicurezza quando usi i Servizi Online e le tue carte di credito.

1. SEGNALA UNA FRODE

TEMI DI AVER SUBITO UNA FRODE ONLINE?

- **Cambia la password di accesso**

Per metterti al riparo da eventuali truffe.
Se hai il sospetto che ti abbiano rubato le credenziali, cambia subito la password del tuo Internet Banking. È una precauzione semplice ma importante, che può metterti al riparo da utilizzi fraudolenti, prima del nostro intervento.

- **Chiama il numero verde: 800 45 00 45**

Segnalaci subito quello che ti successo.
Il servizio con operatore è attivo dal lunedì al venerdì dalle 8:30 alle 21:00. Ti ricordiamo che se sei all'estero dovrai chiamare al numero +39 0522 583585. In alternativa puoi sempre fare affidamento al tuo consulente o alla filiale.

- **Scrivi una e-mail**

Se hai un dubbio e vuoi semplice chiarimento. Puoi scrivere all'indirizzo helpdesk@bancaeuro.it.

Phishing - Come evitare le truffe online

Oggi i criminali informatici, per impossessarsi dei tuoi dati, utilizzano tecniche sempre più sofisticate per poterti trarre in inganno. Come? Via e-mail, SMS, telefono, Internet e social network.
Saper riconoscere i tentativi di frode online è fondamentale per potersi tutelare. In questa pagina trovi utili informazioni per imparare a difendersi.

CHE COS'È?

Il Phishing è un tipo di truffa online attraverso la quale un soggetto cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili (codice fiscale, cellulare ecc) e altri dati riservarti, ad esempio codici di accesso a Servizi online della banca, numero della carta di credito password dispositive ecc, con l'obiettivo di mettere in atto vere proprie frodi.

COME RICONOSCERLO?

Gli attacchi di phishing possono avvenire tramite e-mail, SMS, telefonate, siti internet e social network. Si possono riconoscere perché fanno uso di toni intimidatori con carattere di urgenza, non sono personalizzati, presentano spesso errori di italiano e soprattutto ti invitano con qualche pretesto a cliccare su un link o a scaricare allegati.

COME DIFENDERSI?

Sapevi che quello che ti viene proposto non è sempre vero? Possono sembrare messaggi simili a quelli di Banca Euromobiliare ma, in alcuni casi, sono dei falsi! **Identificare i principali tentativi di phishing è il primo step per difendere i tuoi risparmi.**
Ad esempio diffida da:

- Un'e-mail con un mittente diverso da quelli ufficiali: info@bancaeuro.it, helpdesk@bancaeuro.it.
- Un sms che richiede di cliccare su un link per sbloccare o verificare il tuo conto, oppure che ti invita a chiamare numeri di telefono diversi da quelli Banca Euromobiliare per verificare movimenti sospetti sul tuo conto.
- Una telefonata da un presunto Servizio Clienti che ti chiede codici OTP del tuo My Key.
- Un post social che promette ricompense in premi o denaro in cambio di dati personali.

La Banca non ti chiederà mai di fornire dati personali, codici generati dal tuo My Key, credenziali di accesso, il PIN della carta, tramite email, SMS, telefono e social network. Diffida sempre se ricevi questa richiesta.

COSA È NECESSARIO FARE?

- Se ricevi una telefonata che ti sembra strana dal nostro Servizio Clienti, non esitare a chiedere all'operatore che ti sta chiamando ulteriori informazioni, come nome e cognome e verificali al nostro Numero Verde 800.45.00.45. Ma soprattutto **non fornire mai i tuoi dati personali.**
- Se ricevi un'e-mail o un SMS che ha le caratteristiche degli esempi sopra citati, **non cliccare sui link al loro interno e non inserire mai i tuoi dati.**
- Prima di aprire un link, passaci sopra con il cursore del mouse e **verifica che sia effettivamente collegato a una pagina verosimile.** Se usi lo smartphone, toccalo e tieni premuto (senza togliere il dito) in modo da visualizzare il link completo. Se hai un dubbio o vuoi un chiarimento, inoltra l' e-mail o l'SMS all'indirizzo helpdesk@bancaeuro.it, il nostro Servizio Clienti è pronto a forniti un supporto.
- **L' area riservata dell'Internet Banking è raggiungibile solo da www.bancaeuro.it.** Non è possibile in alcun modo accedere al tuo Internet Banking tramite e-mail, SMS o social network. Quando entri nella tua home page **verifica sempre in alto che la data e l'ora dell'ultimo accesso corrispondano a quelli da te effettuati.**

Cos'è la truffa SIM SWAP?

Fai attenzione se la SIM del tuo smarphone non funziona.
Ecco cosa potrebbe capitare dopo aver subito un attacco di Phishing. Una delle tecniche più recenti di frode è lo SIM SWAP! Come funziona? Dopo che i criminali si sono impossessati delle credenziali di accesso dei tuoi Servizi Online e del tuo numero di cellulare, copiano la Sim del tuo telefono su una nuova scheda Sim controllata da loro.

I segnali più comuni per riconoscerla:
- Il tuo telefono, smette di funzionare, ovvero perde inaspettatamente il segnale e non ti è più possibile inviare/ricevere SMS o fare chiamate.
- Ti potrebbe chiamare un presunto operatore telefonico che ti informa che ci potrebbero essere dei problemi di linea sul tuo smartphone ma di non farci caso. Oppure potresti ricevere un SMS con lo stessa informazione. Non fidarti!
- Potresti ricevere molte chiamate fastidiose che ti spingono a spegnere il telefono per non essere disturbato. Non farlo!

Cosa fare se pensi di essere stato vittima di SIM SWAP:
- Controlla subito il tuo conto.
- Contatta immediatamente il Servizio Clienti al Numero Verde 800.45.00.45 per bloccarne temporaneamente l'operatività.
- Contatta subito il tuo gestore telefonico per informarlo della truffa e bloccare lo scambio della Sim.

2. BLOCCA LA TUA CARTA

HAI SMARRITO O TI HANNO RUBATO LE CARTE DI CREDITO O DEBITO?

Chiama subito il Numero Verde relativo alla tua carta e richiedi subito il blocco. Il servizio è attivo 24 ore su 24 365 giorni all'anno.

- **Se chiami dall'Italia**

CARTA DI DEBITO	800 822 056
CARTA DI CREDITO EGO	800 258 852
NEXI	800 15 15 16
AMERICAN EXPRESS	800 872 000

- **Se chiami dall'estero**

CARTA DI DEBITO	+39 02 608 437 68
CARTA DI CREDITO EGO	+39 0522 583 583
NEXI	+39 02 349 800 20 *
AMERICAN EXPRESS	+39 06 729 003 47

** Numero verde dagli USA +1 800 473 6896*

IMPORTANTE:
Consegna alla tua filiale, entro 10 giorni dal blocco della carta, copia della denuncia che hai presentato alle autorità e che deve contenere l'elenco delle transazioni fraudolente. In caso di impossibilità a recarti in filiale, puoi inviare la denuncia tramite lettera raccomandata.

COME TI SUPPORTIAMO?

3. REGOLE PER UNA NAVIGAZIONE SICURA

La sicurezza, soprattutto online, è un argomento importante. **Con pochi e semplici accorgimenti puoi proteggere i tuoi dati personali e i tuoi dispositivi.** Segui i nostri consigli per imparare a proteggersi.

PROTEGGI I TUOI DEVICE

- **Tieni aggiornato il sistema operativo e il programma antivirus.** È il modo migliore per minimizzare il rischio che un virus alteri il normale funzionamento del tuo smartphone o PC. Puoi farlo in maniera automatica, attraverso le impostazioni dei tuoi device.
- **Scarica solo file attendibili e App ufficiali.** Presta sempre attenzione quando scarichi un file che la fonte (sito e App) sia attendibile. Non fidarti di pop up, messaggi pubblicitari che ti invitano a scaricare file, ecc. Il rischio è che particolari software, denominati Spyware, possano accedere con facilità alle tue informazioni personali.
- **Scegli provider e-mail con filtri antispam, malware e phishing.** Quando crei una casella di posta elettronica affidati a provider sicuri e cerficati. Alcuni di essi ti avvisano immediatamente se c'è qualcosa di sospetto e ti garantiscono una sicurezza in più con l'autenticazione a due fattori.

PROTEGGI IL TUO ACCOUNT

- **Tieni sempre aggiornati e-mail e cellulare.** Tenere il tuo profilo personale sempre aggiornato è una modo semplice ma importante per tutelare il tuo account. Perché? Ci permette di contattarti tempestivamente, in caso di necessità.
- **Controlla sempre l'indirizzo su cui navighi.** Quando usi i motori di ricerca prima inserire i tuoi dati, controlla sempre l'autenticità del sito. Non fidarti di link contenuti in e-mail o SMS o banner pubblicitari che non conosci.
- **Evita il salvataggio automatico delle password.** Disabilita il salvataggio automatico direttamente dall'impostazione del browser che utilizzi per la navigazione, soprattutto se si tratta dei tuoi account finanziari.
- **Usa una connessione sicura.** Per collegarti ai servizi online della banca, utilizza sempre la tua rete Wi-Fi privata o il traffico dati del tuo cellulare, non usare un rete Wi-Fi pubblica e evita di farlo in pubblico. Possibili criminali potrebbero intercettare i tuoi codici di accesso e i tuoi dati personali senza che te ne accorga. Puoi impostare il riconoscimento biometrico all'accesso sull'App BE Mobile.
- **Usa i Social Network in modo consapevole.** Limita le informazioni personali sui tuoi social. I criminali li utilizzano come canale per riuscire a recuperare dati utili sulle loro potenziali vittime.
- **Fai sempre log out.** Dopo che ti sei autenticato ad un sito, una volta terminata la navigazione, ti consigliamo di uscire utilizzando sempre l'apposito tasto "ESCI" o "LOGOUT". È una misura che ti invitamo a fare in particolare quando devi uscire dai Servizi Online.

4. REGOLE PER UNA PASSWORD SICURA

Utilizzare online una password sicura è la prima misura da adottare per proteggerti dalle frodi online. Ma come si crea una password veramente sicura? Segui questi semplici consigli.

PROTEGGI LA TUA PRIVACY INIZIANDO DALLA PASSWORD

Le password che usi online sono come le chiavi di casa tua, è importante quindi avere i giusti accorgimenti per rendere i tuoi accessi a prova di intruso!

- **Crea un password lunga**

Più lunga è una password, più risulta difficile da decifrare. Ti consigliamo una lunghezza di almeno 8 caratteri.

- **Mescola lettere, numeri e caratteri speciali "! ... @ ^ _ ~"**

Quando crei una password **alterna tra loro lettere MAIUSCOLE, minuscole, numeri e caratteri speciali.** Questa combinazione consente di ridurre le probabilità che un criminale possa decifrare una password. Hai paura di non ricordarti la sequenza? Ecco un consiglio! Pensa ad una parola testuale e poi sostituisci alcune lettere con le cifre corrispondenti alla tastiera del telefono e poi aggiungi un carattere speciale (dove vuoi) come l'asterisco.

- **Evita nomi comuni, personali o date importanti**

Non utilizzare parole che siano riconducibili ad informazioni personali che si possono reperire facilmente online e sopratutto sui Social Network. Come ad esempio il nome del proprio cane, data di nascita, cantante preferito ecc.

- **Evita il salvataggio automatico del browser**

Anche se sappiamo che è comodo, **impostare il salvataggio delle password sul broswer potrebbe non essere sicuro.** Ti consigliamo non attivarlo mai, in particolare se si tratta dei Servizi Online della banca. Per disattivarlo entra direttamente nelle impostazioni del browser che utilizzi per la navigazione.

- **Non utilizzare la stessa password per tutto**

Usare la stessa password per accedere a diversi siti è una modalità purtroppo molto diffusa. Ma è la scelta meno sicura che si possa fare! Non utilizzare mai la stessa password per tutto: servizi online della banca, posta elettronica, siti di e-commerce, social network. **Usa una password unica per ogni account, e cambiale spesso!**

ECCO UN ESEMPIO PER UNA PASSWORD SICURA:

TiPr0t3ggiam0N0i* → **SICURA**
password2020 → NON SICURA

NOI TI PROTEGGIAMO

5. LE NOSTRE REGOLE PER LA TUA SICUREZZA

Adottiamo le misure necessarie per proteggere la sicurezza dei tuoi dati, delle tue operazioni online e dei tuoi pagamenti con carta di credito. In questa sezione troverai tutti gli approfondimenti su come ti proteggiamo.

LA TUA NAVIGAZIONE IN SICUREZZA

Quando utilizzi il nostro sito e le nostre App, proteggiamo la tua navigazione e le tue informazioni. Adottiamo tutte le misure necessarie e le tecnologie più avanzate per la tua sicurezza.

COME PROTEGGIAMO I TUOI DATI

- **Utilizzo dei codici di accesso**

Per entrare nei servizi online devi usare il codice utente e la password, che ti viene consegnata in busta sigillata dalla tua filiale. Per rendere ancora più sicuro l'accesso puoi aggiungere al codice utente e password anche una seconda password erogata dal tuo My Key. Se utilizzi l'App Be Mobile invece, hai la possibilità di impostare la biometria all'accesso per garantire una sicurezza a 360° dei tuoi codici personali.

- **Notifica automatica ad ogni accesso**

Ad ogni accesso, ricevi un' e-mail che ti avvisa in tempo reale dell'accesso. Puoi scegliere anche di riceverla via sms o notifica push sul tuo smartphone.

- **Data e ora dell'ultimo accesso**

Ogni volta che effettui l'accesso alla area riservata, vengono visualizzate la data e l'ora dell'ultimo collegamento. Grazie a questa informazione si può avere il pieno controllo di tutti accessi effettuati e riconoscere quelli non effettuati da te.

- **Chiusura sessione dopo 5 minuti di inattività**

In caso di inattività del tuo Internet Banking, la sessione si chiuderà in automatico dopo 5 minuti. È una misura precauzione in caso dovessi dimenticarti di chiuderla correttamente o lasciassi il PC aperto.

COME PROTEGGIAMO LA TUA CONNESSIONE

- **Protocolli di sicurezza e crittografia**

I dati che inserisci all'interno del nostro sito vengono protetti e crittografati. Utilizziamo infatti **protocolli di sicurezza TLS e collegamento SSL in base ai più moderni standard per la crittografia delle informazioni** che transitano sulla rete Internet. Anche le connessioni che utilizziamo sono protette dai più avanzati sistemi di firewall, di protezione da virus e software potenzialmente dannosi.

COME PROTEGGIAMO LE TUE OPERAZIONI

- **Presidio costante**

Oltre ad usare appositi software di sicurezza, **grazie ad un team dedicato effettuiamo costanti controlli sulla correttezza e veridicità delle operazioni online**, in modo da contattarti immediatamente se dovessimo riscontrare un movimento o qualcosa di sospetto.

- **Notifica automatica per i pagamenti**

Ad ogni bonifico ricevi una email di avviso. È una misura semplice, che ti consente di avere un controllo in tempo reale sul tuo conto. Puoi scegliere di impostare questo servizio anche per altre tipologie di pagamento e scegliere se ricevere gli avvisi via e-mail, SMS o notifica push.

- **My Key APP e Biometria**

Per confermare le operazioni è obbligatorio utilizzare My Key App. Come funziona? Si tratta di un' app da scaricare sul proprio smartphone che dialoga con il tuo Internet e Mobile Banking ed associa in modo puntuale l'operazione che stai effettuando (tipologia, importo e beneficiario) ad una notifica di conferma. Per aumentare il livello di sicurezza puoi impostare le conferma attraverso il riconoscimento biometrico (impronta digitale e riconoscimento facciale).