FEDERAZIONE AUTONOMA BANCARI ITALIANI

COMUNICATO STAMPA

BANCHE: FABI, UNA GUIDA IN 10 CONSIGLI PER L'ESTATE SU HOME BANKING, E-COMMERCE E PAGAMENTI DIGITALI

Roma, 17 maggio 2024. Home banking, e-commerce, prestiti online e *buy now pay later*, utilizzo di piattaforme di pagamento virtuale. In vista dell'estate, quando per le vacanze e per i viaggi, a cominciare dalla preparazione e dall'organizzazione, cresce l'utilizzo di sistemi digitali, sia per saldare i conti sia per le prenotazioni, la Fabi (Federazione autonoma bancari italiani) ha predisposto una guida in 10 consigli destinata a tutte le famiglie italiane, alle ragazze e ai ragazzi, ma anche a chi è meno giovane e ormai da tempo usa dispositivi elettronici (*smartphone*, *tablet* e pc) per fare pagamenti o per accedere in banca. La guida si propone di educare tutti gli utenti su come navigare in sicurezza nel mondo digitale, fornendo suggerimenti pratici e facilmente applicabili. Per l'*home banking*, la guida raccomanda di utilizzare connessioni internet private e di verificare che l'indirizzo del sito della banca inizi con "https://" per garantire una connessione sicura. Viene sottolineata l'importanza di password robuste e l'utilizzo dell'autenticazione a due fattori per proteggere l'accesso ai servizi *online*. Si suggerisce di non cliccare mai su *link* o allegati di provenienza dubbia e di controllare sempre l'autenticità dei messaggi direttamente con la banca, per evitare di incappare in tentativi di phishing. Si consiglia di controllare regolarmente i movimenti bancari e di impostare notifiche per ogni transazione effettuata. Quanto all'e-commerce, vengono date indicazioni per verificare l'affidabilità dei venditori online e utilizzare metodi di pagamento sicuri che offrono protezioni aggiuntive. Sul fronte dei pagamenti digitali, la guida invita a proteggere i dispositivi con misure di sicurezza adeguate e a essere cauti nella gestione delle credenziali di pagamento. Si raccomanda, nell'ambito dei prestiti online o del *buy now pay later*, prima di accettare finanziamenti o servizi di pagamento dilazionato, verifica la credibilità e la legittimità dei fornitori; inoltre occorre, leggere attentamente i termini e condizioni per comprendere gli interessi, le commissioni e le conseguenze di un mancato pagamento. Attenzione al proprio dispositivo: l'installazione e l'aggiornamento regolare di *software* antivirus sono essenziali per la sicurezza di telefoni, smartphone, tablet e pc usati per operazioni finanziarie. Non a caso, mantenere aggiornati sistema operativo e applicazioni è cruciale per proteggersi da vulnerabilità di sicurezza. La Fabi incoraggia l'informazione continua su truffe e frodi attraverso risorse e informazione dedicate alla sicurezza *online*: l'educazione finanziaria è fondamentale e il materiale che la Fabi realizza dal 2018, destinato in particolare alle scuole di ogni ordine e grado, partecipando alle campagne del Ministero dell'Economia e dell'Ocse, è disponibile su edufin.fabi.it. «La sicurezza online inizia da noi stessi. Seguire buoni consigli, come i nostri, può ridurre notevolmente il rischio di ritrovarsi vittima di frodi e truffe online. Le lavoratrici e i lavoratori bancari sono a disposizione quotidianamente di tutta la clientela delle banche per dare consigli utili e soprattutto per aiutare chi, purtroppo, subisce frodi o truffe. Qualsiasi sospetto va immediatamente comunicato in banca e alle autorità competenti» commenta il segretario generale della Fabi, Lando Maria Sileoni.

FABI Ufficio Stampa
Email stampa@fabi.it
Telefono 06.8415751
Mobile 331.4386554 / 348.2385090 / 328.1576095

BANCHE, PAGAMENTI, PRESTITI E ACQUISTI ONLINE: ECCO I 10 CONSIGLI DELLA FABI

1. Home banking in sicurezza. Utilizza sempre una connessione internet privata quando accedi al tuo conto bancario *online*. Evita le reti Wi-Fi pubbliche, come quelle in caffè o aeroporti, che possono essere meno sicure. Assicurati che l'indirizzo del sito web della tua banca inizi con "https://" e che ci sia un simbolo di lucchetto nella barra degli indirizzi che indica una connessione protetta.

2. Password robuste e autenticazione a due fattori. Per l'*home banking* e altri servizi *online*, scegli *password* complesse che combinano lettere maiuscole e minuscole, numeri e simboli. Non usare la stessa password per più account. Attiva, ove possibile, l'autenticazione a due fattori (2FA), che richiede un secondo passaggio di verifica per accedere al tuo account, come un codice inviato al tuo telefono e via e-mail.

3. Attenzione ai phishing e alle e-mail sospette. Non cliccare mai su link o allegati provenienti da e-mail sospette che sembrano provenire dalla tua banca o da altri servizi fiduciari. Le banche non chiedono mai dati personali, come password o PIN, via e-mail. Verifica sempre l'autenticità dei messaggi contattando direttamente la banca attraverso i canali ufficiali.

4. Monitoraggio delle transazioni. Controlla regolarmente i movimenti del tuo conto bancario e le transazioni sulle tue carte di credito. Imposta notifiche via SMS o e-mail per essere informato di ogni operazione. In caso di movimenti non autorizzati, contatta immediatamente la tua banca.

5. Acquisti sicuri nell'e-commerce. Quando fai acquisti online, verifica l'affidabilità del venditore e leggi le recensioni degli altri utenti. Utilizza metodi di pagamento sicuri come carte di credito o servizi di pagamento protetti che offrono meccanismi di contestazione e rimborso. Evita i bonifici bancari diretti, specialmente con venditori sconosciuti.

6. Uso cautelativo dei sistemi di pagamento digitale. Quando usi sistemi di pagamento digitale come PayPal, Google Pay, Satispay o Apple Pay, assicurati di proteggere i tuoi dispositivi con *password* o impronta digitale. Non memorizzare mai le tue credenziali di accesso sui dispositivi e non condividere queste informazioni.

7. Prestiti online prudenti e occhio al *buy now pay later*. Prima di accettare un prestito online o optare per un'opzione di pagamento differito, controlla attentamente la legittimità del fornitore e leggi i termini e condizioni. Fai attenzione a tassi di interesse, commissioni nascoste e le penalità in caso di mancato pagamento.

8. Protezione del dispositivo. Installa un software antivirus affidabile su tutti i dispositivi che utilizzi per accedere a servizi finanziari *online* e tienilo aggiornato. Esegui regolarmente scansioni alla ricerca di *malware* e non installare *software* da fonti non verificate.

9. Aggiornamenti del software. Mantieni sempre aggiornati il sistema operativo e le applicazioni sui tuoi dispositivi. Gli aggiornamenti spesso includono correzioni per vulnerabilità di sicurezza che potrebbero essere sfruttate da malintenzionati.

10. Educazione finanziaria continua. Rimani informato sulle ultime truffe e frodi *online* leggendo la stampa specializzata, partecipando a eventi pubblici, anche a distanza, e utilizzando risorse fornite da enti di tutela dei consumatori. Più sei informato, minori sono le possibilità di cadere vittima di truffe. Molto materiale è disponibile su edufin.fabi.it.

FABI Ufficio Stampa
Email stampa@fabi.it
Telefono 06.8415751
Mobile 331.4386554 / 348.2385090 / 328.1576095

I 10 CONSIGLI DELLA FABI DA PORTARE IN VACANZA

1. HOME BANKING IN SICUREZZA

Utilizza sempre una connessione internet privata quando accedi al tuo conto bancario online. Evita le reti Wi-Fi pubbliche, come quelle in caffè o aeroporti, che possono essere meno sicure. Assicurati che l'indirizzo del sito web della tua banca inizi con "https://" e che ci sia un simbolo di lucchetto nella barra degli indirizzi che indica una connessione protetta.

2. PASSWORD ROBUSTE E AUTENTICAZIONE A DUE FATTORI

Per l'home banking e altri servizi online, scegli password complesse che combinano lettere maiuscole e minuscole, numeri e simboli. Non usare la stessa password per più account. Attiva, ove possibile, l'autenticazione a due fattori (2FA), che richiede un secondo passaggio di verifica per accedere al tuo account, come un codice inviato al tuo telefono e via e-mail.

3. ATTENZIONE AL PISHING E ALLE MAIL SOSPETTE

Non cliccare mai su link o allegati provenienti da e-mail sospette che sembrano provenire dalla tua banca o da altri servizi fiduciari. Le banche non chiedono mai dati personali, come password o PIN, via e-mail. Verifica sempre l'autenticità dei messaggi contattando direttamente la banca attraverso i canali ufficiali.

4. MONITORAGGIO DELLE TRANSAZIONI

Controlla regolarmente i movimenti del tuo conto bancario e le transazioni sulle tue carte di credito. Imposta notifiche via SMS o e-mail per essere informato di ogni operazione. In caso di movimenti non autorizzati, contatta immediatamente la tua banca.

5. ACQUISTI SICURI NELL'E-COMMERCE

Quando fai acquisti online, verifica l'affidabilità del venditore e leggi le recensioni degli altri utenti. Utilizza metodi di pagamento sicuri come carte di credito o servizi di pagamento protetti che offrono meccanismi di contestazione e rimborso. Evita i bonifici bancari diretti, specialmente con venditori sconosciuti

I 10 CONSIGLI DELLA FABI DA PORTARE IN VACANZA

6. USO CAUTELATIVO DEI SISTEMI DI PAGAMENTO DIGITALE

Quando usi sistemi di pagamento digitale come PayPal, Google Pay, Satispay o Apple Pay, assicurati di proteggere i tuoi dispositivi con password o impronta digitale. Non memorizzare mai le tue credenziali di accesso sui dispositivi e non condividere queste informazioni.

7. PRESTITI ONLINE PRUDENTI E OCCHIO AL BUY NOW PAY LATER

Prima di accettare un prestito online o optare per un'opzione di pagamento differito, controlla attentamente la legittimità del fornitore e leggi i termini e condizioni. Fai attenzione a tassi di interesse, commissioni nascoste e le penalità in caso di mancato pagamento.

8. PROTEZIONE DEL DISPOSITIVO

Installa un software antivirus affidabile su tutti i dispositivi che utilizzi per accedere a servizi finanziari online e tienilo aggiornato. Esegui regolarmente scansioni alla ricerca di malware e non installare software da fonti non verificate.

9. AGGIORNAMENTI DEL SOFTWARE

Mantieni sempre aggiornati il sistema operativo e le applicazioni sui tuoi dispositivi. Gli aggiornamenti spesso includono correzioni per vulnerabilità di sicurezza che potrebbero essere sfruttate da malintenzionati.

10. EDUCAZIONE FINANZIARIA CONTINUA

Rimani informato sulle ultime truffe e frodi online leggendo la stampa specializzata, partecipando a eventi pubblici, anche a distanza, e utilizzando risorse fornite da enti di tutela dei consumatori. Più sei informato, minori sono le possibilità di cadere vittima di truffe. Molto materiale è disponibile su edufin.fabi.it.