ABI Associazione Bancaria Italiana

Polizia di Stato

CERTFin
CERT Finanziario Italiano

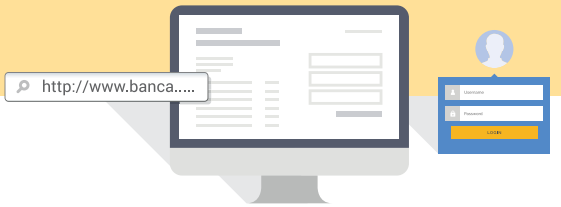
FONDAZIONE per l'EDUCAZIONE FINANZIARIA e al RISPARMIO

HOME BANKING, CARTE, E-COMMERCE...

REGOLE SEMPLICI PER PAGAMENTI SICURI

3 UTILI CONSIGLI PER...

Usare in sicurezza l'home banking



1. Per connetterti al sito della banca **digita direttamente l'indirizzo nella barra di navigazione** e controlla che **il nome del sito sia scritto correttamente**; non cliccare mai su link che rimandano al sito della banca se sono all'interno di email o sms sospetti.

2. Quando sei sul sito della banca, clicca due volte sull'**icona del lucchetto** nella barra di navigazione e verifica la correttezza dei dati che vengono visualizzati (trovi l'icona a sinistra se utilizzi come ***browser*** Mozilla e Chrome, a destra per Internet Explorer).

3. Modifica periodicamente i codici di accesso alla tua area riservata e **controlla regolarmente le movimentazioni del conto corrente** per assicurarti che le transazioni riportate siano quelle che hai realmente effettuato. I sistemi di notifica messi a disposizione dalla tua banca possono esserti molto utili per verificare le operazioni.

LO SAPEVI CHE...

Il **PHISHING** è una truffa che consiste nell'invio di email o SMS (nel qual caso si parla di **SMISHING**) fraudolenti che sembrano della tua banca e mirano a carpire dati riservati. Ricorda che la banca o qualsiasi Autorità non richiederanno mai via email o SMS i dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali.

Il **VISHING** è un'evoluzione del phishing. Tramite email, chat o sms si viene contattati da un presunto operatore della banca (anche attraverso una voce pre-registrata) che tenta di carpire, con l'inganno, informazioni private. Ricorda, come già anticipato, che la banca non richiederà mai telefonicamente le tue informazioni personali.

3 UTILI CONSIGLI PER...

Usare in sicurezza le carte di pagamento

1. **Custodisci la tua carta** con cura (mai **insieme al *PIN*!**) ed evita di separartene (ad esempio al ristorante); non comunicare mai ad altri le **informazioni di dettaglio delle tue carte.**

2. Se ti accorgi di **un uso non autorizzato** della tua carta comunicalo subito alla tua banca; mentre se la smarrisci o te la rubano, **bloccala immediatamente**, in modo da evitarne l'uso fraudolento e **rivolgiti alle forze dell'ordine** per sporgere denuncia.

3. Quando sei allo **sportello automatico** (ATM) della banca segui alcuni accorgimenti, come impedire che qualcuno possa leggere e memorizzare il tuo PIN mentre lo digiti (ad esempio, copri la tastiera con la mano) o lasciarti distrarre da estranei mentre compi operazioni (potrebbe trattarsi di un tentativo di raggiro).

LO SAPEVI CHE...

Il **3DSecure** (3DS) è un sistema di protezione antifrode per le carte di credito che garantisce una maggiore tutela per gli acquisti online, poiché abbina la carta di pagamento a un codice univoco e dinamico – diverso per ogni acquisto - che viene richiesto per autorizzare il pagamento online sui siti convenzionati 3DS. Se stai effettuando un pagamento con carta su un sito di e-commerce che non usa il sistema 3DS assicurati che abbia comunque degli efficaci presidi di sicurezza, ad esempio, come vedrai piu avanti, dovresti visualizzare nella barra del browser la scritta HTTPS.

Il **CVV** (Card Validation Value), oppure CVC (Card Validation Code) o CIN (Card Identification Number) è un codice di sicurezza composto da 3 o 4 numeri presente sul retro della carta di pagamento che serve a verificare che questa sia realmente in possesso di chi sta facendo un acquisto online: potrebbe essere richiesto come ulteriore conferma durante le transazioni.

3 UTILI CONSIGLI PER...

Usare in sicurezza l'e-commerce

1. Evita di effettuare transazioni online da **computer condivisi o postazioni in luoghi che potrebbero essere poco sicuri**, come hotel e Internet cafè, e al termine di ogni acquisto, ricorda di effettuare il ***log-out*** dal sito di e-commerce.

2. Utilizza **credenziali diverse per autenticarti su siti diversi** ed evita il "salvataggio automatico" delle password sul browser.

3. Per **evitare** di incorrere in **truffe di natura commerciale**, valuta sempre le recensioni lasciate da altri utenti sull'**affidabilità del venditore** a cui ti stai rivolgendo: un'offerta troppo conveniente potrebbe nascondere una truffa.

LO SAPEVI CHE...

Nel campo indirizzo, cioè nella barra del browser, la scritta cambia da http a **HTTPS** quando passi ad una connessione protetta da un "certificato di sicurezza", utile per identificare il mittente delle informazioni sul sito e utilizzato sempre per svolgere pagamenti online. Presta quindi molta attenzione che il testo sia in https, soprattutto quando sei sul sito della banca o devi compiere operazioni online.

Quando si parla di **SPAM** ci si riferisce a richieste che possono arrivare via email o SMS che invitano all'apertura di allegati o rimandano a link sospetti (potrebbero sembrare inviate dalla tua banca, da compagnie telefoniche, circuiti di pagamento, insomma da siti noti, proprio per indurti ad aprirli).

3 UTILI CONSIGLI PER...

Usare in sicurezza il mobile banking

1. Installa e mantieni sempre **aggiornati antivirus, sistema operativo** e applicativi e ricorda di disattivare Wi-Fi, geolocalizzazione e ***bluetooth*** quando non li usi.

2. Utilizza **esclusivamente app ufficiali** e, in fase di installazione, fai **attenzione ai permessi richiesti** assicurandoti che siano strettamente connessi al servizio che intendi utilizzare. In caso di furto o smarrimento del tuo dispositivo avverti la tua banca affinché interrompa il servizio app di mobile banking.

3. Per maggiore sicurezza **imposta il blocco automatico del tuo dispositivo** quando entra in ***stand-by*** e, per proteggere i tuoi dati, quando possibile, **attiva la *crittografia*** del dispositivo e della memory card.

LO SAPEVI CHE...

Il **REMOTE LOCK** e **REMOTE WIPE** sono funzionalità che possono essere abilitate su smartphone e tablet e che consentono al proprietario, in caso di furto o smarrimento del proprio smartphone, di bloccare il terminale (remote lock) o di cancellare, da un altro PC, tutti i dati in esso contenuti (remote wipe).

Con **JAILBREAKING** e **ROOTING** si intendono le procedure che permettono di ottenere controlli privilegiati su smartphone e tablet, consentendo tra l'altro l'installazione di applicazioni alternative rispetto a quelle ufficiali e di modificare i file di sistema. Fai molta attenzione perché queste modifiche delle impostazioni di sistema sono molto pericolose e possono facilitare l'infezione dei dispositivi attraverso virus e software malevoli, anche in fase di download delle app.

3 UTILI CONSIGLI PER...

Usare in sicurezza il computer

1. Verifica che siano attivi gli **aggiornamenti automatici** del sistema operativo e degli altri software installati. Mantieni sempre aggiornato un **antivirus** ed elimina periodicamente i ***cookies*** e i ***file temporanei*** Internet utilizzando le opzioni del tuo browser.

2. Non aprire mai **allegati o link sospetti**, soprattutto nel caso di ***file eseguibili*** (che terminano con .exe) e non installare software se non sei certo siano affidabili.

3. Non utilizzare memorie esterne (come chiavette USB) di **dubbia provenienza**; verifica la sicurezza di questi dispositivi facendo le scansioni automatiche previste dai principali software antivirus al momento dell'installazione. E ricorda, un uso sicuro del proprio computer è il primo passo per transazioni sicure!

LO SAPEVI CHE...

Il **FIREWALL** è un software che serve a filtrare il traffico dati in entrata e in uscita e proteggere da intrusioni indesiderate che possono compromettere la privacy o agevolare l'installazione di software malevoli. Una volta installato un firewall sul computer tutte le comunicazioni passano attraverso questo applicativo in modo da proteggere al meglio la navigazione online.

Il termine **MALWARE**, abbreviazione di "malicious software" indica un software dannoso che viene installato sul computer senza il tuo consenso.

3 UTILI CONSIGLI PER...

Usare in sicurezza i social network

1. **Soffermati sulle politiche di gestione della *privacy*** adottate dai canali social: chi può vedere quello che pubblichi? Chi può contattarti? Personalizza al meglio il tuo profilo per avere più o meno visibilità a seconda delle tue esigenze.

2. Presta molta attenzione nel **pubblicare video, foto o post con informazioni personali**; una volta condivisi è molto difficile controllarne la diffusione. Non dimenticare che tutti i contenuti condivisi sui social possono fornire informazioni utili per attacchi di spear phishing, furti di identità e altri tipi di violazione, anche in relazione alla persona fisica.

3. **Non usare la stessa password** per account social, email e account bancario: può sembrare la soluzione più semplice ma ti esponi a dei rischi! Quando possibile, utilizza metodi di autenticazione che prevedono più fattori, per innalzare i livelli di sicurezza (ad esempio per le operazioni bancarie password più PIN casuale inviato via SMS).

LO SAPEVI CHE...

L'INGEGNERIA SOCIALE (dall'inglese social engineering) è la sottrazione mirata di dati e codici segreti di una persona tramite l'analisi delle sue relazioni sociali (ad esempio sui social network).

Lo **SPEAR PHISHING** è un esempio di ingegneria sociale; si tratta di un'email, un SMS o una richiesta di contatto che sembrano provenire da una persona o un'azienda che conosci. Tale tecnica fa sì che tu sia meno sospettoso e fornisca le informazioni che ti vengono chieste. Fai molta attenzione al mittente delle comunicazioni.

e Infine....

- **Rifletti attentamente prima di allegare alle email o inviare attraverso altri canali immagini relative ai tuoi strumenti di pagamento.** Valuta ogni volta il destinatario a cui le invii e il motivo per cui ritieni opportuno farlo.

- In particolare, **evita di inviare via cellulare, fax o email la fotografia di un assegno (circolare o bancario)** per concludere una transazione commerciale. Se la controparte fosse in malafede, potrebbe utilizzarla per "costruire un clone" dell'assegno da incassare al posto dell'originale.

- Quando ricevi un buono d'acquisto via mail da un esercente, **verifica la provenienza del messaggio prima di fornire qualsiasi dato o informazione personale.**

GLOSSARIO

B

Bluetooth
è una tecnica di telecomunicazione senza fili che permette a due dispositivi di comunicare tramite una frequenza radio scambiandosi file, foto, documenti, video e così via.

Browser
programmi/applicazioni che consentono di navigare ed interagire su Internet.

C

Cookies
file che vengono creati quando si visita un sito web per identificare l'utente e memorizzarne ricerche di navigazione e preferenze sul web. Tendenzialmente non sono pericolosi a meno che non siano generati da siti poco sicuri.

Crittografia dei dati
è un sistema che rende ogni dato illeggibile se non si possiede la chiave di decriptazione, ad esempio una password, un PIN o le impronte digitali.

F

File eseguibili
file che contengono un programma scritto in un formato specifico che lo rende pronto per l'esecuzione all'interno di un determinato sistema operativo (come Microsoft Windows o MAC OS).

File temporanei
copie dei file create automaticamente dalla maggior parte delle applicazioni (ad esempio Word) mentre vengono utilizzate dall'utente.

L

Log-out
la procedura di uscita o disconnessione da un sistema o applicazione informatica a cui si era precedentemente connessi attraverso una procedura denominata di Log-in.

P

PIN (Personal Identification Number)
è il codice identificativo associato ad ogni carta di pagamento che deve essere digitato per poter utilizzare la carta di debito e talvolta anche la carta di credito.

Privacy
traducibile in italiano con "riservatezza" sta ad indicare il diritto di una persona di controllare le informazioni che la riguardano; la "Privacy" indica l'insieme delle norme che regolano la tutela e l'utilizzo dei dati personali.

S

Stand-by
è la modalità "pausa" di un dispositivo, una fase in cui non è operativo ma comunque pronto per passare dall'inattività temporanea all'attività.

978-88-449-1147-8

Per dubbi, segnalazioni, denunce, puoi rivolgerti alla Polizia Postale e delle Comunicazioni.

È possibile anche online:
http://www.commissariatodips.it

ACU
Associazione Consumatori Utenti
Organizzazione senza scopo di lucro

ADICONSUM
Associazione Difesa Consumatori e Ambiente promossa dalla CISL

Adoc

Casa del Consumatore

CITTADINANZATTIVA

CONFCONSUMATORI
CONFEDERAZIONE GENERALE DEI CONSUMATORI

Federconsumatori

LEGA CONSUMATORI

MOVIMENTO CONSUMATORI

MOVIMENTO DIFESA del Cittadino

U.Di.Con.
UNIONE per la DIFESA dei CONSUMATORI

1955
UNC
CONSUMATORI.IT

Per maggiori informazioni sulle attività del CERTFin
www.certfin.it

ABISERVIZI BANCARIA EDITRICE