Sicurezza informatica

In un'era in cui la tecnologia ha influenzato e modificato le abitudini della nostra vita quotidiana, anche il settore bancario ha vissuto evoluzioni a seguito dall'avvento della digitalizzazione. Nuovi canali per gestire in autonomia e mobilità l'operatività bancaria, nonché strumenti di pagamento digitali come mobile payments e digital wallet, sono esempi di opportunità offerte dall'innovazione.

Lo sviluppo tecnologico ha tuttavia esposto gli utenti a maggiori tentativi di frode: per riconoscere tempestivamente le insidie del web ed essere in grado di prevenirle, anche durante la fruizione di servizi finanziari, la cultura dell'informazione gioca un ruolo fondamentale.

La tecnologia ci riserva benefici ma ci espone anche a rischi, come l'intensificarsi dei tentativi di frode. Cosa si intende per truffa online?

La truffa online è un **reato** che viene commesso, per la maggior parte dei casi, tramite **siti web non autentici** e **applicazioni non ufficiali**. Lo scopo è **ingannare** la vittima, anche grazie all'utilizzo di **tecniche persuasive**, inducendola a comunicare informazioni dalle quali il malintenzionato potrà trarre **illeciti profitti**.

L'**attenzione** e l'**informazione** sono soluzioni per eludere i criminali informatici; saper inoltre **ben valutare le richieste** che si ricevono e **non farsi condizionare da facili guadagni** sono ulteriori metodi per non rimanere coinvolti in questa tipologia di frode.

Inoltre, se grazie alla giusta cautela si è intercettato un tentativo di raggiro, è bene segnalarlo con assoluta tempestività all'**autorità competente**, nonché informare la **banca** affinché possano essere presi provvedimenti e attuate azioni per contrastare il diffondersi della truffa.

A quali elementi è bene prestare attenzione per riconoscere tempestivamente un tentativo di frode?

Le **truffe online** sono sempre più sofisticate e in continua evoluzione. Possono avvenire attraverso **differenti canali di contatto** come e-mail (*phishing*), SMS o messaggi WhatsApp (*smishing*), chiamate (*vishing*) e social network.

Molteplici sono i pretesti utilizzati dai malintenzionati: ecco perché è bene **non agire con impulsività**, dedicare il giusto tempo alla **lettura delle comunicazioni** e **prestare attenzione ad alcuni elementi** chiave che possono aiutare a riconoscere come tale un tentativo di frode.

Mittente	Anche se il nome appare analogo a quello della banca, in una frode l'indirizzo e-mail non corrisponde a quello ufficiale dell'istituto.
La presenza di refusi, errori grammaticali e ortografici sono segnali che contraddistinguono una possibile truffa.	**Forma**
Urgenza	La banca avvisa gli utenti con preavviso e non invia mai richieste di ultimatum. Solleciti, per eseguire con urgenza bonifici o per comunicare tempestivamente i dati di una Carta, devono destare sospetto.
Se in una comunicazione inaspettata è presente un allegato, è sconsigliato aprirlo e scaricarne il contenuto. Il file potrebbe infatti essere un *malware* che permetterà a soggetti non autorizzati di entrare in possesso di documenti riservati e informazioni bancarie, nonché infettare il dispositivo.	**Allegati**

Quali comportamenti e corrette abitudini è utile adottare per tutelarsi al meglio?

Ridurre il rischio di attacchi e truffe online è una priorità di aziende e società che, con costante impegno, rafforzano i propri **presidi di sicurezza** per garantire una **sempre maggior tutela dei consumatori**.

Per contrastare le potenziali minacce del web, anche la collaborazione del singolo gioca un ruolo fondamentale: **adottare semplici accortezze e virtuosi comportamenti** può contribuire concretamente a prevenirle.

Installare e **mantenere aggiornati** antivirus su PC, smartphone e tablet. **Scaricare** inoltre le **applicazioni** solo dagli **store ufficiali**.

Impostare password robuste utilizzando lettere, numeri e caratteri speciali. Cambiarle con frequenza, **non utilizzare** le **stesse per più account** e **disabilitarne** il **salvataggio automatico**.

Prediligere dispositivi personali, in particolare quando si utilizzano applicazioni bancarie, e **disattivare** le **reti Wi-Fi pubbliche** poiché **potrebbero non essere sicure**.

Diffidare di chiamate in cui viene richiesta, con il pretesto di dare assistenza, l'installazione di **software** per controllare **da remoto dispositivi personali**.

Non comunicare dati delle **Carte** e **Codici** per accedere ad applicazioni della banca: sono **strettamente personali** e nessun operatore è autorizzato a contattare il cliente per richiederli.

Limitare la **condivisione di informazioni** sui social network (come ad esempio numeri di telefono, indirizzo di residenza) e **scegliere un adeguato livello di privacy** per evitare furti di identità.

Acquisti online: quando sono un buon affare e quando invece sono una truffa?

Con l'avvento del **Black Friday** e del **Cyber Monday** gli acquisti online raggiungono livelli record e, con l'aumentare progressivo delle vendite, si **intensificano** anche gli **attacchi di criminali informatici.**

Durante questo periodo, infatti, è oltremodo consigliato **mantenere alto il livello di attenzione** e approcciarsi in modo metodico agli acquisti, ad esempio:

- rivolgendosi a siti di e-commerce conosciuti;
- prediligendo modalità di pagamento con carta di credito;
- diffidando di rivenditori che spingono a prendere decisioni rapide.

Oltre a ciò, è importante:

Valutare le offerte: se appaiono troppo convenienti da sembrare quasi inverosimili, prima di compiere azioni è consigliato **verificare l'affidabilità del sito** anche attraverso la lettura delle **recensioni**.

Diffidare di **comunicazioni** che invitano a cliccare su link per inserire il **PAN della Carta** o il numero di un **documento d'identità**, al fine di **confermare un acquisto o sbloccare la consegna** di un pacco in giacenza.

Attivare sulle Carte **servizi di protezione** per prevenirne usi illeciti sul web e impostare **alert** che ne notificano gli utilizzi. **Controllare** inoltre regolarmente i **movimenti** dei propri conti per individuare con **tempestività** transazioni non autorizzate.

In conclusione: perché è importante l'educazione digitale?

In un'epoca in cui il digitale è diventato parte integrante della gestione dell'operatività bancaria, la **sicurezza informatica** non può essere trascurata.

In Mediobanca Premier **investiamo nell'innovazione** e adottiamo **evolute misure di protezione** al fine di tutelare al meglio i nostri clienti. Poniamo inoltre l'attenzione nel sensibilizzare e promuovere la cultura dell'**educazione digitale**: l'informazione è infatti il primo passo per **sfruttare le opportunità della tecnologia e prevenirne i potenziali rischi**.

Pertanto, per rafforzare i consigli già condivisi in questo articolo, abbiamo realizzato una **Guida** che approfondisce **come riconoscere e contrastare** le principali tipologie di **frode in ambito bancario**.
È sempre a disposizione nella sezione *Accesso e sicurezza* del sito mediobancapremier.com.