Associazione Difesa Utenti Servizi Bancari Finanziari Assicurativi Postali

A.D.U.S.B.E.F. Toscana "G. Caselli"

BREVE VADEMECUM SULLA SICUREZZA DELLE OPERAZIONI ON-LINE

In questi giorni in cui le maggiori attività quotidiane vengono svolte in ambiente domestico, con un conseguente aumento di acquisti on-line ed uso di strumenti di pagamento elettronici, è ancora più importante prestare maggiore attenzione verso la sicurezza delle transazioni sia su siti internet di vendita che bancari.

Di seguito pochi semplici accorgimenti utili per compiere in maggiore sicurezza le operazioni:

1. Verificare sempre la sicurezza del sito su cui si opera.

In particolare, qualora si operi in ambiente di home banking verificare sempre il protocollo di sicurezza della pagina (https) al fine di non incorrere in transazioni su siti non affin possibili ipotesi di man in the browser o altri attacchi informatici.

Qualora si notino rallentamenti ingiustificati nell'accesso all'area riservata di home banking cessare la sessione e verificare presso il proprio istituto di credito i motivi.

2. Prestare maggiore attenzione agli attacchi in forma di phishing.

In momenti di incertezza e di crisi si è maggiormente portati a prestare minore attenzione ai messaggi che riceviamo ed a riporre maggiore affidamento in essi. Prima di aprire allegati o cliccare link oppure fornire nostre credenziali a terzi è sempre importante verificare l'affidabilità del messaggio che li richiede e/o l'indirizzo mail da cui ci proviene.

Può accadere infatti di incorrere in errore proprio perché l'indirizzo che pone in essere simili attacchi ad una prima lettura appaia simile ad altri a noi noti.

3. Resta in ogni caso di fondamentale importanza non inviare credenziali o codici di accesso richieste con comunicazioni "civetta".

Si ricorda che le credenziali di accesso **NON vengono mai richieste** tramite mail e/o contatti telefonici

4. Un accorgimento altrettanto importante è quello di evitare di installare sul proprio PC programmi scaricati da siti poco affidabili o poco sicuri. Al contempo si dovrà procedere alla verifica di di una corretta installazione e aggiornamento degli aggiornamenti del sistema operativo su cui si opera, del firewall e dell'antivirus.

5. Anche quando operiamo su siti internet già conosciuti è sempre importante verificare il protocollo di sicurezza della pagina e verificare di essere sulla pagina desiderata.

6. **Nelle transazioni di acquisto e di pagamento su siti sarà altresì importante seguire i protocolli di sicurezza indicati per il buon esito dell'operazione, prestando particolare attenzione a possibili finestre di reindirizzamento ad altre pagine o siti, soprattutto nel momento in cui inseriamo i dati della carta di credito o di altro strumento di pagamento.**

7. **Attiviamo, se possibile, i protocolli di sicurezza messi a disposizione dal proprio istituto di credito per gli ambienti di home banking quali : servizi di OTP Password sul cellulare èer la validazione di operazioni, sms alert e comunicazioni di accesso alla propria area riservata home banking.**

   Questi strumenti permettono un maggiore controllo, anche in tempo reale, su atti dispositivi e violazioni degli strumenti di pagamento e accessi non autorizzati su home banking.

8. **Dato il sicuro aumento delle sessioni on-line di acquisto in questo particolare momento è importante non salvare mai password e dati di accesso e soprattutto effettuare il logout alla fine di ogni sessione.**

   In particolare è opportuno non lasciare aperte le sessioni sul proprio indirizzo e-mail e pec né tantomeno sul browser: è necessario pertanto terminare ogni sessione aperta procedendo ad effettuare il logout alla fine di essa seguendo le indicazioni del sito o del browser.

9. **Una volta terminate le operazioni di accesso al proprio ambiente di home banking è sempre importante effettuare il logout al termine dell'operatività di home banking.**

   Ciò al fine di aumentare la riservatezza dei propri dati e per una maggiore sicurezza qualora l'operazione sia fatta in ambiente condiviso (pc utilizzato da più utenti), ma anche per evitare quelle vulnerabilità generate dalla semplice chiusura della pagina su cui si sta operando.

10. **È importante comunque ricordare che gestori di servizi di pagamento ed di home banking non richiedono mai credenziali di accesso o altre operazioni idonee alla identificazione del cleinte al di fuori dei canali gestiti con alto livello di sicurezza dagli stessi predisposti.**

*

È importante, infine, ricordare che in momenti di disagio o di crisi in cui ognuno di noi è esposto alla ricezione di un alto numero di informazioni, spesso su più canali, possono aumentare le ipotesi di phishing e di violazione della sicurezza dei propri strumenti di pagamento e di comunicazione.

Diviene quindi importante prestare maggiore attenzione ai criteri di sicurezza minimi nell'impiego di essi ricordando sempre che attacchi informatici come il phishing ruotano proprio attorno a tale elemento emozionale e ad una interazione intelligente con la vittima, nella quale il portatore dell'attacco sfrutta la comunicazione e spesso il timore generato da asseriti malfunzionamenti o blocchi dello strumento di pagamento per poter poi carpire informazioni riservate dalla vittima.

Francesco Cocchi
Delegato ADUSBEF