DECALOGO DELLA SICUREZZA

1. **Diffidate di qualunque E-mail che richieda l'invio di dati personali**
   Diffidate di qualunque richiesta di invio, tramite posta elettronica o inserimento su pagina web, di password, dati riservati, numeri di carte di credito, chiavi di accesso al servizio home banking o qualsivoglia informazione personale. Se pur graficamente identica ai colori del sito cui generalmente vi collegate, si tratta certamente di un tentativo di estorsione dei vostri dati di accesso. Una banca non richiederebbe mai ai propri clienti tali informazioni e ancor meno via posta elettronica o sms.
2. **Non cliccate sui link presenti nelle E-mail di dubbia provenienza**
   E' preferibile non cliccare su link riportati in queste mail, in quanto potrebbero condurre a pagine del tutto simili a quelle reali, ma opportunamente realizzate per rubare i vostri dati di accesso. Le mail che rappresentano potenziali minacce sono facilmente riconoscibili in quanto, se presentano anche una sola delle caratteristiche del punto precedente, sono tali da ritenersi false. Se ricevete una mail di questo tipo informate il vostro referente bancario. La banca, pur non potendo impedire l'invio di ulteriori mail al vostro indirizzo di posta, potrà comunque allertare gli altri clienti del pericolo.
3. **Verificare il certificato di sicurezza (SSL) del sito cui vi connettete**
   Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'URL che compare nella barra degli indirizzi del browser comincia con **https://** e non con **http://**. Nella parte inferiore della pagina è presente un lucchetto. Cliccando su di esso è possibile verificare che il proprietario del certificato di sicurezza sia proprio la banca o l'ente fornitore del servizio di cui vogliamo usufruire.
4. **Verificate la correttezza degli indirizzi nella barra del browser**
   Verificate sempre che l'indirizzo cui vi collegate sia quello fornitovi dalla banca. Alcuni siti utilizzano URL che somigliano molto a quelli reali, ma in realtà sono differenti. Un esempio pratico può chiarire meglio il problema. Se l'URL corretto del nostro servizio è **www.lamiabanca.it**, allora tutti gli indirizzi che **terminano** con **lamiabanca.it** prima dello slash sono sicuri. Quindi:

   ```
   http://banking.lamiabanca.it/etc...
   è un URL valido (lamiabanca.it)

   http://homebanking.lamiabanca.it/etc...
   è un URL valido (lamiabanca.it)

   http://www.lamiabanca.it.8798.it/etc...
   NON è un URL valido (8798.it)

   http://lamiabanca.ita.it/etc...
   NON è un URL valido (ita.it)
   ```
5. **Verificate sempre l'origine delle pagine che visitate**
   Nonostante quanto detto nel punto precedente, in taluni casi una falsa pagina web opportunamente preparata, può visualizzare nella barra degli indirizzi del proprio browser, l'URL con cui il navigatore ha dimestichezza. Questa tecnica sfrutta alcuni bachi del nostro sistema operativo e/o browser. Ecco quindi, la necessità di aggiornare il proprio software alle ultime versioni, patch.
6. **Diffidate delle modifiche al sito non annunciate preventivamente**
   Diffidate degli improvvisi cambi di modalità con i quali vi viene chiesto di inserire i codici di accesso all’home banking: ad esempio, se questi vengono richiesti improvvisamente

tramite pop-up (una finestra aggiuntiva di dimensioni ridotte) anziché tramite la solita pagina. Generalmente, la banca notifica ai propri clienti, con un debito anticipo, ogni modifica di questo tipo.

7. **Verificate regolarmente il vostro estratto conto**
   Controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emettitore della carta di credito. Attivate i sistemi di notifica gratuiti che tali enti spesso forniscono, mediante i quali è possibile ricevere notifica di qualsiasi addebito mediante sms o mail.
8. **Proteggetevi dal malware, software malevolo**
   Proteggetevi dal software malevolo, detto "malware" e dagli eventuali bug (bachi - errori di programmazione) del vostro sistema. Questa tipologia di software, che si può installare navigando siti non sicuri o aprendo mail con allegati sospetti, ha come obiettivo il danneggiamento, o l'alterazione del funzionamento del vostro sistema. Ne esistono varie tipologie, partendo da quelli relativamente innocui, in grado di spiare la vostra navigazione e inviarne un resoconto ad aziende preposte ad indagini di mercato, a quelli pericolosi, in grado di installarsi, riprodursi, e diffondersi, o in grado di registrare tutto ciò che viene digitato sulla tastiera del vostro pc (**keyloggers**) inviando poi i dati a malintenzionati, o inviando in autonomia mail contenenti dati sensibili (**trojan**) o addirittura in grado di "scattare fotografie" al vostro desktop in determinate situazioni e poi inviarle via posta elettronica (**screen grabbers**).
9. **Aggiornate sempre il sistema operativo e i vostri software**
   E' necessario, quindi, verificare sempre, secondo le modalità di ogni singolo software, che il sistema operativo e le applicazioni utilizzate siano aggiornate alla versione più recente, o che siano state scaricate e installate le eventuali patch in grado di risolvere i problemi di sicurezza. Inoltre è bene installare un **antispyware**, o un **antitrojan**, un **antivirus** o addirittura un **firewall** (alcuni molto validi, sono a disposizione di tutti gratuitamente).
10. **Per qualsiasi chiarimento o dubbio contattate la vostra banca**
    Non esitate a contattare la vostra banca, o il call center preposto, per qualsiasi segnalazione, anomalia, o dubbio. Il personale preposto sarà disponibile a verificare con voi le situazioni che via via si presenteranno al fine di fugare ogni dubbio e rendere la vostra navigazione e fruizione del servizio sempre più sicura.