

Gentile Cliente,

Vogliamo richiamare la Sua attenzione su alcuni fenomeni fraudolenti che stanno interessando i servizi di *Internet Banking* forniti dalle banche, e si concretizzano con “*phishing*” ed i “*Malware*”.

Il *phishing* è una frode informatica ideata allo scopo di sottrarre i dati personali a Clienti che utilizzano servizi di *Internet Banking* come il nostro (ad esempio codici di accesso al servizio, *password*, ecc...).

La frode è attuata dai truffatori tramite l’invio di falsi messaggi *e-mail*, apparentemente provenienti dalla Banca e composti utilizzando il logo, il nome e la grafica tipica della banca imitata. Queste *e-mail* invitano il destinatario a collegarsi, tramite l’attivazione del *link* contenuto nel messaggio, ad un sito *Internet* del tutto simile a quello della banca, dove vengono richieste le informazioni riservate di cui sopra.

Le frodi informatiche possono essere realizzate anche con l’installazione sul *personal computer* dell’utente di “*Malware*” ovvero programmi o frammenti di codice informatico in grado di produrre danno al terminale. Ne esistono varie tipologie, come diversi sono gli effetti dannosi che ne possono conseguire. Tra i casi più frequenti si riscontra la presenza di *worm*: si tratta di frammenti di codice, autonomi ed indipendenti, che possono essere scaricati sul *personal computer* durante la navigazione in *Internet* su siti dannosi.

Questi programmi esistono solo nella memoria del terminale e ne compromettono la corretta operatività modificando i collegamenti nelle pagine *internet* abitualmente visitate, al fine di realizzare il reindirizzamento ai siti contraffatti che riproducono fedelmente le pagine *web* originali e sottrarre le credenziali di autenticazione al servizio. Attraverso questi *form* i truffatori possono raccogliere automaticamente queste informazioni per poi utilizzarle per effettuare disposizione bancarie fraudolente a danno dei clienti.

Tale meccanismo può conoscere anche varianti più sofisticate e pericolose che arrivano alla clonazione del sito originale su un dominio simile ma contraffatto. Se erroneamente dovesse inserire i suoi dati personali all’interno di *form* falsi La invitiamo a:

- provvedere **immediatamente a modificare la *password* di accesso al servizio, o bloccare il servizio stesso** digitando per 5 volte una *password* errata;
- contattare subito il **Numero Verde 800.670999**.

In ogni caso, Le raccomandiamo di seguire con la massima attenzione le indicazioni di seguito riportate.

**1) illimity Bank S.p.A. non richiede mai codici, *password* o altre informazioni riservate tramite *email*.**

È necessario, quindi, diffidare di *e-mail*, anche se ricevute da mittenti conosciuti, dove vengono richiesti dati riservati. In nessun caso, illimity Bank richiede ai propri Clienti informazioni quali *password*, User ID, codici di accesso, codici generati dal dispositivo Token, PIN o numeri di carte di pagamento o altre informazioni riservate tramite *e-mail*.

**2) È necessario verificare preventivamente il mittente delle *e-mail*.**

È possibile riconoscere le truffe attuate via *e-mail*, in quanto generalmente queste:

- non sono personalizzate e contengono messaggi generici di richiesta di informazioni personali o riservate, per motivi non ben specificati (es.: scadenza dei codici, smarrimento, problemi tecnici o di sicurezza);
- fanno spesso uso di toni “intimidatori”, come le minacce di sospensione del servizio in caso di mancata risposta, che non sono mai presenti in comunicazioni della nostra Banca;
- non riportano una data di scadenza per l’invio delle informazioni;
- hanno spesso un italiano pieno di errori in quanto i messaggi sono generati dal truffatore con sistemi di traduzione automatica.

Per identificare una *e-mail* contraffatta, in sostanza, bisogna controllare la struttura dei testi e l’intestazione per verificarne la provenienza. Nel caso in cui riceva una *email* sospetta o comunque non attesa, non esiti a contattare il nostro Numero Verde 800.670999.

**3) A ricevimento di messaggi *e-mail* è sempre necessario evitare di attivare i *link* presenti nei messaggi (con un click del mouse sullo stesso *link*), ovvero aprire file allegati alle *e-mail*.**

Infatti, i siti *web* proposti, soprattutto se richiedono informazioni riservate o *password*, non vanno visitati, neppure per brevi periodi. Il *link* proposto potrebbe non essere quello “visualizzato” ed i *files* ricevuti potrebbero comportare rischi.

Non cliccate sui *link* presenti in *e-mail* ricevute, in quanto questi collegamenti potrebbero condurvi ad un sito maligno opportunamente contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del *browser* viene visualizzato l'indirizzo corretto, non fidatevi, l'indirizzo *web* visualizzato potrebbe essere stato alterato dal truffatore. Quindi, verificate che l'indirizzo del sito sul quale state navigando sia effettivamente <http://www.illimity.com>: **digitare sempre l'indirizzo completo nel browser tutte le volte che si desidera entrare in banca via Internet offre la sicurezza di essere sul sito ufficiale della Banca.**

**4) Durante la navigazione in Internet, è necessario evitare di fornire informazioni finanziarie o dati riservati.**

È opportuno non inserire mai *password* o numeri di carte di credito/debito in qualsiasi sito *web*, senza aver preventivamente verificato che il protocollo di trasmissione risulti "sicuro" (estensione HTTPS://, che identifica il protocollo di sicurezza SSL) e che il sito *web* risulti autentico (verifica del certificato). È possibile effettuare tali verifiche controllando la presenza del prefisso HTTPS:// nell'indirizzo *web* e che sia evidenziata l'icona a forma di "lucchetto chiuso" di colore oro (che indica il protocollo SSL a 128 bit) nella barra di stato del *browser*. Tale protocollo ha lo scopo di proteggere e garantire la riservatezza delle informazioni del Cliente durante l'utilizzo dei nostri servizi bancari via *Internet*. Per verificare il certificato di protezione dei siti, si può procedere tramite un doppio *click* sulla predetta icona a forma di lucchetto chiuso, ovvero tramite la funzione "proprietà" delle pagine protette dal protocollo SSL (tasto destro del *mouse*).

**5) È consigliato evitare il "salvataggio automatico" delle credenziali di autenticazione o delle password nelle memorie locali del browser o del personal computer utilizzato per la navigazione.**

I codici di identificazione (user id e *password*) utilizzati per accedere ai nostri servizi bancari tramite *Internet*, non devono mai essere "salvati" nelle memorie del *browser* o del *personal computer*. È opportuno verificare che la funzione di "completamento automatico" del *browser* non risulti attiva.

Per disattivarla, da INTERNET EXPLORER:

- cliccare sul menu "Strumenti" ed attivare "Opzioni Internet";
- cliccare quindi sulla voce "Contenuto" e "Completamento automatico";
- se presente, eliminare il "flag" dalla voce "Nome utente e password sui moduli" e cliccare sui pulsanti "Cancella moduli" e "Cancella password";
- Premere OK e chiudere quindi le finestre di opzioni aperte.

Da FIREFOX:

- cliccare sul menu "Opzioni" ed attivare nuovamente "Opzioni";
- cliccare quindi sulla voce "Privacy" selezionare "utilizza impostazioni personalizzate" nella voce "Impostazioni cronologia" e togliere il flag dalla voce "Conserva la cronologia delle ricerche e dei moduli";
- cliccare sulla voce "Sicurezza" togliere il flag dalla voce "Ricorda le password dei siti". □ Premere OK per chiudere la finestra di opzioni.

Per assistenza nell'esecuzione di queste operazioni o su come effettuare le impostazioni con altri browser (Google Chrome, Opera, etc.) può contattare il nostro Numero Verde 800.670999.

**6) È assolutamente consigliato adottare prodotti software che prevedano filtri per la posta indesiderata.**

Questi sistemi sono in grado di attenuare i rischi filtrando molte *e-mail* inviate con scopi illeciti, ovvero pericolose.

**7) È assolutamente consigliato utilizzare e mantenere aggiornato un idoneo Software Antivirus.**

Le *e-mail* inoltrate per scopi fraudolenti possono contenere anche programmi maligni, creati allo scopo di carpire e di trasmettere dati personali riservati all'elaboratore utilizzato dal criminale. I prodotti Antivirus più aggiornati sono in grado di intercettare ed annullare tali pericolosi programmi. Oltre ai prodotti commerciali sono disponibili diversi Antivirus gratuiti per uso personale che offrono un ottimo livello di protezione.

**8) È assolutamente consigliato utilizzare e mantenere aggiornato un Personal Firewall.**

L'impiego di questo programma di sicurezza, soprattutto durante la navigazione in *Internet*, previene lo scambio di comunicazioni indesiderate in ingresso o in uscita dal personal computer utilizzato dall'Utente. Come per gli Antivirus, oltre ai prodotti commerciali sono disponibili diversi Personal Firewall gratuiti per uso personale che offrono un ottimo livello di protezione.

**9) È opportuno aggiornare il Sistema Operativo e tutti i programmi utilizzati, con cadenza almeno semestrale.**

Le aziende produttrici dei Sistemi Operativi e dei *browser* rendono periodicamente disponibili *on-line*, e scaricabili gratuitamente, gli aggiornamenti agli stessi (le cosiddette *patch*), che incrementano tra l'altro la sicurezza di questi programmi. Sui siti *web* di queste aziende è anche possibile verificare che il vostro *browser* sia aggiornato: in caso contrario, è consigliabile scaricare ed installare le *patch*. Mantenere aggiornato il Sistema Operativo, il *browser*, il gestore della posta elettronica ed in generale i programmi *software* utilizzati previene l'utilizzo fraudolento delle cosiddette "Vulnerabilità" di questi prodotti, che sono normalmente "sfruttate" dai criminali informatici.

**10) Segnalare immediatamente all'Autorità Giudiziaria o di Polizia ed alla propria Banca il ricevimento di email aventi scopi o contenuti fraudolenti.**

Nel caso in cui riceviate una *e-mail* con contenuti di questo tipo, non rispondete all'e-mail stessa, ed informate subito illimity Bank S.p.A. tramite il Numero Verde o recandovi in filiale e l'Autorità Giudiziaria o di Polizia. La denuncia alle Autorità, in casi costituenti reato, consente alle stesse un immediato intervento ed alla Banca di attivare contromisure difensive a tutela dei propri Clienti.

**11) Diffidate in caso di improvvisi cambiamenti di modalità con la quale Vi viene chiesto di inserire i vostri codici di accesso al servizio di Internet Banking.**

Nella circostanza di improvvisi cambiamenti di modalità, non ufficialmente comunicati dalla Banca, con i quali viene chiesto di inserire i vostri codici di accesso all'*home banking*, ad esempio, se questi vengono chiesti non tramite la pagina ufficiale del sito ma tramite inusuali finestre di *pop-up* (una finestra aggiuntiva di dimensioni ridotte), contattate la Banca tramite il *call center* o recandovi in Filiale.

**12) Digitate sempre il link della pagina di accesso al sito dell'Istituto e al servizio di Internet Banking.**

Qualora vogliate accedere al servizio di *Internet Banking*, o al sito dell'Istituto, digitate sempre correttamente l'indirizzo nella finestra del *browser*.

L'unico indirizzo di accesso è il seguente: <http://www.illimity.com>.

Per maggiore sicurezza è consigliabile non memorizzare tali indirizzi nei preferiti del *browser*.

**13) Proteggere il dispositivo Token.**

Custodite accuratamente il Vostro dispositivo Token, in modo che nessun soggetto estraneo ne venga in possesso o possa impadronirsene. I codici generati dal dispositivo Token non devono essere mai comunicati o utilizzati se non all'atto della richiesta eseguita nell'ambito del servizio per la conferma delle operazioni dispositive.