

Premessa

Con il presente documento la **Banca di Forlì Credito Cooperativo** intende fornire ai nuovi utilizzatori di servizi bancari on-line (Home Banking, Remote Banking, Trading on line, ecc) alcune informazioni relative ai rischi connessi all'utilizzo e alla memorizzazione di dati importanti quali password di accesso a servizi bancari on line in un computer, in particolare quando questo viene connesso ad internet.

Le informazioni fornite in questo documento non possono essere esaustive della problematica in oggetto, né possono garantire la completa sicurezza del computer e del collegamento. La **Banca di Forlì Credito Cooperativo** declina ogni responsabilità derivante dall'utilizzo del presente documento anche a causa di eventuali errori o inesattezze in esso contenuto.

Il problema

Il collegamento ai servizi on-line avviene tramite la digitazione, da parte del cliente, di nome utente e password; il server che gestisce l'autorizzazione non è in grado di stabilire se i dati di autenticazione siano stati immessi dal cliente o da un terzo malintenzionato che ne sia venuto in possesso in maniera illegittima.

In linea generale, esistono malintenzionati che cercano di carpire dati sensibili dai computer degli utenti internet al fine di utilizzarli per scopi illeciti. Questo avviene principalmente attraverso i seguenti strumenti:

- **Virus, worm, trojan horses, malaware, spyware, keyloggers, ecc.**

Si tratta di programmi creati appositamente per "infettare" il computer preso di mira, renderlo vulnerabile agli attacchi posti in essere dai loro creatori e divulgare informazioni personali e sensibili ivi memorizzate. Altra caratteristica peculiare di questi programmi è la loro altissima capacità di diffusione e di replicazione quando il computer è collegato ad una rete informatica. Si diffondono principalmente tramite posta elettronica, siti internet "infettati", chat, siti di scambio files (peer to peer);

- **Phishing**

È una tecnica che indirizza l'utente di servizi on line ad una pagina di accesso identica a quella legittima, al fine di far digitare all'utilizzatore ignaro i propri dati di accesso e carpirli per poi poterli utilizzare per scopi illeciti;

- **Altro ?**

Purtroppo le conoscenze informatiche e il numero di persone che si dedicano a queste attività illecite non consentono di escludere la nascita di nuove tecnologie fraudolente.

Come difendersi da Virus, worm, trojan horses, malaware, spyware, keyloggers, ecc. ?

Il primo consiglio è di rivolgersi a personale qualificato per la installazione, la configurazione e l'aggiornamento del software dei Vostri computer in particolare se utilizzati per scopi professionali. Inoltre:

- 1) Per potersi instaurare e diffondere, questi programmi utilizzano, nella maggior parte dei casi, falle del sistema operativo. È opportuno quindi mantenere sempre **aggiornato il sistema operativo del proprio computer**, attivando gli **aggiornamenti automatici** in genere previsti dal produttore di software.
- 2) Installare e aggiornare almeno settimanalmente un *antivirus* ed un *firewall* (software che impedisce l'accesso al proprio computer da parte di altri utenti internet).
- 3) Installare e aggiornare regolarmente un *antispyware*.
- 4) Tenere un comportamento responsabile nell'utilizzo dei servizi connessi ad Internet. Ad esempio:
 - a. Evitare di aprire messaggi di posta elettronica se non si è sicuri del contenuto/provenienza.
 - b. Evitare di visitare siti dal contenuto palesemente illegale.

Come difendersi dal "Phishing" ?

Per difendersi dal "phishing" è sufficiente collegarsi ai servizi on line esclusivamente tramite la digitazione dell'indirizzo fornito dalla **Banca di Forlì Credito Cooperativo**. Si ricorda comunque che:

- 1) Gli Istituti di Credito non richiedono mai utenze, password o dati personali tramite messaggi di posta elettronica;
- 2) **Non rispondere mai a queste e-mail:** nel dubbio, contattare la Banca che apparentemente Vi ha inviato la comunicazione;
- 3) Qualora il messaggio contenga allegati o un collegamento (link) ad una pagina internet, **non aprire né l'allegato né cliccare sul collegamento** anche su sollecitazioni ad entrare nel sito della Banca per urgenti comunicazioni, in quanto potrebbero condurre entrambi ad un sito contraffatto;
- 4) Diffidare ancor di più se il **messaggio** contiene argomenti intimidatori: per esempio, in caso di mancata risposta, sospensione del "codice utente";
- 5) **Se per errore avete inserito i Vostri dati, provvedete a bloccare i codici chiamando le filiali della Banca.**

Protegete i Vostri codici di accesso ai servizi bancari

Che cos'è il "phishing" ?

Il meccanismo è semplice: consiste nel ricevere una comunicazione, apparentemente da parte della Banca del cliente (nella maggior parte dei casi tramite la posta elettronica), nella quale vengono richiesti i dati personali tramite un modulo incluso nella e-mail stessa o tramite un collegamento (link) ad una pagina internet (che può essere simile a quella della Banca).

Come giustificazione a questa comunicazione, vengono riportate problematiche tecniche non meglio precisate, offerte commerciali, ecc...

Inserendo i propri dati, l'ignaro cliente finisce per svelare "codice utente" e "password" che possono essere così utilizzati dai pirati informatici per compiere operazioni illegali.

Il fenomeno è particolarmente insidioso perché i messaggi, nella maggior parte dei casi, sembrano effettivamente inviati da Banche molto note, in modo tale da non sollevare sospetti nel destinatario.

Come proteggersi ?

Sfuggire a questi "attacchi" è, di contro, piuttosto semplice.

Di seguito, alcune indicazioni di carattere generale:

1. Gli Istituti di Credito non richiedono mai utenze, password o dati personali tramite messaggi di posta elettronica
2. **Non rispondere mai a queste e-mail:** nel dubbio, contattare la Banca che apparentemente Vi ha inviato la comunicazione
3. Qualora il messaggio contenga allegati o un collegamento (link) ad una pagina internet, **non aprire né l'allegato né cliccare sul collegamento** anche su sollecitazioni ad entrare nel sito della Banca per urgenti comunicazioni, in quanto potrebbero condurre entrambi ad un sito contraffatto.
4. Diffidare ancor di più se il **messaggio** contiene argomenti intimidatori: per esempio, in caso di mancata risposta, sospensione del "codice utente".
5. Se per errore avete inserito i Vostri dati, provvedete a **bloccare i codici** chiamando le filiali della Banca.