

# GINO E MARGHERITA

in

## Dal denaro reale al denaro virtuale

### Decalogo della sicurezza on line

Con qualche piccola attenzione è possibile riconoscere le truffe che arrivano via e-mail e gli altri stratagemmi escogitati dai pirati informatici per carpire informazioni sui nostri conti on line.

Ecco un breve decalogo di regole da seguire per dormire sonni tranquilli:

1. **Diffida di qualunque e-mail ti richieda l'inserimento di dati riservati** riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o informazioni personali. La tua banca, infatti, non richiederà mai tali informazioni via e-mail.
2. **Le e-mail truffaldine di solito non sono personalizzate** e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (come scadenza, smarrimento, problemi tecnici eccetera); fanno uso di toni "intimidatori" (per esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente); promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione; non riportano una data di scadenza per l'invio delle informazioni.
3. **Nel caso in cui tu riceva e-mail con richieste di questo tipo, non rispondere** ma informa subito la tua banca tramite il call center o recandoti in filiale.
4. **Non cliccare su link presenti in e-mail sospette**, in quanto questi collegamenti potrebbero condurti a un sito contraffatto, difficilmente distinguibile dall'originale. Diffida inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, in particolare quelli con il simbolo @.
5. **Quando inserisci dati riservati in una pagina web, assicurati che si tratti di una pagina protetta**: queste pagine sono riconoscibili in quanto l'indirizzo comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto. Per controllare l'autenticità della connessione sicura puoi fare doppio click sul lucchetto in basso a destra e verificare la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale.
6. **Diffida se improvvisamente cambia la modalità con la quale ti viene chiesto di inserire i codici di accesso all'home banking**: per



## **GINO E MARGHERITA** in

### **Dal denaro reale al denaro virtuale**

esempio se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (nuove finestre). In questo caso, contatta la vostra banca tramite il call center o recandoti in filiale.

7. **Controlla regolarmente gli estratti conto del conto corrente e della carta di credito** per assicurarti che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contatta la banca e/o l'emittente della carta di credito.
8. **Le aziende produttrici dei browser (i programmi che permettono di navigare in Internet) permettono di scaricare gratuitamente gli aggiornamenti del software (le patch) che incrementano la sicurezza** dei browser stessi. Sui siti di queste aziende è anche possibile verificare che il tuo browser sia aggiornato; in caso contrario, ti consigliamo di scaricare e installare le patch appena si rendono disponibili.
9. **Tieni sempre aggiornato il software antivirus.** In questo modo impedirai a e-mail o siti di phishing di installare sul computer , senza che tu te ne accorga, un "codice malevolo" atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Usa inoltre un software firewall per proteggere il traffico in entrata e in uscita dal tuo PC.
10. **In caso di dubbio, rivolgiti alla tua banca!**

