



 Consulta le altre guide della nostra raccolta!

servizi.po.cariscom.it/servizioclienti/nuoveguide.asp

ABI Lab

 Tecnologia utile

Un'opportunità. Sicuramente!

Home Banking



3 • Cosa fare

3.1. Proteggi il tuo PC

Ecco alcuni consigli che ti permettono di mettere il tuo PC al riparo da sguardi indiscreti:

1. Difendi da virus e spyware il PC dal quale effettui le operazioni di home-banking installando e mantenendo aggiornati opportuni **software di protezione (anti-virus, anti-spyware...)** ed effettua scansioni periodiche.
2. Tieni costantemente aggiornati il sistema operativo e gli applicativi del tuo PC, mediante l'installazione delle cosiddette **patch** ("toppe" di protezione). Scarica sugli aggiornamenti ufficiali, disponibili sui siti delle aziende produttrici.
3. Proteggi il traffico in entrata e in uscita dal tuo PC mediante l'installazione di opportuni programmi di filtraggio del flusso di dati, denominati **firewall**.
4. Durante la navigazione in Internet, non permettere che vengano eseguite attività da remoto senza la tua autorizzazione e consenti l'**installazione dal web dei soli programmi di cui è possibile verificare la provenienza**.
5. Spesso il contagio implica una modifica improvvisa delle impostazioni di sistema o un **peggioramento delle prestazioni generali** (es: rallentamento, apertura di finestre non richieste...). Tali cambiamenti possono essere indici di sospetta infezione.

6. Verifica l'**autenticità della connessione** con la tua banca, mediante il controllo accurato del nome del sito nella barra di navigazione. Ove presente, è opportuno cliccare due volte sull'icona del lucchetto (o della chiave) presente nella finestra di navigazione e verificare la correttezza dei dati che vengono visualizzati.



ABI Lab

 Tecnologia utile

6

3.2. L'importanza della prevenzione

Ecco alcune semplici regole comportamentali di prevenzione che ti permettono di non cadere nelle trappole più comuni.

1. Diffida di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali. **La tua banca non richiederà mai tali informazioni.**
2. Se vuoi connetterti al sito della tua banca, **scrivi direttamente l'indirizzo nella barra di navigazione. Non cliccare su link presenti in e-mail sospette**, in quanto questi potrebbero condurti a un sito contraffatto, molto simile all'originale.

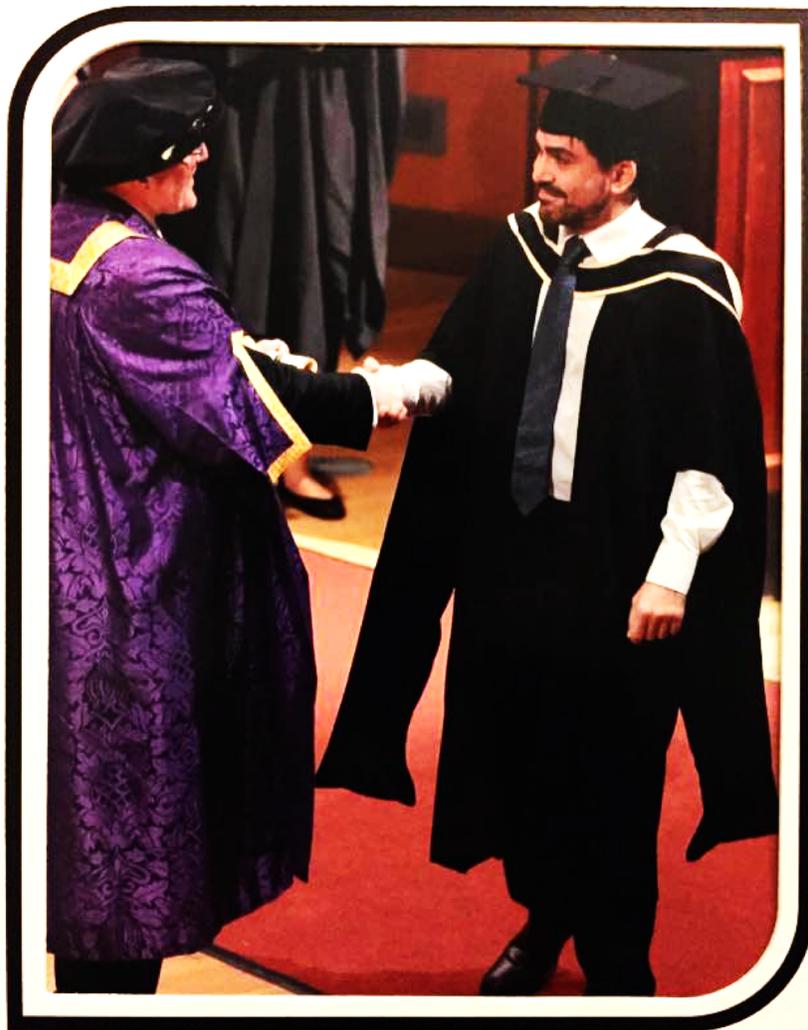
3. **Controlla regolarmente le movimentazioni del tuo conto corrente** per assicurarti che le transazioni riportate siano quelle realmente effettuate.

4. **Diffida di qualsiasi messaggio** (proveniente da posta elettronica, siti web, contatti di instant messaging, chat o peer-to-peer) **di rivolga l'invito a scaricare programmi o documenti di cui ignori la provenienza.**

5. **Presta attenzione se riscontri anomalie** rispetto alle abituali modalità con cui ti viene richiesto l'inserimento dei dati personali sul tuo sito di home-banking.

6. Internet è un po' come il mondo reale: come non daresti a uno sconosciuto il codice PIN del tuo bancomat, allo stesso modo **non consegnare i tuoi dati senza essere sicuro dell'identità di chi li sta chiedendo**. In caso di dubbio, rivolgiti alla tua banca!





Royal Holloway, University of London





MAR GLACIALE ARTICO

MAR GLACIALE ARTICO

MAR GLACIALE ARTICO

CANADA

STATI UNITI

Groenlandia

RUSSIA

OCEANO PACIFICO SETTENTRIONALE

OCEANO ATLANTICO SETTENTRIONALE

OCEANO



BRASILE

HERIDIONALE

OCEANO ATLANTICO MERIDIONALE

INDIA

AUSTRALIA

OCEANO PACIFICO MERIDIONALE

OCEANO ANTARTICO

OCEANO ANTARTICO

OCEANO ANTARTICO