

La protezione del tuo PC.

I nostri Servizi via internet sono sicuri, ma con la tua collaborazione potrai avere un PC sempre protetto. Ecco alcune buone regole da tenere in mente.

1) Presta sempre attenzione alle email sospette.

Verifica sempre il mittente di email sospette e, anche se conosciuto, diffida da quelle che contengono messaggi generici e non personalizzati.

Nel caso in cui ti sia richiesto di cliccare un link, prova ad accedere al sito indicato digitando direttamente l'indirizzo nella barra degli indirizzi del browser e in ogni caso, diffida da link che prevedano l'inserimento di password.

Presta attenzione se si riscontrano anomalie rispetto alle abituali modalità con cui viene richiesto l'inserimento dei dati personali sul sito dei Servizi via internet.

2) Non installare software e non aprire nessun file di cui non conosci la provenienza.

3) Non effettuare il salvataggio automatico delle password.

Nel caso in cui la funzione di completamento automatico delle password fosse già attiva, è sufficiente rispondere "no" alla richiesta di salvataggio delle password.

Per disabilitare e cancellare le password già salvate:

- con Internet Explorer:

- clicca sulla funzione Opzioni Internet nel menù Strumenti;
- nella cartella Contenuto, clicca sul tasto Completamento Automatico;
- elimina la selezione da Nome utente e password sui moduli;
- cancella i dati precedentemente memorizzati cliccando sui tasti Cancella Moduli e Cancella Password;
- completa l'operazione cliccando il tasto OK su tutte le finestre precedentemente aperte.

- con Firefox:

- clicca sul menù Strumenti ed attivare Opzioni;
- clicca quindi sulle voci Privacy, Impostazioni e seleziona Password salvate;
- premere OK per chiudere la finestra di opzioni.

4) Proteggi sempre il tuo PC con software antivirus e anti-intrusione.

Un Antivirus è un ottimo strumento per stare al sicuro da tentativi di intrusione e virus. Ricordati di effettuare nel tempo i vari aggiornamenti segnalati dal produttore stesso anche nel suo sito.

5) Controlla il livello di protezione del sito prima di comunicare codici e dati personali.

Prima di inserire codici personali, password e numeri di carta di credito, verifica sempre che la trasmissione dei dati sia protetta.

Controlla che nella barra dell'indirizzo del sito sia presente il prefisso **https://**. Puoi inoltre verificare se il protocollo di sicurezza SSL a 128 bit, che protegge la trasmissione dei dati, sia attivo controllando la presenza di un **lucchetto chiuso** in basso a destra sulla finestra del browser internet (basta cliccare sul lucchetto).

6) Evita programmi di condivisione file su internet (file sharing, peer to peer).

Condividere i propri file attraverso internet potrebbe permettere l'accesso al computer anche ad "ospiti" indesiderati, che potrebbero carpire altre informazioni oltre a quelle che avete deciso di condividere.

Truffe on line, come difendersi.

Il phishing.

Il phishing, senza violare i sistemi di sicurezza della banca, punta a catturare in modo fraudolento i codici di accesso ai Servizi via internet dei clienti.

Ciò avviene attraverso l'invio di una email che sembra provenire dalla banca, in cui si richiede di accedere a un link (che sembra riportare al sito ufficiale della banca) e di inserire i propri codici di accesso. In realtà, seguendo le istruzioni riportate, il cliente si collega al sito del truffatore, che spesso imita quello della Banca, e trasmette le informazioni personali inserite.

Come riconoscerlo.

Ti raccomandiamo di non dare mai seguito a email o telefonate che richiedano di inserire o comunicare i propri codici di identificazione: le nostre politiche non prevedono in alcun caso la richiesta di fornire i tuoi codici di identificazione via email o telefonicamente.

Le email sul phishing spesso riportano errori grammaticali e fanno a volte riferimento a una vincita in denaro o alla scadenza delle password di accesso.

Cosa fare.

Ti invitiamo ad accedere ai Servizi via internet scrivendo sempre l'indirizzo del nostro sito all'interno della barra dell'indirizzo del browser.

Nel caso avessi erroneamente comunicato i codici a seguito di un messaggio di phishing, ti invitiamo a cambiare subito il Codice PIN. Se hai ricevuto email sospette apparentemente provenienti dalla Società, ti invitiamo a contattare immediatamente il **Servizio Assistenza Clienti** o il numero verde **800.825.099**.

Ricorda sempre le **regole per proteggere il tuo PC** e mantieni sempre aggiornato il tuo programma di Antivirus!