

## ***Come proteggersi dal crimeware – Decalogo per i clienti***

È stata rilevata negli ultimi mesi la comparsa nel contesto nazionale di una nuova modalità di furto dell'identità elettronica, legata alla diffusione presso le postazioni dei clienti di *home-banking* di codice malevolo in forma di *spyware* (una tipologia di virus informatico).

Tali virus, denominati *crimeware* per le finalità criminali che ne sono alla base, sono in grado di reperire le informazioni personali disponibili sui PC contaminati e trasmetterle al frodatore, che in seguito le riutilizza per scopi illeciti.

Alcuni accorgimenti possono rivelarsi utili per contrastare la diffusione di tale fenomeno fraudolento. In particolare può risultare utile quanto segue:

1. Proteggete dalle epidemie informatiche il PC dal quale effettuate operazioni di *home-banking* tramite **l'installazione di un software anti-virus**. Alcune aziende producono inoltre uno specifico *software anti-spyware*, che potete addizionalmente installare sul PC.
2. Effettuate **scansioni periodiche** e tenete costantemente **aggiornato il vostro software anti-virus** (ed eventualmente l'*anti-spyware*) verificando costantemente la **disponibilità delle connessioni** verso il sito dell'azienda che lo produce.
3. Tenete costantemente **aggiornata la protezione** del sistema operativo e degli applicativi presenti sul PC, mediante l'installazione delle cosiddette **patch** (letteralmente "toppe", con riferimento alle vulnerabilità che vanno a proteggere), che vengono rilasciate dalle rispettive aziende produttrici. Fate riferimento esclusivamente agli **aggiornamenti ufficiali**, disponibili gratuitamente sui siti Internet delle stesse aziende.
4. **Protegete il traffico dati in entrata e in uscita** dal vostro PC mediante l'installazione di opportuni strumenti di filtraggio delle comunicazioni, denominati **firewall**.
5. Durante la navigazione in Internet, limitate la possibilità che vengano eseguite **attività da remoto senza la vostra autorizzazione** e consentite l'installazione dal web dei soli programmi di cui è possibile verificare la provenienza.
6. Spesso l'**avvenuto contagio** si traduce anche in una modifica non richiesta delle impostazioni di sistema e in un peggioramento delle sue prestazioni generali (es. rallentamento, apertura di *pop-up* non richiesti). Monitorate opportunamente tali cambiamenti come indici di sospetta infezione.
7. Diffidate di qualsiasi messaggio (proveniente da posta elettronica, siti *web*, contatti di *instant messaging*, *chat* o *peer-to-peer*) vi rivolga l'invito a scaricare **programmi o documenti di cui ignorate la provenienza**.
8. Prestate attenzione se riscontrate **anomalie** rispetto alle abituali modalità con cui vi viene richiesto l'inserimento dei dati personali **sul vostro sito di home-banking**.
9. **Verificate l'autenticità della connessione con la vostra banca**, mediante il controllo accurato del nome del sito. Ove presente, è opportuno inoltre cliccare due volte sull'icona del lucchetto (o della chiave) presente in basso a destra nella finestra del *browser*, per verificare la correttezza dei dati relativi al certificato del sito cui ci si sta connettendo.
10. **Controllate regolarmente gli estratti conto** del vostro conto corrente per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario contattate la vostra banca.