Frodi on line... nuove truffe in agguato!!!

Riteniamo che solo conoscendo le varie tipologie di truffa ci si possa difendere, e per tale motivo, desideriamo informarti sulle più nuove e le più diffuse modalità adottate dagli hacker informatici.

Una nuova truffa in agguato: Man in the Browser!

Ad affiancare il phishing, il pharming e il crimeware una nuova truffa!

In sintesi un nuovo trojan (un piccolo software denominato **Karber**), durante la normale attività di navigazione attraverso siti non sicuri, si inserisce sui computer degli utenti e si attiva nel momento in cui l'utente effettua un bonifico bancario online o un'altra operazione di pagamento dal proprio conto. Karber cambia l'importo ed il beneficiario dell'operazione.

Non temere ... anche da questa truffa ci si può difendere, osservando poche e semplici regole:

- installa software di protezione per PC (antivirus, antispyware, ecc.);
- mantieni aggiornati tali software (antivirus e antispyware) ed esegui controlli periodici per identificare possibili file infetti, rimuovendoli;
- verifica al termine di ogni operazione che i dati visualizzati ex-post coincidano con quanto disposto (codice IBAN del beneficiario e importo).

Ricordiamo di seguito i più famosi e ormai conosciuti Phishing, Pharming e Crimeware.

Il **PHISHING** è un tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, ad esempio numeri di carta di credito, username e password per l'accesso ai sistemi di pagamento on line, coordinate bancarie e così via.

Gli autori delle frodi sono in grado di inviare milioni di messaggi fraudolenti ad indirizzi di posta elettronica casuali ricavati dalla "rete" . Tali messaggi in apparenza sembrano provenire da siti web sicuri, come la tua banca o la società di emissione della carta di credito, ma in realtà sono sofisticate imitazioni che hanno il solo scopo di carpire dati personali per un successivo utilizzo illecito.

Spesso tali e-mail:

- non sono personalizzate e contengono un messaggio generico di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici, aggiornamento archivi, ecc.);
- fanno uso di toni 'intimidatori', ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente.

Ciò che sorprende e che talvolta convince i malcapitati è l'elevato livello di contraffazione dei marchi inseriti nel corpo della mail.

Il **PHARMING** è un tipo di frode ancora più occulta ed ingannevole. L'hacker in questo caso realizza pagine web identiche a quelle di siti già esistenti in modo che l'utente sia convinto di trovarsi nel sito ufficiale del fornitore di servizi a cui si è collegato.

Quando l'utente inserisce le credenziali di accesso, queste vengono carpite per successivi usi fraudolenti.

La sostituzione della pagina autentica con quella falsa avviene attraverso il cambio dell'indirizzo di collegamento effettuato da un virus presente sul PC attraverso il quale ci si è connessi ad internet.

In questo caso a tradire i malfattori sono proprio gli indirizzi di connessione spesso strani e chiaramente non riferiti al servizio che si sta usando, accompagnati talvolta da difformità nella grafica e nei testi originali.

Il **CRIMEWARE**, termine ottenuto dalla fusione delle parole crime (crimine) e software, definisce una modalità di furto di identità elettronica legata alla contaminazione delle postazioni degli utenti di home banking con specifiche tipologie di virus informatici che infettano il PC nel corso della navigazione su siti "strani" od effettuando il download di file da siti non certificati.

Tali tipologie di virus (spesso denominate spyware o trojan) possono reperire autonomamente alcune informazioni disponibili sui PC infetti o catturare codici durante la digitazione, trasmettendoli al truffatore.

Per ridurre notevolmente i rischi di frode informatica basta seguire poche e semplici regole che riepiloghiamo di seguito:

- **installare ed aggiornare un software di protezione** (antivirus, antispyware, ecc,);
- **mantenere aggiornato un apposito programma di protezione del proprio PC** (antivirus e antispyware) ed **effettuare controlli periodici per identificare** possibili **file infetti** e **rimuoverli**;
- **tenere costantemente aggiornati il sistema operativo e gli applicativi del proprio PC, mediante l'installazione delle cosiddette patch** ('toppe' di protezione). **Scaricare solo gli aggiornamenti ufficiali, disponibili sui siti delle aziende produttrici**;
- **verificare l'autenticità della connessione con la propria banca, mediante il controllo accurato del nome del sito nella barra di navigazione**. Ove presente, opportuno cliccare due volte sull'icona del lucchetto (o della chiave) presente in basso a destra nella finestra di navigazione e verificare la correttezza dei dati che vengono visualizzati;
- notare eventuali modifiche improvvise delle impostazioni di sistema o un peggioramento delle prestazioni generali (es. rallentamento, apertura di finestre non richieste, ecc.). Tali cambiamenti possono essere indici di sospetta infezione;

E' importante inoltre:

- **non rispondere** mai alle e-mail che contengono **richieste 'sospette'**;
- **non abboccare** alla richiesta di cliccare su fantomatici link per accedere a **siti web bancari**;
- **segnalare** eventuali **mail sospette** che fanno espresso riferimento al **nostro istituto all'indirizzo** canali.innovativi@bcp.it;
- **controllare periodicamente la movimentazione del proprio conto corrente e delle carte di credito e segnalare tempestivamente eventuali anomalie**;

- **diffidare di qualsiasi messaggio** (proveniente da posta elettronica, siti web, contatti di instant messaging, chat o peer-to-peer) **rivolga l'invito a scaricare programmi o documenti di cui si ignora la provenienza**;
- **prestare attenzione se si riscontrano anomalie rispetto alle consuete modalità con cui viene richiesto l'inserimento dei dati personali sul sito di home banking**;
- **variare spesso la password di accesso e la dispositiva** e farlo immediatamente anche se si ha solo un fugace dubbio circa un tentativo di truffa.

Se si pensa di aver già risposto ad una e-mail sospetta fornendo dei dati riservati oppure si è visitato un link riportato nella stessa, occorre segnalarlo immediatamente alla propria filiale e alle forze dell'ordine.
L'uso dell'O.T.P. (One Time Password). riduce di molto il rischio di truffe on line in quanto la password eventualmente "consegnata" al malfattore ha una durata massima di 60 secondi!!!
E' bene ricordare una cosa di fondamentale importanza: **nessun istituto bancario chiederà mai dati e codici personali via e-mail o sul sito. E' sempre una truffa!!**

Infine ... **Da vittime a complici**
Talvolta il percorso completo della frode non si ferma all'acquisizione illegale dei dati personali dei Clienti; itruffatori infatti spesso ricorrono alla collaborazione inconsapevole degli stessi.
Mediante la pubblicazione di falsi annunci di lavoro, che richiedono la sola disponibilità di un conto corrente di appoggio e di un po' di tempo, vengono reclutati complici involontari, il cui compito di fare da tramite e trasferire il denaro all'estero attraverso società di money transfer.
Nel caso in cui il Cliente accetti, nonostante una comprovabile buona fede, diventa responsabile di un'azione di riciclaggio di denaro e come tale perseguibile penalmente. Per evitare di cadere nella trappola, occorre **non accettare mai facili guadagni in cambio della disponibilità del proprio conto corrente per operazioni di trasferimento di denaro di cui si ignora la provenienza!**