Cos'è il *phishing*

Attenzione alle richieste "strane"...

Il phishing è un modo per indurre gli utenti a rivelare con l'inganno informazioni personali o finanziarie attraverso un messaggio di posta elettronica o un sito Web.

Una comune frode tramite il phishing in linea si basa su un messaggio di posta elettronica simile a un avviso ufficiale inviato da un'origine attendibile, ad esempio una banca, una società emittente di carte di credito o un commerciante su Internet di chiara reputazione.
I destinatari del messaggio di posta elettronica vengono indirizzati a un sito Web fraudolento, in cui viene richiesto di specificare informazioni personali, ad esempio un numero di conto o una password. Queste informazioni vengono quindi utilizzate per appropriarsi dell'identità altrui.

Come riconoscere un messaggio di posta elettronica attendibile

Il mittente del messaggio è conosciuto dal destinatario?

Se il messaggio proviene da una persona sconosciuta, prestare massima attenzione e aprire il messaggio solo dopo attenta valutazione. Se il messaggio sembra provenire da una persona conosciuta, insospettirsi qualora l'oggetto risulti strano o inadeguato, oppure gli allegati contengano file di programma, come per esempio *offerta.exe*; infatti gran parte dei virus odierni in circolazione sono in grado di simulare indirizzi di posta elettronica facendo in modo che il messaggi sembri provenire da una persona conosciuta.

Il mittente ci ha già scritto messaggi precedentemente?

Se si conosce la persona o la società che ha inviato il messaggio ma non sono mai stati ricevuti messaggi di posta elettronica in precedenza, verificare il motivo per il quale si è ricevuto il messaggio. Controllare il testo dell'oggetto e il nome file dell'eventuale allegato. Se una qualsiasi parte del testo sembra sospetta, eliminare il messaggio oppure analizzarlo con un software antivirus aggiornato prima di aprirlo.

Era atteso di ricevere messaggi dal mittente?

Se la ricezione non era prevista, inviare un messaggio di posta elettronica distinto al mittente, senza aprire il messaggio per rispondere, e chiedere conferma dell'effettivo invio del messaggio.

L'oggetto del messaggio o il nome dell'allegato è coerente con il messaggio e con il contenuto?

È possibile che un messaggio non previsto il cui oggetto è incomprensibile apparentemente inviato da un amico sia in realtà stato inviato da un virus che simula l'invio con l'indirizzo di posta elettronica dell'amico. I messaggi nel cui oggetto si invita a eseguire un'operazione, ad esempio "Importante! Aprire immediatamente l'allegato!" sono quasi certamente non sicuri ed è pertanto opportuno non aprirli, se non dopo avere effettuato una scansione del messaggio con un antivirus aggiornato.

Cosa fare per proteggersi dal phishing (dal "Decalogo ABI")

Il phishing è una frode informatica ideata allo scopo di rubare i dati personali di un utente (es. chiavi di accesso al servizio di home banking, numero di carta di credito); viene attuato da truffatori che inviano false e-mail apparentemente provenienti da una banca o da una società emittente carte di credito, composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata, che invitano il destinatario a collegarsi tramite un link a un sito Internet del tutto simile a quello della banca e a inserirvi, generalmente attraverso una finestra pop-up che si apre dallo stesso link, le informazioni riservate.

Esempio di phishing: "*Gentile utente, durante i regolari controlli sugli account non siamo stati in grado di verificare le sue informazioni. In accordo con le regole di xxxxxx abbiamo bisogno di confermare le sue reali informazioni. è sufficiente che lei completi il modulo che le forniremo. Se ciò non dovesse avvenire saremo costretti a sospendere il suo account.*"

Ecco alcune semplici regole che possono aiutare gli utenti Internet a non cadere in questo tipo di truffe:

1. Diffidate di qualunque mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali. La vostra banca non richiederà tali informazioni via e-mail.
2. È possibile riconoscere le truffe via e-mail con qualche piccola attenzione; generalmente queste e-mail:
    - non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici)
    - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente
    - non riportano una data di scadenza per l'invio delle informazioni
3. Nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca tramite il call centre o recandovi in filiale.
4. Non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate.
5. Diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @.
6. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto.
7. Diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca tramite il call centre o recandovi in filiale.
8. Controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito.
9. Le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (cosiddette patch) che incrementano la sicurezza di questi programmi. Sui siti di queste aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.
10. Internet è un pò come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat®, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi alla vostra banca!