



Direzione Regionale della Lombardia

*Settore Audit e Sicurezza
Ufficio Sicurezza*

Tentativi di truffa via e-mail Come riconoscerli e difendersi

Recentemente sono stati segnalati dei casi di *phishing*, che coinvolgono direttamente l’Agenzia delle Entrate ed altri Enti ad essa connessi (come ad esempio il caso di Equitalia). Il fenomeno del *phishing* consiste in una attività truffaldina che sfrutta delle tecniche di ingegneria sociale e che mira ad ottenere l’accesso ad informazioni personali con la finalità del furto d’identità o la sottrazione di somme di denaro. Il meccanismo utilizzato si basa su comunicazioni artefatte che sembrano provenire da fonti istituzionali (enti statali o convenzionati, Poste, istituti bancari o assicurativi, solo per citarne alcuni). Solitamente questi messaggi vengono recapitati mediante l’utilizzo della posta elettronica, ma possono pervenire anche tramite SMS o semplici contatti telefonici.

Come riconoscere un messaggio di phishing

- Occorre prestare molta attenzione all’indirizzo e-mail dal quale proviene il messaggio, nonché all’indirizzo e-mail al quale il messaggio invita a trasmettere i dati richiesti. Nei casi di *phishing* più banali si tratta solitamente di indirizzi di posta elettronica non coerenti con il testo del messaggio (riferiti a persone sconosciute registrate presso domini Internet non istituzionali).

Questo sembra il mittente del messaggio, bisogna tenere conto che questo dato è facilmente manipolabile. Un truffatore potrebbe assumere l’identità di una persona con la quale scambiamo abitualmente delle comunicazioni.

Questa è la casella e-mail (esattoria.romaest) al quale verrà spedito il messaggio di risposta con i dati richiesti dal truffatore.

-----Messaggio originale-----
Da: Dott.ssa Rocchi [mailto:esattoria.romaest@googlemail.com]
Inviato: martedì 3 giugno 2008 22.43
A: ROSSI MARIO
Oggetto: Cartella esattoriale n° 002 200400330768173

Questo è il dominio (googlemail.com) presso il quale è residente la casella e-mail del truffatore. La casella “esattoria.romaest” non risiede presso un dominio coerente con l’oggetto del messaggio (nel nostro caso dovrebbe essere equitaliaonline.it), in verità la casella fa riferimento **ad un dominio estraneo a qualsiasi istituzione.**

Fig. n. 1 - L’instestazione di un messaggio di phishing.

Nell’esempio riportato in figura 1 si nota che il mittente del messaggio è la *Dott.ssa Rocchi*, invece, la casella alla quale verrà indirizzata l’eventuale risposta è *esattoria.romaest*, residente presso il dominio Internet *googlemail.com*.

- Altri indizi utili per scoprire un tentativo di *phishing* si possono ricavare da un esame accurato del testo della e-mail. Spesso vi sono grossolani errori di grammatica, di solito viene utilizzato un linguaggio impreciso o un tono colloquiale non conforme ad una comunicazione istituzionale, oppure si fa riferimento ad atti inesistenti o si invita il destinatario ad eseguire procedure inconsuete (vedi esempio in figura 2).

Roma, 03 Giugno 2008

Con la presente si comunica che dai risconti di qu
Dipartimento di Esattoria la Cartella
 002 200400330768173 di euro 655,20 è stata pagata oltre la scadenza
 (come da allegato).

Il pagamento della **cartella unica delle tasse** effectu **pecuniarie**
 la scadenza, per il periodo dal
 1 Aprile al 30 Aprile, è gravato del 5% di pene **pecunarie** (art.3 legge
16 Maggio 1983 n. 77).

Rimane quindi un debito di **euro 32,76** che potrà essere saldato
 direttamente presso i nostri
 uffici o **con bonifico bancario con i dati già in Vostro possesso**.

La invitiamo, altresì, a verificare
 qualora fosse in disaccordo, di
 contattarci presso i Nostri uffici.

Nel rimanere a disposizione per ulteriori chiarimenti, e gradita
 l'occasione per porgere distinti
 saluti.

Dipartimento Esattoria
il Vice Reponsabile
Avv. Romina Rocchi

**Dipartimento di Esattoria?
 Non esiste!**

Cartella di pagamento

pecuniarie

**La legge alla quale si riferisce il
 testo non esiste!**

**Esiste veramente un Avv. Romina Rocchi presso
 l'istituzione dalla quale proviene la comunicazione?**

**Il meccanismo della truffa consiste nel richiedere il versamento di somme
 modeste (es. 32,76 euro) tramite bonifico bancario (metodo comodo e
 veloce) sul conto corrente di un prestanome (a volte inconsapevole).**

Fig. n. 2 - le incongruenze riscontrabili nel testo del messaggio.

- Nei casi di *phishing* più sofisticati e mirati, il truffatore può cercare di indurre in errore il destinatario della truffa, inviando un messaggio del tutto identico a quelli che solitamente vengono inviati dagli interlocutori istituzionali. Il truffatore fa affidamento su meccanismi psicologici molto efficaci, ad esempio scrivendo che, per *motivi di sicurezza*, è necessario procedere ad una verifica delle credenziali bancarie, invita il destinatario a connettersi ad un sito Internet tramite un link contenuto nel testo della e-mail. Nel caso in cui si utilizzasse il link messo a disposizione nella e-mail, ci si troverebbe di fronte ad un sito Internet assolutamente identico a quello istituzionale e se si proseguisse nella procedura di autenticazione, inserendo login e password, questi dati verrebbero inoltrati al truffatore. Nella figura 3 viene esemplificato un tentativo di *phishing* di questo tipo a danno di Poste Italiane. Osservando attentamente l'esempio si nota che la veste grafica della pagina è identica a quella autentica, ma l'indirizzo Internet verso il quale si viene indirizzati utilizzando il link fornito nel messaggio non corrisponde a quello delle Poste Italiane.

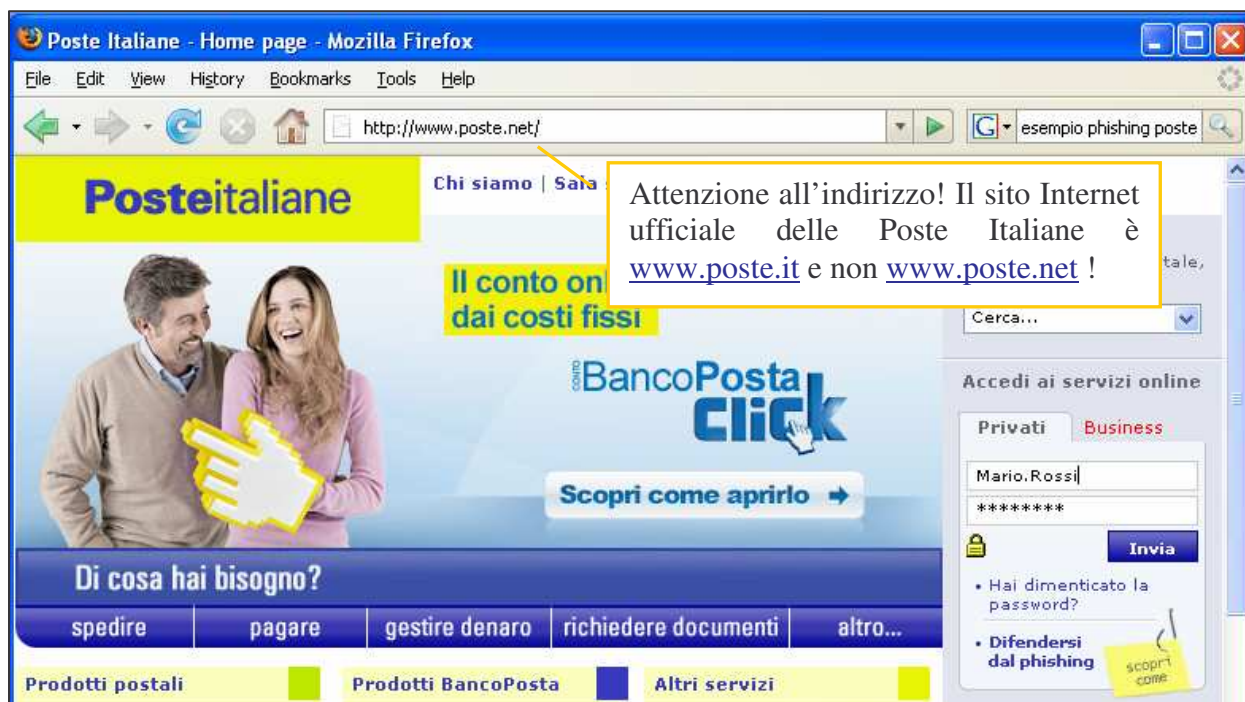


Fig. n. 3 - Falso sito Internet delle poste Italiane.

Anche nei casi più subdoli e sofisticati, il meccanismo della truffa consiste sempre nell'indurre a rivelare dati riservati (ad esempio login e password del proprio account di Banca via Internet, i dati della carta di credito, il pin del bancomat, etc).

Per non cadere vittima di questi tranelli, occorre sempre ricordare che, proprio perché questi meccanismi di truffa sono noti, nessun Ente o Istituzione attua iniziative che potrebbero mettere a repentaglio le informazioni personali dei cittadini. In altri termini, gli istituti bancari, le Poste Italiane, l'Agenzia delle Entrate o qualsiasi altra Istituzione, non richiederebbero mai ad un loro utente di rivelare informazioni riservate (né per e-mail né per telefono), o di versare somme di denaro tramite canali diretti.

E' necessario, dunque, prestare sempre attenzione al tenore dei messaggi che si ricevono e verificare la corretta provenienza degli stessi, tenendo sempre presente che, in caso di dubbio, è preferibile non rispondere, ma attivarsi per ottenere informazioni che sciolgano ogni riserva, piuttosto che rivelare dati che potrebbero venir utilizzati per provocare un danno.

Qualora si sia certi della falsità del messaggio è necessario cancellarlo senza inoltrarlo ad altri, avvertendo l'autorità di polizia competente.