



## PROGETTO DI RICERCA SUL PHISHING

### *REPORT SULL'ANALISI DELLA PERCEZIONE SOCIALE DEL FENOMENO*

**GIUGNO 2006**

Il progetto di ricerca, è iniziato nel settembre 2005 con le prime analisi pilota e si prefigge di analizzare il fattore umano nell'ambito della dinamica delle più diffuse frodi on-line, in particolare rispetto al fenomeno emergente del "phishing". Vengono prese in considerazione le reazioni emotive e comportamentali e la valutazione del rischio da parte degli utenti di internet nonché le caratteristiche delle email che vengono inviate ai cittadini. La finalità dello studio è centrata sulla prevenzione del fenomeno attraverso la progettazione di percorsi di sensibilizzazione mirata.

### STRUMENTI DI RICERCA UTILIZZATI

#### *QUESTIONARIO OFRPO*

Il Questionario strutturato O.F.R.P.Q. (On-line Fraud Risk Perception Questionnaire) dell'ICAA è stato realizzato dal Prof. Marco Strano (ICAA) e dalla D.ssa Roberta Bruzzone (ICAA) e somministrato ad un campione di 5000 utenti di internet. Lo strumento misura, a livello quantitativo, l'incidenza generale del fenomeno phishing in un preciso intervallo di tempo (un mese) in una specifica popolazione, le sue tipologie e la reazione psicologica del soggetto ricevente. Il questionario OFRPO è assolutamente anonimo, è composto da 14 items (più un item di controllo) e da una sezione contenente le informazioni biografiche dell'utente. Il tempo di compilazione è di circa 10 minuti. Il periodo preso in esame per lo studio italiano sul phishing è stato il mese di maggio 2006.

#### *Caratteristiche del campione*

Sono stati selezionati 5000 utenti di internet (50% maschi e 50% femmine) appartenenti a diverse classi di età e occupazioni, provenienti da città italiane di varie dimensioni. Il campione ha visto l'inclusione solo di utenti di internet che utilizzano la posta elettronica almeno una volta al mese, scaricandola sul proprio computer o leggendola direttamente sul web. Le persone intervistate

E' possibile riprodurre integralmente o parzialmente il presente report citando la fonte: ICAA-ANSAIF-ISCOM-SYMANTEC. Progetto di ricerca sul phishing. *Report sull'analisi della percezione sociale del fenomeno*. Giugno 2006.

sono state raggiunte in prevalenza attraverso somministrazioni *random* davanti a centri commerciali ed altri luoghi di aggregazione (università, ministeri, aziende, manifestazioni sportive e culturali ecc.) nonché attraverso la consultazione di mailing list.

### **INTERVISTA SEMISTRUTTURATA O.F.R.P.I.**

Intervista semistrutturata O.F.R.P.I. (On-line Fraud Risk Perception Interview) realizzata dall'ICAA e somministrata ad un campione di 100 utenti di internet estrapolati da quelli a cui è stato somministrato il questionario O.F.R.P.Q.. Lo strumento approfondisce dal punto di vista qualitativo gli atteggiamenti e le reazioni di soggetti che hanno subito un tentativo di frode (*phishing*). Le aree tematiche maggiormente indagate dallo strumento sono sostanzialmente 2: l'efficacia della truffa ("*.....cosa ti ha dato maggiormente sospetto nell'email che hai ricevuto...*") e il livello di fiducia nell'e-banking correlato al tentativo di truffa ("*dopo aver ricevuto l'email di phishing hai ancora fiducia nel sistema e-banking?.....*"). L'intervista ha un tempo di somministrazione di circa 45 minuti e viene condotta da psicologi-criminologi qualificati ed appositamente addestrati. Le interviste sono state realizzate nel mese di giugno 2006.

## **ANALISI DEI DATI (Giugno 2006)<sup>1</sup>**

### *Incidenza del fenomeno*

La percentuale degli intervistati che nell'ultimo mese (aprile/maggio 2006) ha ricevuto delle email di phishing è del **36%**. Il rimanente **64%** non riferisce alcuna ricezione di tale forma di messaggio nell'intervallo di tempo considerato.

### *Reazioni delle vittime*

Il **5%** del campione ha visitato il link indicato dall'email di phishing prima di eliminarla, mentre il rimanente **95%** ha cancellato il messaggio senza visitare il link. Le interviste *OFRPI* hanno poi evidenziato che la maggior parte di coloro che hanno visitato il link lo hanno fatto in maniera abbastanza automatica e per distrazione. Solo una minima percentuale per curiosità. Tra gli intervistati solo **un soggetto** (1 su 1800 soggetti che hanno ricevuto email di phishing tra i 5000 intervistati) ha dichiarato di essere caduto nella trappola comunicando dei suoi dati riservati ma non sembra aver subito poi un attacco al suo conto. I motivi che hanno fatto sì che gli intervistati non siano caduti nella trappola sono diversi. Nel **50%** dei casi il soggetto si è accorto subito da solo che si trattava di un tentativo di truffa. Nel **30%** dei casi invece il soggetto si è reso

---

<sup>1</sup> A cura di M. Strano e R. Bruzzone (ICAA)

E' possibile riprodurre integralmente o parzialmente il presente report citando la fonte: ICAA-ANSSAIF-ISCOM-SYMANTEC. Progetto di ricerca sul phishing. *Report sull'analisi della percezione sociale del fenomeno*. Giugno 2006.

conto dopo averci pensato un pò che si trattava di un'email di truffa. Nel rimanente **20%** dei casi il soggetto ha capito che si trattava di una truffa perché gli è stato fatto notare da qualcuno.

#### *Come le vittime si sono accorte del tentativo di truffa*

Una discreta percentuale degli intervistati **40%** già conosceva il problema phishing ed ha capito che si trattava di un'email di quel genere. Al **15%** è sembrato poco verosimile che la loro Banca/Posta chiedesse via email user-id e password. Al **15%** è sembrato strano che la Banca/Posta italiana scrivesse in inglese. Il **10%** ha fiutato la trappola poiché l'email ricevuta era inverosimile per errori di grammatica, grafica e contenuti. Il rimanente **20%** ha addotto altre motivazioni specialmente per l'incongruenza della richiesta (es. non aveva il conto nella banca che aveva scritto o non aveva fornito alla banca l'indirizzo email).

#### *Caratteristiche delle email di phishing*

Le email di phishing ricevute erano scritte in Italiano nel **65%** dei casi, nel **33%** in Inglese e nel rimanente **2%** in altre lingue. La tipologia di servizi simulati dalle email di phishing che ha ricevuto il campione intervistato si riferiscono ad una Banca italiana nel **30%** dei casi, ad una Banca estera nel **10%**, alle Poste nel **30%**, al commercio elettronico (ebay ecc.) nel **20%** e ad altri servizi nel **10%**.

#### *Segnalazione del problema da parte della vittima*

A seguito della ricezione dell'email di phishing una percentuale del **45%** degli intervistati non ha informato nessuno dell'evento. Il **38%** si è invece confidato con dei colleghi di lavoro o dei conoscenti. Il **15%** ha informato la propria banca o le Poste dell'accaduto mentre il rimanente **2%** ha informato le Forze di Polizia con varie modalità.

#### *Valutazione del tentativo di truffa da parte della vittima*

Il **55%** del campione ha valutato il tentativo di truffa come sufficientemente astuto e verosimile ma non abbastanza per ingannarlo. Il **30%** lo ha giudicato goffo e improbabile per tutti. Il **15%** degli intervistati ha giudicato il tentativo di truffa molto astuto e verosimile e di non esserci caduto solo per caso

#### *Modifica livello di fiducia nel sistema di e-banking*

Il **60%** degli intervistati ha riferito che il fenomeno phishing non ha particolarmente influenzato la loro fiducia nel sistema bancario/postale/commerciale via internet. Il **15%** degli intervistati invece ha affermato di aver in parte perduto fiducia nel sistema dopo il manifestarsi del fenomeno. Circa il **24%** degli intervistati ha riferito che non nutriva molta fiducia nel sistema e-banking ed e-commerce neanche prima dell'avvento del

fenomeno phishing. Infine, lo **0,3%** del campione ha affermato di aver perso fiducia nel sistema dopo aver ricevuto delle email di phishing.

#### *Quantificazione del fenomeno phishing*

Il campione intervistato ha fornito una stima sommaria sul numero totale di email di phishing ricevute dall'inizio del fenomeno. Il **40%** del campione afferma di aver ricevuto da 1 a 5 email. Il **30%** da 6 a 10 email. Il **20%** da 11 a 20. Il rimanente **10%** afferma di averne ricevute più di 20.

#### *Conclusioni*

Da una prima analisi dei dati ottenuti dalla somministrazione del questionario e delle interviste, il rischio proveniente dal fenomeno phishing sembra essere in Italia abbastanza ridimensionato. Il numero di soggetti che ha fornito dati personali attraverso i falsi siti è infatti decisamente irrisorio. Sul piano della fiducia nel sistema elettronico i tentativi di truffa on-line sono riusciti ad incidere negativamente su circa il 16% degli intervistati mentre il rimanente 84% ha mantenuto la sua convinzione originaria. La ricerca ha fornito interessanti indicazioni per ridurre ulteriormente i potenziali rischi attraverso la costruzione di un sistema di prevenzione mirato. Nel prosieguo dello studio verranno ulteriormente analizzati i dati in possesso dell'equipe rispetto alle variabili biografiche (età, sesso, professione, area geografica ecc.). Saranno inoltre somministrati altri questionari a più piccoli campioni ad intervalli periodici (mensili) fino alla fine dell'anno in corso, per valutare eventuali variazioni di incidenza del fenomeno.

## QUESTIONARIO PER LA RILEVAZIONE DELL'INCIDENZA DEL PHISHING

ON-LINE FRAUD RISK PERCEPTION QUESTIONNAIRE – M. STRANO, R. BRUZZONE 2005 (ICAA)

Come è noto, negli ultimi tempi sono giunte agli utenti di internet delle email che invitano a collegarsi ad un sito di una banca o delle Poste o di e-commerce e di inserire l' user-id (nome utente) il numero pin (la password) per controllare che tutto funziona bene. In realtà si tratta di truffe poiché il sito della banca è finto, realizzato dai truffatori che sperano così, ottenuti i dati dell'utente, di svuotare il conto. Tale tecnica è stata denominata "phishing". La preghiamo di aiutarci in questa ricerca che tenta di misurare tale fenomeno criminale compilando il seguente questionario anonimo (NON FIRMARE). Grazie per la collaborazione.

**Nell'ultimo mese, ha ricevuto delle email di phishing?**

- Sì
- No

**In che lingua erano scritte in prevalenza le email di phishing ricevute (una sola risposta)?**

- Italiano
- Inglese
- Altre lingue

**Ha visitato il link indicato da qualche email di phishing prima di eliminarla?**

- Sì
- No

**È caduto nella trappola comunicando dei suoi dati riservati?**

- Sì
- No

**Non sono caduto nella trappola perché (una sola risposta):**

- mi sono accorto subito da solo che si trattava di un tentativo di truffa
- mi sono accorto dopo averci pensato un pò che si trattava di un'email di truffa
- mi è stato suggerito da qualcuno

**Se si è accorto subito della truffa, perché? (indichi una sola risposta: la causa primaria)**

- Conoscevo il problema del phishing e ho capito che si trattava di un'email di quel genere
- Mi è sembrato strano che la mia Banca/Posta mi scrivesse in inglese
- Mi è sembrato poco verosimile che la mia Banca/Posta mi chiedesse user-id e password
- L'email ricevuta era inverosimile per errori di grammatica, grafica e contenuti
- Per altri motivi: \_\_\_\_\_

**Se è caduto nella trappola, ha subito qualche danno finanziario?**

- Sì
- No

**Che tipologia di servizi simulavano le email di phishing che ha ricevuto (può dare più di una risposta)?**

- Banca italiana
- Banca estera

- Poste
- Commercio elettronico (ebay ecc.)
- Altro \_\_\_\_\_

**Ha informato qualcuno della ricezione dell'email di phishing (può dare più di una risposta)?**

- No, nessuno
- Sì, la mia banca
- Sì, le forze di polizia
- Sì, dei miei colleghi di lavoro e dei conoscenti

**Come ha valutato il tentativo di truffa (una sola risposta)?**

- goffo, improbabile per tutti
- sufficientemente astuto e verosimile ma non abbastanza per ingannare me
- molto astuto e verosimile e solo per caso non ci sono caduto

**Dopo aver ricevuto un'email di phishing, ha perso fiducia nel sistema bancario/postale/commerciale via internet (una sola risposta)?**

- Sì
- No
- In parte
- Non avevo fiducia neanche prima

**Sarebbe in grado di quantificare, da quando è iniziato il fenomeno, quante email di phishing ha ricevuto?**

- 0-5
- 6-10
- 11-20
- più di 20

## **INFORMAZIONI BIOGRAFICHE**

**ETA'** \_\_\_\_\_

### **SESSO**

- MASCHIO
- FEMMINA

**PROFESSIONE** \_\_\_\_\_

**TITOLO DI STUDIO (LIVELLO E SETTORE)**

---

NB: è possibile l'utilizzazione dello strumento OFRPQ dietro specifica autorizzazione degli autori