

Codice Attività: TS 3015

CENTRALE DI ALLARME PER ATTACCHI INFORMATICI (Pos. 2603/3015)

Scheda di segnalazione sul Phishing

Si fa riferimento alla lettera circolare ABI TS/004496 del 12/09/03 inerente la costituzione della “Centrale d'allarme per attacchi informatici”.

Vista la rilevanza assunta sia su scala nazionale che internazionale da un nuovo tipo di frode informatica, denominata Phishing, si rimette in allegato la relativa scheda di segnalazione. La stessa comunicazione è stata trasmessa tramite e-mail alla lista di contatti della Centrale di allarme in data 16/12/2004.

La scheda di segnalazione contiene inoltre due decaloghi comportamentali che descrivono possibili contromisure che il cliente e la banca possono valutare al fine di limitare i danni e contenere l'espansione di tale fenomeno.

Si rammenta che l'obiettivo della Centrale di allarme è la costituzione di un presidio atto a individuare e contrastare gli attacchi ai sistemi informatici e telematici cui è affidata la continuità dell'attività bancaria e dei servizi resi dalle banche.

A tal fine le banche che non abbiano ancora indicato un proprio rappresentante per la lista di contatti o che desiderino aggiornare il riferimento attuale, possono comunicare via e-mail - all'indirizzo ts@abi.it - il nominativo della persona prescelta, la sua funzione e i suoi riferimenti e-mail e telefonici (fisso e mobile).

Allegato: Scheda di segnalazione sul Phishing

OGGETTO - PHISHING

Comunicazione del: 14/12/04

Identificativo	0004
Data	Scoperta: 29/01/04 aggiornata: 14/12/04
Denominazione:	Acquisizione per scopi illegali di dati personali di clienti di banche e organizzazioni finanziarie attraverso una finestra apribile da una e-mail.
Tipologia:	Frode on line
Risorse minacciate:	Dati di accesso (user ID e password) dei clienti di Internet banking, numeri di carta di credito, identità del cliente

VALUTAZIONE DELLA MINACCIA:

Priorità di intervento:	Bassa
Diffusione:	Alta
Danno:	Medio
Velocità di distribuzione:	Alta

INFORMAZIONI TECNICHE

Nota	<p>Il phishing consiste nella creazione e nell'uso di e-mail e siti web ideati per apparire come e-mail e siti web istituzionali di organizzazioni finanziarie o governative, con lo scopo di raggirare gli utenti Internet di tali enti e carpire loro informazioni personali riguardanti il proprio account, quali le proprie password per accedere a servizi di home banking o il proprio numero di carta di credito. Tali informazioni vengono catturate dai 'phishers' e vengono successivamente riutilizzate per scopi criminali, come frodi finanziarie o furti di identità.</p> <p>Tipicamente, le e-mail di phishing contengono false dichiarazioni finalizzate a creare l'impressione che ci sia una minaccia immediata o un rischio di disabilitazione per l'account della persona cui sono destinate.</p> <p>Da un punto di vista tecnico le e-mail sono in formato HTML e contengono un collegamento nascosto a un sito web contraffatto, che si presenta come se si riferisse al reale sito istituzionale (offuscamento dell'URL).</p> <p>Esistono casi in cui il collegamento inserito nella e-mail fa riferimento ad un sito maligno che funge da 'man-in-the-middle', reindirizzando in real-time al sito istituzionale (benigno) le informazioni che dal cliente gli vengono inviate e viceversa. In tali casi è anche possibile che il sito maligno controlli le finestre pop-up del sito benigno, alterandole e carpendone il contenuto.</p> <p>Altre tecniche di attacco, meno diffuse, consistono nella diffusione di worm che permettono di effettuare 'key-logging' (registrazione dei caratteri digitati dal cliente) o 'screen grabbing' (istantanee della schermata su cui sono state digitate le informazioni sensibili).</p>
-------------	---

CONSIGLI

Per la protezione e la prevenzione	Si riporta di seguito l'elenco delle principali contromisure da applicare al fine di contrastare il fenomeno del phishing. Si rimanda ai decaloghi comportamentali
---	--

	<p>allegati alla scheda per approfondimenti ulteriori. E' opportuno:</p> <ul style="list-style-type: none"> - Evitare per quanto possibile l'utilizzo di pop-up per operazioni che richiedano l'autenticazione e l'inserimento di dati da parte del cliente. - Definire policy stringenti per il contatto del cliente via e-mail. - Dare diffusione di tale tipologia di frode sia all'interno dell'azienda stessa che alla clientela. - Segnalare agli utenti che la banca non prevede la possibilità di richiedere via email la password e quindi che simili richieste non provengono dalla banca. - Predisporre sul sito di Home Banking suggerimenti comportamentali alla clientela. - Dare informazione all'Help Desk clienti affinché possa supportare la clientela su eventuali richieste di informazioni riguardanti tale frode. - Adottare password diversificate per l'ingresso al sistema di home banking e per la conferma delle operazioni dispositive.
--	---

RIMOZIONE

	<p>Essendo un fenomeno esterno al sistema aziendale non è possibile disporre di un mezzo che garantisca la totale rimozione della minaccia. Risulta comunque opportuno:</p> <ul style="list-style-type: none"> - Prevedere un processo di aggiornamento/cambio di userId e password del cliente su richiesta a seguito della perdita della riservatezza di tali dati. - Acquisire tutte le informazioni possibili sulla sessione Internet durante la quale si è verificato l'eventuale accesso dell'utente che ha fraudolentemente acquisito i dati del cliente della banca; - Raccogliere informazioni relative ai domini di partenza delle e-mail di phishing e comunicarle repentinamente alla Polizia Postale e delle Comunicazioni.
--	---

REFERENZE

	<ul style="list-style-type: none"> - AI Software: "Il knowledge discovery per l'individuazione e la prevenzione delle frodi finanziarie", presentazione del Forum ABI Lab, 2-3/12/2004, disponibile sul sito www.abilab.it. - Symantec: "Soluzioni di protezione da spam e phishing", presentazione del Forum ABI Lab, 2-3/12/2004, disponibile sul sito www.abilab.it. - Polizia Postale e delle Comunicazioni: lettera circolare del 29 gennaio 2004 "Segnalazione nuova tipologia di truffa on line" disponibile sul sito www.abilab.it. - www.antiphishing.org: sito ufficiale dell'Anti-Phishing Working Group, organismo statunitense di vigilanza sulle truffe legate al phishing.
--	--

Come proteggersi dal phishing – Decalogo per i clienti

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,...). Il phishing 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. Queste e-mail 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 po' come il mondo reale: come non darestes 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 !

Come proteggersi dal phishing – Decalogo per le banche

Sebbene il fenomeno del phishing sia un tipo di frode che agisce all'esterno del sistema bancario, alcuni accorgimenti possono essere ravvisati, in modo da ridurne per quanto possibile l'incidenza tra i propri clienti. In particolare può risultare opportuno quanto segue.

1. Definire policy aziendali stringenti per il contatto del cliente via e-mail; ad esempio, stabilire i processi autorizzativi e gli indirizzi di posta elettronica abilitati per l'invio di e-mail ai clienti, non utilizzare mai un indirizzo e-mail che non appartiene al dominio web della banca.
2. Pubblicizzare ai dipendenti e ai clienti della banca le policy di utilizzo dell'e-mail; in particolare, evidenziare che in nessun caso la banca chiederà ai clienti informazioni quali chiavi di accesso al servizio di home banking, codici di carte di pagamento o altre informazioni personali via e-mail.
3. Per favorire la massima consapevolezza dei clienti, diffondere le policy di utilizzo del contatto via e-mail della banca attraverso canali diversificati; ad esempio tramite spazi sul sito istituzionale, comunicazioni cartacee, messaggi in filiale,...
4. In caso di e-mail inviate ai clienti, non inserire link a pagine interne del sito istituzionale o a siti esterni, ma rimandare a comunicazioni che si trovano nella home page del sito, in modo che il cliente possa verificare l'autenticità della comunicazione, digitando manualmente l'indirizzo web della banca nella barra degli indirizzi del proprio browser.
5. Aggiungere un ulteriore livello di autenticazione (con password differenziata) per l'esecuzione di operazioni dispositive tramite il servizio di home banking. Si tratta di un ulteriore accorgimento in grado di limitare i danni prodotti da questo tipo di frode.
6. Prevedere un processo di modifica / aggiornamento delle chiavi di accesso al servizio di home banking su richiesta o necessità legata alla perdita della riservatezza di tali dati. Se non è possibile un'immediata modifica delle chiavi di accesso, è opportuno predisporre un servizio di blocco immediato delle chiavi stesse.
7. Non utilizzare pop up per operazioni che richiedano interazione con l'utente, in particolar modo per l'autenticazione e l'inserimento di dati. Il pop up di navigazione è la modalità principale con cui vengono condotte queste frodi e quindi può essere utilizzato come elemento di riconoscimento della frode da parte dell'utente.
8. Predisporre un apposito indirizzo e-mail ed eventualmente un numero telefonico cui i clienti possano rivolgersi in caso di sospetta frode. Può inoltre essere utile costituire una raccolta delle segnalazioni pervenute.
9. Dare informazione all'help desk clienti e al call centre della banca affinché possa supportare la clientela su eventuali richieste di informazioni riguardanti questa tipologia di frode.
10. In caso di rilevazione di un attacco di phishing, informare la Polizia Postale e delle Comunicazioni.