ABI Lab
Tecnologia utile

Polizia di Stato

CONSORZIOCBI
customer to business interaction

Azioni di sensibilizzazione della Clientela Corporate per un utilizzo sicuro dei servizi di Internet Banking

Marzo 2013

Premessa

L'Internet Banking è a oggi tra i servizi web maggiormente utilizzati dalle imprese, con una crescente operatività on line, e la previsione è di un trend positivo e in continuo aumento sia del numero di utenti che della tipologia di servizi cui si fa ricorso.

A fronte dei benefici dell'innovazione tecnologica e del boom di utilizzatori del canale on line per l'accesso ai servizi bancari, è importante tenere conto dei rischi connessi. Per tale motivo, oltre a un'intensa attività di contrasto e prevenzione a opera delle banche e della Polizia Postale e delle Comunicazioni sono state messe in campo numerose azioni di sensibilizzazione degli utenti.

In questo contesto si colloca il presente documento di indicazioni rivolto alla clientela Corporate per un utilizzo sicuro dei servizi di Internet Banking all'interno della propria azienda, al fine di aumentare la consapevolezza sul tema del cybercrime da parte degli utenti. È utile evidenziare il carattere non prescrittivo delle indicazioni riportate, che vogliono essere un utile ausilio per incrementare il livello di sicurezza nello svolgimento delle operazioni di Internet Banking. Tuttavia è necessario che le aziende contribuiscano individualmente a mitigare il rischio di frodi prestando la massima attenzione nello svolgimento delle operazioni e attuando, a seconda del contesto di riferimento, opportune procedure e attività in grado di prevenire il fenomeno.

Tale iniziativa, condivisa con il Consorzio ABI Lab[1], con il Consorzio CBI[2] e con la Polizia Postale e delle Comunicazioni, si pone l'obiettivo di mantenere sempre elevato il livello di informazione e conoscenza degli utenti di Internet Banking rispetto a tutte le misure che si ritiene opportuno mettere in atto al fine di minimizzare il rischio di frodi, in linea con il mandato di tutti i soggetti coinvolti

[1] Il Consorzio ABI Lab è il Centro di Ricerca e Innovazione per la Banca promosso dall'Associazione Bancaria Italiana in un'ottica di cooperazione tra banche e intermediari finanziari, partner tecnologici e Istituzioni. I temi di sicurezza informatica sono trattati all'interno dell'Osservatorio Sicurezza e Frodi Informatiche (www.abilab.it).

[2] Il Consorzio CBI, promosso dall'Associazione Bancaria Italiana, definisce gli standard tecnici e normativi utilizzati dagli Istituti Finanziari per offrire sul mercato il Servizio CBI. Esso governa l'infrastruttura tecnica che consente a tutti i Consorziati di veicolare alla propria clientela i flussi dispositivi, informativi e documentali oggetto del Servizio (www.cbi-org.eu).

Struttura del documento

Le azioni di sensibilizzazione proposte sono di seguito suddivise in tre sezioni, più precisamente sono state classificate in:

a. policy aziendali;
b. indicazioni per la protezione delle postazioni dalle quali viene svolta l'attività di Internet Banking (PC utente);
c. buone pratiche di comportamento dell'utilizzatore dei servizi di Internet Banking.

Nella prima sezione sono riportate policy aziendali e attività di controllo che si ritiene utile implementare all'interno dei diversi contesti aziendali in modo da poter assicurare la maggior sicurezza possibile in fase di accesso ai siti di Internet Banking e di esecuzione delle operazioni informative e dispositive.

La seconda parte comprende utili indicazioni che, se attuate, possono incrementare il livello di sicurezza dei terminali aziendali dai quali viene svolta l'operatività on line. Tali misure di protezione contribuiscono infatti a proteggere le credenziali di autenticazione e, in linea generale, tutti i dati bancari sensibili, in modo da impedire quanto più possibile che eventuali attacchi fraudolenti indirizzati alle aziende Corporate possano andare a buon fine.

La terza tipologia di raccomandazioni comprende tutti quegli accorgimenti che i diversi utenti che svolgono le attività di Internet Banking per conto delle aziende dovrebbero porre in essere, in modo da incrementarne ulteriormente i livelli di sicurezza nello svolgimento delle operazioni. Si ritiene che tali indicazioni siano utili anche a livello generale, ossia fuori dal contesto aziendale, in quanto rappresentano valide prassi operative che ogni soggetto che opera telematicamente potrebbe adottare per garantire il livello massimo di sicurezza disponibile.

A. *Policy aziendali*

Di seguito vengono illustrate le raccomandazioni che si ritiene utile implementare a livello di policy per la clientela Corporate.

a.1 Tra le misure di prevenzione delle frodi che le aziende dovrebbero adottare, in primo luogo **si consiglia di definire e divulgare una policy aziendale in materia di sicurezza informatica relativamente all'utilizzo dei servizi di Internet Banking da parte dei dipendenti designati**. Tale policy dovrebbe comprendere una evidenziazione dei rischi correlati allo svolgimento di un'operazione bancaria in via telematica. Inoltre è opportuno specificare ruoli e relative responsabilità all'interno dell'azienda, compiti specifici e incarichi assunti relativamente alle attività di Internet Banking; nelle policy dovrebbero essere elencati altresì gli strumenti utilizzati dall'azienda, i device e le postazioni da cui è possibile operare, identificando quindi luoghi e punti di accesso alla rete internet da proteggere. Inoltre, **si ritiene opportuno che le policy siano condivise all'interno dell'organizzazione**, e in particolare dettagliatamente illustrate ai responsabili e alle figure incaricate di svolgere le operazioni telematiche.

a.2 In secondo luogo, **si suggerisce di identificare preventivamente gli utenti da abilitare all'utilizzo del servizio di Internet Banking**, definendo una corretta attribuzione dei profili di accesso e delle autorizzazioni concesse per l'uso degli applicativi, **e di individuarne le postazioni dedicate**. In questo modo si consente di abilitare solo alcuni dipendenti all'utilizzo dei canali e degli applicativi aziendali necessari per il corretto svolgimento delle attività, siano esse a fini informativi o dispositivi, limitando in tal modo una circolazione non completamente sicura di dati sensibili e credenziali. Inoltre, attraverso tali accorgimenti, potrà essere più agevole effettuare attività di controllo ex-post sulle operazioni e, in caso di qualsiasi evenienza o anomalia a posteriori, si potrà determinare con riferimento a una specifica attività, quando è stata effettuata, chi l'ha posta in essere, da quale postazione è stata gestita, etc.

a.3 **Si raccomanda** inoltre **di adottare tutti gli strumenti di II fattore** (quali token, smart card, certificato digitale, codici OTP etc.) **messi a disposizione dalla banca** per garantire la massima sicurezza in fase di accesso all'Internet

Banking o di autorizzazione delle operazioni, **consigliando di renderne obbligatorio l'uso a tutti gli utenti secondo le specifiche profilazioni preventivamente definite dall'azienda.** È proprio nelle fasi di accesso e autorizzazione all'operatività on line, infatti, che agiscono i malware (ad es. keylogger, spyware, trojan, etc.) utilizzati dalle organizzazioni criminali per i loro attacchi informatici fraudolenti, al fine di memorizzare le credenziali degli utenti e utilizzarle all'insaputa dei titolari per attività e operazioni illecite. In aggiunta, **è auspicabile attivare l'uso del II canale di comunicazione quando messo a disposizione dalla banca** in modo da avere una corrispondenza sulle operazioni svolte una volta portate a termine. In questo modo è possibile venire a conoscenza, con tempistiche molto rapide, di eventuali operazioni dispositive di Internet Banking non autorizzate, e conseguentemente prendere provvedimenti e attivare tutte le contromisure a disposizione. Tale canale alternativo, da prevedere per ogni operazione o per alcune operazioni ritenute più a rischio sulla base di livelli di tolleranza definiti dalla singola banca, potrà essere reso disponibile all'azienda scegliendo la modalità tecnologica e organizzativa più opportuna in base alle caratteristiche delle diverse realtà Corporate.

a.4 **Si consiglia di avviare iniziative di informazione e/o di formazione interna all'azienda in materia di sicurezza rivolte agli utenti abilitati al servizio di Internet Banking**. Tali attività hanno l'obiettivo di educare e aggiornare i dipendenti abilitati a compiere le operazioni telematiche circa gli aspetti fondamentali di sicurezza relativamente a tali operazioni. **Si consiglia di svolgere periodicamente tali iniziative** attraverso momenti di approfondimento e/o di aggiornamento sui trend in atto e sulle misure di sicurezza da adottare, consentendo eventualmente un confronto tra i vari dipendenti su possibili anomalie riscontrate o sulle prassi operative effettivamente utilizzate nello svolgimento di tali operazioni, con l'obiettivo di incrementare la sensibilità sull'argomento. Si evidenzia infatti l'assoluta necessità di istruire quanto più possibile gli utilizzatori dei servizi di Internet Banking riguardo il tema della sicurezza on line, in quanto eventuali operazioni (anche semplicemente informative) svolte con un livello di attenzione non adeguato o effettuate da postazioni non preventivamente identificate potrebbero rendere di fatto inefficaci le misure di sicurezza previste dall'azienda di riferimento.

a.5 **Si consiglia di verificare giornalmente le movimentazioni bancarie effettuate**, controllando che le transazioni riportate siano quelle realmente svolte. Per tali attività si ritiene efficace far riferimento alla lista movimenti resa

disponibile dalla banca per ogni operazione posta in essere. Tale attività consentirebbe di avere sotto controllo le operazioni dispositive realizzate durante la giornata, in modo da poter controllare ex-post la corrispondenza tra le operazioni preventivamente autorizzate e quanto effettivamente effettuato.

a.6 **Si suggerisce di predisporre delle procedure che definiscano una corretta gestione delle password di accesso per i servizi di Internet Banking, gestendo contestualmente il loro aggiornamento periodico**. **Tale aggiornamento potrà avvenire in modo autonomo o secondo procedura definita dalla propria banca** Con tale semplice pratica, infatti, si riduce il rischio che eventuali profili compromessi vengano utilizzati in maniera continuativa. Tale attività dovrà accompagnarsi a quelle di aggiornamento delle postazioni utilizzate e dei relativi software installati, di seguito descritti, nell'ottica di ridurre sensibilmente il rischio che tali dati vengano utilizzati per scopi illeciti.

a.7 **È auspicabile prevedere attività periodiche di controllo delle postazioni utente abilitate all'accesso ai servizi di Internet Banking, predisponendo altresì procedure che gestiscano correttamente le password di accesso a tali postazioni e il loro aggiornamento periodico**. Mantenere costantemente elevato il livello di sicurezza delle postazioni, infatti, è un'azione rilevante ai fini di una completa prevenzione delle frodi informatiche. Si consiglia quindi di verificare periodicamente i terminali dai quali vengono effettuate le operazioni di Internet Banking, in modo da ridurre quanto più possibile il rischio che vengano infettati da malware.

a.8 **Si consiglia di definire e divulgare procedure che identifichino le modalità di comunicazione tra l'utente abilitato al servizio, la banca e le Autorità competenti** a fronte delle diverse anomalie o degli incidenti riscontrati nell'utilizzo del servizio di Internet Banking. La definizione di tali procedure consente alle aziende di gestire più rapidamente le anomalie/inefficienze riscontrate nello svolgimento delle operazioni, in modo da avere tempestivamente indicazioni su come comportarsi e su come prendere opportuni provvedimenti in relazione a quanto riscontrato. Si suggerisce, a tal proposito, di rendere facilmente accessibili agli utenti abilitati all'utilizzo del servizio di Internet Banking i canali di contatto messi a disposizione dalla banca stessa (numeri di telefono della filiale, numero del contact center, numero verde, casella di posta elettronica, etc.), eventualmente integrando tali informazioni nella Intranet aziendale, e si consiglia altresì di aggiornare

regolarmente i recapiti dei principali utilizzatori dei servizi (e-mail e telefono), in modo che possano essere tempestivamente contattati in caso di anomalie. In particolare, in caso di disconoscimento di operazioni fraudolente, si raccomanda di attivare le procedure previste per la denuncia di quanto accaduto, avviando la comunicazione con le Autorità Competenti (Polizia Postale e delle Comunicazioni). Operando in modo tempestivo e agendo in sintonia con tutti gli attori di riferimento, infatti, è possibile ridurre drasticamente l'esposizione e gli impatti degli attacchi informatici fraudolenti.

B. Indicazioni per la protezione delle postazioni dalle quali viene svolta l'attività di Internet Banking (PC utente)

In questo paragrafo si riportano alcune indicazioni ritenute utili per aumentare il livello di protezione delle postazioni da cui vengono svolte le operazioni bancarie in via telematica.

b.1 **Si consiglia di difendere da virus e spyware i PC dai quali si effettuano le operazioni di Internet Banking installando e mantenendo aggiornati opportuni software di protezione** (anti-virus, anti-spyware, anti-spam, sistemi di protezione del browser, etc.). In questo modo si garantisce la sicurezza dei dati archiviati nelle diverse postazioni e in tutta la rete locale, limitando la possibilità di diffusione di virus o trojan all'interno dell'azienda. Inoltre, aggiornando costantemente i software di protezione, si consente di riconoscere virus e programmi infettati di recente creazione, che altrimenti versioni obsolete non sarebbero in grado di identificare. A tal proposito, è utile effettuare scansioni periodiche di tutti i PC collegati alla rete aziendale, al fine di minimizzare il rischio di diffusione dei malware nella rete. **Si raccomanda in aggiunta di proteggere il traffico in entrata e in uscita dai PC mediante l'installazione di opportuni programmi di filtraggio del flusso di dati** (firewall) **e di non disabilitare le impostazioni di protezione** configurate. In questo modo è possibile vincolare la navigazione e il libero flusso di dati verso la rete web attraverso filtri automatici personalizzati, che possono essere definiti a seconda delle esigenze. In aggiunta, si consiglia di estendere l'adozione di tali accorgimenti anche alla rete Wi-Fi dell'azienda e di proteggere tale rete attraverso password comunicate solo a utenti opportunamente individuati, adottando contestualmente le misure di gestione delle credenziali prima citate.

b.2 Analogamente a quanto evidenziato nel precedente punto, **si raccomanda di tenere costantemente aggiornati il sistema operativo e gli applicativi dei PC mediante l'installazione delle cosiddette patch** ("toppe" di protezione). **È auspicabile, inoltre, scaricare solo gli aggiornamenti ufficiali**, disponibili sui siti delle aziende produttrici, in quanto versioni differenti potrebbero essere compromesse e quindi rendere malfunzionanti i sistemi operativi utilizzati. In questo modo, oltre agli antivirus e gli altri software di

protezione, si mantengono aggiornati l'intero sistema operativo e tutte le sue funzionalità, garantendo che siano supportate versioni successive delle applicazioni installate.

b.3 Si suggerisce di profilare e controllare la navigazione in Internet in base alle specifiche esigenze lavorative, a livello di rete e/o a livello di singola postazione. In quest'ultimo caso, una misura di sicurezza potrebbe essere, a titolo puramente esemplificativo, quella di **limitare la navigazione sul web** (anche ad esempio con ricorso a white list) **o la possibilità di installare programmi dei quali non è possibile verificare la provenienza**. Si consiglia quindi di permettere solo agli amministratori di sistema (e in generale a un numero quanto più limitato di utenti possibile) di compiere azioni di modifica delle configurazioni impostate, in modo da ridurre il rischio che erroneamente vengano apportate variazioni tali da rendere inefficienti le impostazioni di sicurezza precedentemente applicate. Inoltre si ritiene utile, con lo scopo di incrementare la sicurezza, limitare o vietare agli utilizzatori abituali delle postazioni la possibilità di scaricare e installare programmi di cui non è possibile verificarne la provenienza e il relativo livello di sicurezza. In tal senso, si consiglia di impedire che applicazioni scaricate dalla rete o portate dall'esterno tramite hard disk o memorie di massa (es. chiavette USB, memorie degli smartphone, etc.) possano essere installate nelle diverse postazioni e quindi possano circolare liberamente nella rete aziendale senza sufficienti controlli.

b.4 In aggiunta a quanto sopra descritto, **si consiglia di differenziare i profili degli utenti in base alle specifiche esigenze operative** (es. abilitazione a funzionalità informative e/o dispositive) al fine di minimizzare i rischi. Pertanto sarebbe opportuno creare differenti profili di utilizzatori dei terminali dai quali è possibile accedere alla rete aziendale ed effettuare operazioni di Internet Banking, in modo da ridurre il rischio che vengano poste in essere transazioni non autorizzate o che si riduca il livello di protezione delle postazioni e dell'intera rete aziendale. Allo stesso tempo **è auspicabile**, nel configurare le diverse tipologie di profilo utente dei dipendenti dell'azienda, **limitare/eliminare i diritti di "amministratore" sulle singole postazioni**, contrastando la possibilità di installazione di codice malevolo.

b.5 **Qualora non siano state implementate le procedure descritte**, o ci sia particolare necessità per garantire la sicurezza delle credenziali di accesso, **è auspicabile svolgere tutte le movimentazioni bancarie da un PC dal**

quale è particolarmente controllato e profilato l'utilizzo della posta elettronica e la navigazione in rete. In tal modo, si riduce drasticamente il rischio di compromissione dei terminali utilizzati e di sottrazione delle credenziali di accesso all'Internet Banking. Tali postazioni, ovviamente, dovranno essere preventivamente messe in sicurezza attraverso scansioni e installazioni di adeguati e aggiornati software di protezione.

C. Buone pratiche di comportamento dell'utilizzatore dei servizi di Internet Banking

Si illustrano di seguito alcuni utili suggerimenti in merito ai corretti comportamenti che gli utenti di Internet Banking dovrebbero adottare. Tali indicazioni rappresentano delle best practice di carattere generale che ogni individuo che svolge operazioni bancarie on line dovrebbe mettere in pratica al fine di ridurre il rischio che le proprie credenziali vengano sottratte o violate, al di là dello specifico utilizzo per fini aziendali.

Alcuni di questi suggerimenti, tuttavia, sono da considerarsi superflui se l'azienda ha già correttamente profilato i propri utenti e ha opportunamente protetto le postazioni da cui svolgono la loro attività.

c.1 **Si consiglia di diffidare di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'Internet Banking o altre informazioni sensibili**: nessuna banca, infatti, chiederà mai di fornire direttamente tali informazioni. Spesso l'attività fraudolenta comprende azioni nelle quali i frodatori si identificano come dipendenti della banca presso cui il cliente ha acceso i suoi rapporti nel tentativo di sottrargli i propri dati sensibili. Queste azioni, oltre che telefonicamente, vengono compiute anche attraverso ulteriori canali, come gli SMS o le e-mail, inviati allo stesso cliente con l'invito a rispondere inserendo codici o fornendo dati sensibili; inoltre si ritiene utile evidenziare che tali indicazioni vengono spesso fornite a seguito di falsi alert (es. invio di un'infondata notifica riguardo tentativi di accesso fraudolento ai propri dati da parte di terzi).

c.2 **Se si desidera connettersi al sito internet della banca si suggerisce di scrivere direttamente l'indirizzo web nella barra di navigazione**, evitando di cliccare su link presenti in eventuali e-mail anche se apparentemente provenienti dalla banca, in quanto questi potrebbero condurre a un sito contraffatto molto simile all'originale. All'interno delle comunicazioni rivolte al cliente attraverso le quali i frodatori svolgono la loro attività, infatti, viene solitamente inserito un link che riconduce a un sito web, il quale a primo impatto può essere confuso con quello ufficiale della banca, in quanto molto simile. Tuttavia il sito internet potrebbe essere contraffatto o contenere codice

malevolo in grado di memorizzare i dati digitati, per poi utilizzarli in maniera impropria per le attività fraudolente. Si raccomanda quindi di prestare attenzione in caso di anomalie rispetto alle abituali modalità con cui viene richiesto l'inserimento delle credenziali di accesso al sito di Internet Banking. Qualora si riscontrino anomalie riguardo i contenuti presenti nelle e-mail ricevute, o qualora si avverta il dubbio riguardo l'autenticità delle informazioni all'interno delle stesse, si consiglia di segnalare tempestivamente quanto accaduto alla propria banca di riferimento e alle Autorità competenti.

c.3 **Si consiglia di diffidare di qualsiasi messaggio** (proveniente da posta elettronica, siti web, social network, contatti di instant messaging, chat o peer-to-peer) **che rivolga l'invito a scaricare programmi o documenti di cui si ignora la provenienza**. I programmi eseguibili potrebbero essere infettati da virus o codici malevoli che possono compromettere la sicurezza della postazione da cui si opera o dell'intera rete aziendale; analoga considerazione vale per alcuni documenti (come ad esempio falsi documenti amministrativi o altri file in formato word, excel o pdf), che al loro interno possono contenere dei virus nascosti. Qualora non siano presenti in azienda sistemi di protezione tramite firewall o non siano previste limitazioni circa la possibilità di scaricare e installare programmi eseguibili, si consiglia di adottare un approccio quanto più possibile diffidente al riguardo.

c.4 **Si suggerisce di conservare con la massima cura i codici e gli strumenti di accesso al servizio di Internet Banking e di non condividerli con altri soggetti**. La diffusione dei codici personali e delle credenziali di accesso aumenta notevolmente il rischio di subire eventuali attacchi fraudolenti nella misura in cui i terminali da cui operano i destinatari di tale informazione non abbiano lo stesso livello di protezione e di sicurezza delle postazioni aziendali.