Tentativi di truffe online: impariamo a riconoscerli!

Negli ultimi mesi abbiamo ricevuto alcune segnalazioni di **tentativi di frode** nei confronti dei nostri clienti Self Bank, che mirano ad ottenere le credenziali di accesso, i codici dispositivi OTP e l'indirizzo email collegato alla postazione Self Bank.

Si tratta di email/sms che **simulano la provenienza da Banca Marche** e invitano i clienti a collegarsi a un link inserito nel messaggio per aggiornare dati anagrafici o confermare operazioni. In realtà il collegamento è al sito del truffatore, che può così raccogliere dati e informazioni personali.

Per informarvi e per aiutarvi a riconoscere un' email o un sms di phishing, di seguito vi forniamo alcuni esempi sulle tecniche attualmente utilizzate dai malviventi per porre in essere truffe telematiche ai danni dei clienti titolari di Self Bank.

Sono state registrate 3 tipologie di attacco:

1. "EMAIL" DI PHISHING CON INVITO A CLICCARE IN UN LINK

Il cliente (o non cliente della banca) riceve un' email con il logo di Banca Marche o di Nuova Banca Marche con la quale viene invitato a cliccare su un link al fine di certificare il proprio indirizzo email o confermare il proprio conto.

Le email provengono da falsi indirizzi di posta elettronica (*es. informa0@pec.bancamarche.it, informa3@pec.bancamarche.it, servizio@bancamarche.it, noreplay_marche@bancamarche.it*). Chi accetta, riceve una sequenza di videate, sempre dotate di nostro logo, in cui viene chiesto di inserire le credenziali di accesso (utente e password) e più codici dispositivi OTP. Di seguito riportiamo alcuni esempi delle più frequenti email di phishing rilevate:

Esempio email 1

BancaMarche

La informiamo che il suo indirizzo e-mail non risulta ancora certificato secondo la norma ISO/IEC 36003, che e' lo standard di riferimento internazionale per la gestione della sicurezza delle informazioni.

Certifica il tuo indirizzo e-mail entro 24 h.

Clicca QUI per procedere alla verifica.

Coerentemente con gli obiettivi aziendali di trasparenza verso la clientela, attraverso la certificazione, la Banca desidera inoltre fornire un'ulteriore elemento di valutazione dei servizi offerti.

Esempio email 2

-------- Messaggio originale --------
Oggetto: Comunicazioni dalla banca!
Data: Thu, 05 Nov 2015 10:39:43 -0500
Mittente: Banca Marche <servizio@bancamarche.it>

Gentile cliente,
cartella esattoriale nr 99557/2015 procedimento sanzionatorio amministrativo nr 59509/2015 raccomandata in allegato direttamente nella sezione del sito Banca Marche, accedere al sito cliccando qui

Esempio email 3

Da: Banca Marche <informaU@pec.bancamarche.it>
A:
Cc:
Oggetto: Confermare conto
Messaggio | DOCUMENTO BANCA MARCHE.html (3 KB)

Gentile cliente da Banca Marche
Per ragioni di Sicurezza e Protezione,
e per il miglioramento del nostro servizio e necessario confermare il tuo conto.

Si prega di scaricare il file allegato e compilare il modulo

© Banca Marche 2015 - Partita Iva 01574601216

Esempio email 4

-------- Messaggio originale --------
Da: Banca Marche <40nymldncjgvda4@nuovabancamarche.it>
Data: 15/02/2016 20:17 (GMT+01:00)
A: 1
Oggetto: URGENTE: Confermare indirizzo E-Mail.

BancaMarche
Nuova Banca delle Marche SpA

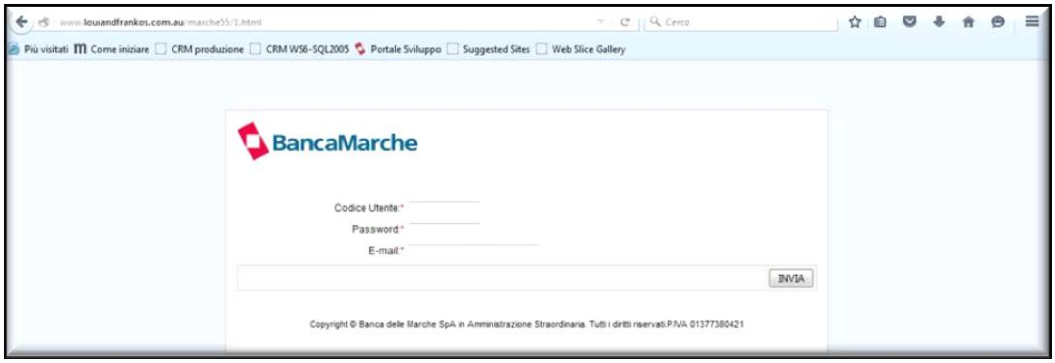
Gentile Cliente,
Confermare indirizzo e-mail.

<<< CLICCA QUI >>>

Al termine la preghiamo di attendere 24 ore prima di accedere nuovamente al suo conto in modo da poter rendere effettivi i nuovi sistemi di sicurezza.
La ringraziamo per la collaborazione.

Nuova Banca Marche ©2016 – P.I. 0115053230360 – Note legali –

Di seguito un esempio delle pagine web utilizzate per catturare le credenziali di accesso ed i codici dispositivi OTP:



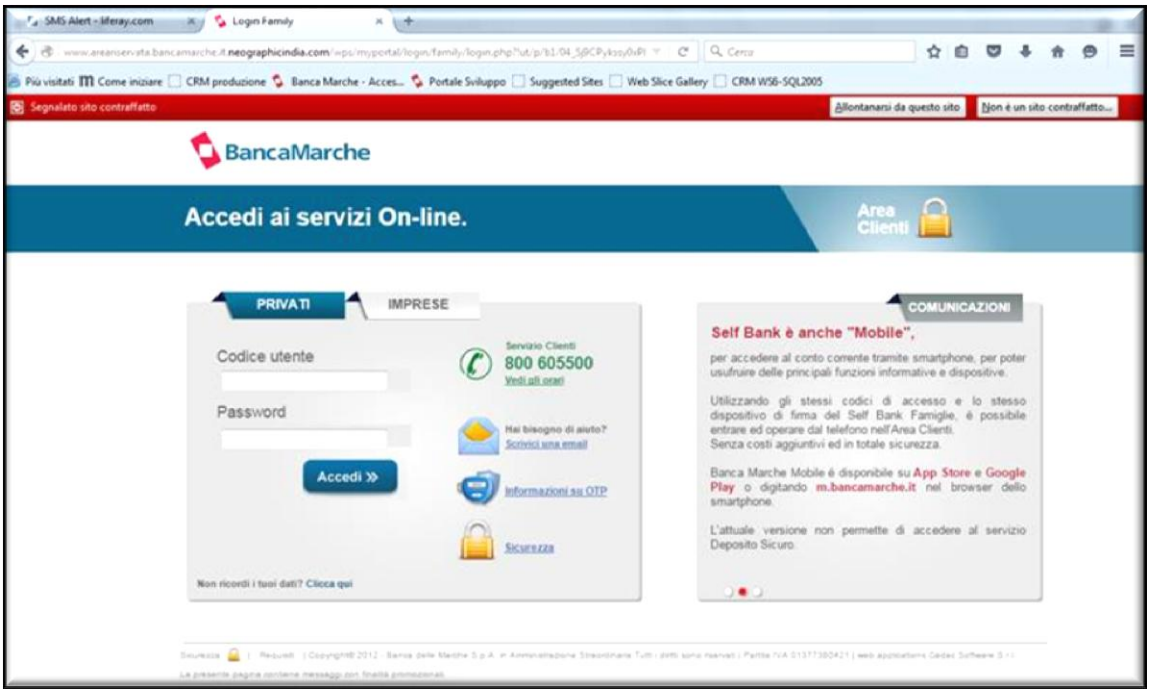
2. “SMS” DI PHISHING CON INVITO A CLICCARE IN UN LINK

Il cliente riceve un SMS su smartphone nel quale viene invitato a selezionare un link che, qualora aperto, reindirizza ad un sito “clone” che riproduce la pagina di accesso all’Area Clienti del Self Bank, sviluppata allo scopo di estorcere le credenziali dei clienti che lo selezionano.

A questo punto si innesca una sequenza di richieste, prima delle credenziali di accesso (utenza e password) e poi dei codici OTP.

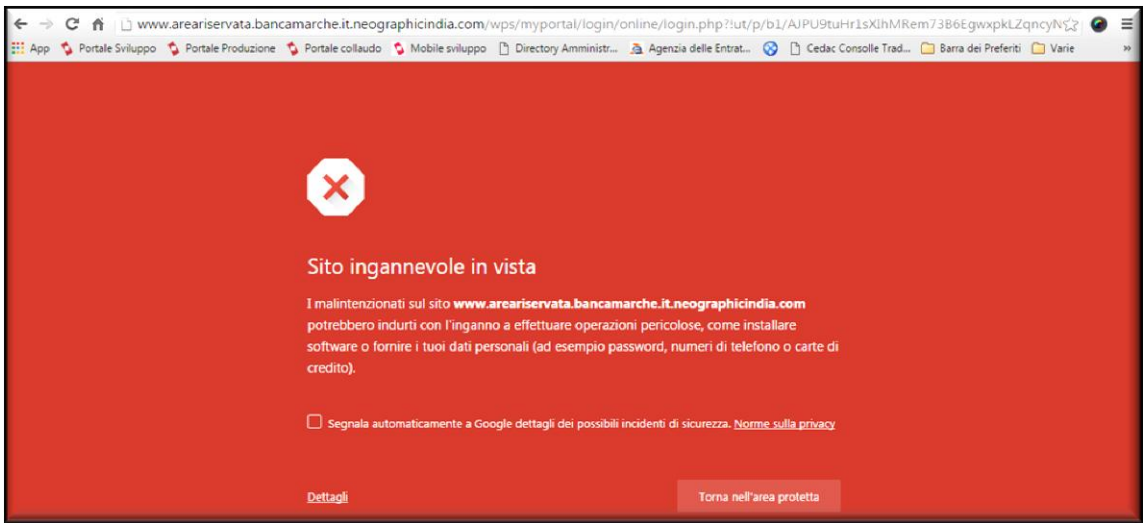
Gli SMS provengono da numeri falsi (*es. 342.4129292*). Questi sono due esempi di messaggi fraudolenti che è possibile ricevere:

ed un esempio di sito clone utilizzato per catturare le credenziali di accesso ed il codice dispositivo OTP:



Segnaliamo che quasi tutti browser, se aggiornati all'ultima versione disponibile, si accorgono della presenza di un sito malevole e avvisano l'utente. Per questo motivo è molto importante mantenere sempre aggiornato il proprio browser.

Di seguito un esempio della pagina mostrata dal browser "Chrome" quando si clicca sul link malevolo. Il browser avvisa il cliente a non proseguire.



Evidenziamo che sia gli indirizzi delle email che spediscono le comunicazioni di phishing, che i siti malevoli su cui si viene indirizzati, hanno sempre una parte consistente del nome che assomiglia a quello di Banca Marche (senza però essere uguale), in maniera tale da trarre più facilmente in inganno. Solo la presenza del "lucchetto" nella barra degli indirizzi (l'indirizzo deve iniziare https://) garantisce sulla comprovata affidabilità del sito.

3. MAN ON THE BROWSER TRAMITE “TROJAN/MALWARE” INSTALLATO SU PC DEL CLIENTE.

Il “man on the browser” è una particolare tipologia di minaccia informatica che si configura come una forma di intercettazione dell’attività “lecita” del cliente, dove l'hacker fa credere al cliente di comunicare con la banca, quando di fatto l'intera comunicazione è controllata da chi esegue l’attacco.

Tale attività fraudolenta è abbastanza rara, avviene a seguito dell’installazione sul pc del cliente di un trojan o malware (virus, software malevoli), che il cliente potrebbe aver acquisito durante la navigazione su siti non attendibili o a seguito dell’apertura di allegati ad email/sms provenienti da mittenti sospetti. In buona sostanza, mentre il cliente accede all’Area Clienti della banca, il malvivente intercetta le credenziali di accesso e l’OTP e li usa per disporre operazioni fraudolente a danno del cliente.

RICONOSCILO PER NON ABBOCCARE!

Il phishing è una tecnica di frode informatica mirata a sottrarre i dati degli utenti attraverso email/sms che imitano le comunicazioni ufficiali della banca e che conducono in realtà a siti contraffatti. Per non rischiare di essere frodato è comunque importante saperlo riconoscere:

Occorre verificare che le email/sms non contengano un messaggio generico di richiesta di informazioni personali (credenziali, carta di credito, etc.).

Diffidare se sono presenti degli errori di ortografia o sono scritte in una forma poco corretta.

Non inserire dati o codici identificativi se è presente un link che riporta ad una pagina esterna

COSA FARE NEL CASO DI RICEZIONE DI EMAIL/SMS SOSPETTI

Qualora si dovessero presentare le situazioni sopra descritte, occorre ignorare o cancellare i messaggi, evitando di provare a dare seguito ad alcuna azione richiesta nel testo del messaggio.

Se si è caduti nella truffa fornendo le proprie credenziali ed i codici OTP, occorre procedere come segue:

- contattare il servizio di Help Desk di Banca Marche al numero verde 800.605500 o all'indirizzo email internet.banking@bancamarche.it,
- procedere con l'immediata bonifica del proprio computer mediante utilizzo di un adeguato programma antivirus, servendosi se del caso del supporto di un tecnico,
- variare tempestivamente la password di accesso (eventualmente anche usando un computer/dispositivo diverso).

RICORDA CHE:

Banca Marche utilizza tutte le misure necessarie per tutelare la sicurezza dei dati e delle transazioni:

- l'accesso all'Area Clienti è protetto da codici identificativi personali che permettono l'autenticazione solo all'utente che ne è in possesso;
- l'utilizzo di alcune funzionalità all'interno dell'Area Clienti e l'invio delle disposizioni alla banca viene consentito solo previo inserimento del "codice numerico OTP", generato da un dispositivo elettronico di firma;
- la riservatezza dell'autenticazione e dello scambio dei dati è garantita dal protocollo TLS che fa uso di una chiave pubblica RSA a 2048 bits. La crittografia è certificata da Verisign/Symantec.

Banca Marche:

- non invia mai email/sms in cui si chiede di inserire la password di accesso, codici di sicurezza delle carte o di compilare moduli per verificare la vostra identità;
- non richiede mai l'inserimento del codice OTP nel box di accesso all'Area Clienti;
- non invia mai email/sms che contengano link ad aree operative del sito o allegati da scaricare;
- l'unica modalità di accesso corretta all'area personale del sito della Banca è quella di digitare nel browser l'indirizzo dell'Area Clienti, controllando che la pagina inizi con "https" e sia presente il lucchetto nella barra degli indirizzi.

SERVIZIO SMS/EMAIL ALERT

Per migliorare la sicurezza dei servizi online in Area Clienti e su Self Bank (anche in versione Mobile) è possibile attivare il servizio di Alert via SMS e/o via Email. L'attivazione del servizio può essere fatta online o richiesta in Filiale.

Il servizio permette di essere tempestivamente avvisato nei seguenti casi:

- accesso all'Area Clienti via Internet o via Banca Marche Mobile;
- cambio della password d'accesso all'Area Clienti;
- operazioni disposte tramite Self Bank o Banca Marche Mobile, in addebito sui conti o sulle carte On Card collegate, sulla base di un livello soglia scelto.

L'avvisatura, se attivata, viene generata per le seguenti operazioni dispositive: Bonifico Italia-SEPA, revoca Bonifico Italia SEPA, Bonifico Estero (funzione non disponibile su Banca Marche Mobile), Ricarica Carta On Card, Trasferimento fondi On Card, Ricarica Carta Eura/MY, Pagamento bollettini postali.

Il servizio di Alert via SMS è a pagamento, con un costo pari a 0,16 euro per ciascun SMS ricevuto (addebitato dalla compagnia telefonica sul credito telefonico, indipendentemente dal piano tariffario). Sono invece gratuiti il servizio di Alert via Email ed l'avvisatura SMS del cambio password.

Proteggi i tuoi dati

Ricorda di variare periodicamente la password e di utilizzare ed aggiornare periodicamente un programma antivirus.

In caso di ricezione di email/sms dubbie occorre segnalarle al Servizio Clienti Banca Marche.

Servizio Clienti

Chiama il numero

800 605500

internet.banking@bancamarche.it