Attenzione al Phishing!

Più Banca.

Il **Phishing è una frode informatica** ideata allo scopo di rubare i dati personali di un utente (es. password e PIN per l'accesso al servizio di Internet Banking, numero di carta di credito) tramite invio di **false e-mail** o tramite **malware** (virus o trojan horse) scaricati o trasmessi all'insaputa mediante scambi di files sul computer.

Truffatori inviano **false e-mail** apparentemente provenienti da una banca o da una società emittente carte di credito, composte utilizzando il logo, il nome ed il layout tipico dell'azienda imitata, nonché domini simili.
Queste e-mail invitano il destinatario a collegarsi tramite un link a un sito Internet del tutto simile a quello della banca e ad inserirvi, generalmente attraverso una finestra pop up che si apre dallo stesso link, le informazioni riservate.

I malware, come **virus o trojan horse**, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Normalmente non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati o trasmessi e vengono scaricati senza saperlo sul computer.

Invitiamo i nostri clienti ISI di:
- **non rispondere ad e-mail sospette**
- **verificare la correttezza del domain www.caribz.it prima di accede all'applicazione ISI**
- **non fornire le proprie credenziali fuori dall'ambiente ISI**
- **proteggere il PC con un antivirus (crimeware)**
- **contattare per qualsiasi dubbio o anomalia la Cassa di Risparmio al numero 840 052 052 o via e-mail all'indirizzo: info@sparkasse.it**

CASSA DI RISPARMIO
SPARKASSE

Esempio Phishing

Più Banca.

Esempio e-mail fraudolenta!

Da: Cassa di Risparmio di Bolzano SpA [mailto:servizi@caribz.it]
Inviato: giovedì 28 ottobre 2010 10.20
Oggetto: Il vostro servizio e scaduto.

Gentile Cliente,

Il vostro servizio Internet Banking e scaduto. Dovete rinnovarlo subito altrimenti il vostro conto verra chiuso.
Se volete usare questo servizio in futuro, dovete procedere subito.
Per continuare, clicca qui.

Registratevi con il vostro conto Internet Banking e seguite i passaggi necesari.

Vi ringraziamo,
Cassa di Risparmio di Bolzano SpA

Cliccando quì l'utente viene indirzzato sul sito clonato.

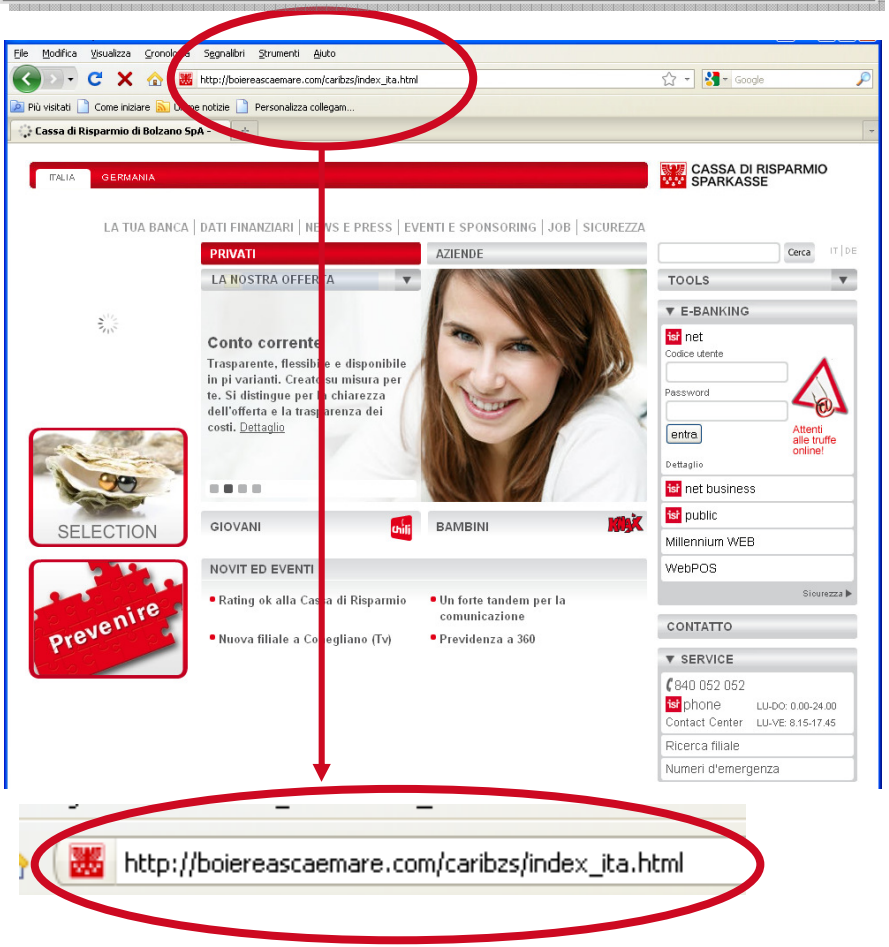
CASSA DI RISPARMIO
SPARKASSE

Esempio Phishing

Più Banca.

Dopo aver cliccato sul link all'interno della e-mail fraudolenta, l'utente viene indirzzato al sito clonato.

Sito clonato



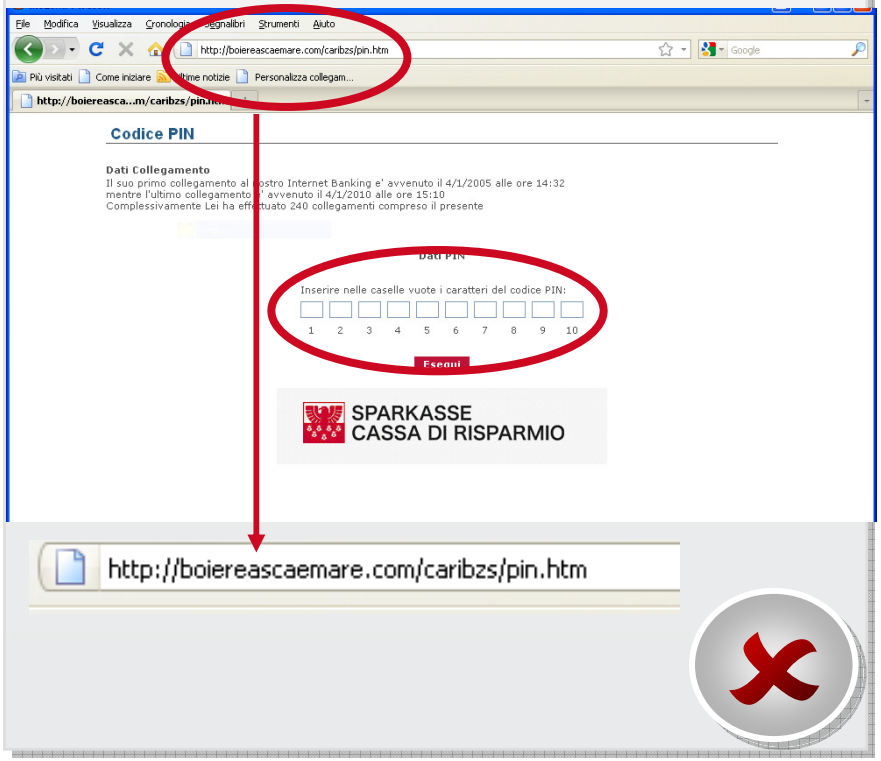
Sito ufficiale Cassa di Risparmio di Bolzano www.caribz.it

CASSA DI RISPARMIO SPARKASSE

Esempio Phishing ISI-net

Più Banca.

Sito clonato



Sito ufficiale Cassa di Risparmio di Bolzano www.caribz.it

Pertanto, invitiamo i nostri clienti ISI di

- **non rispondere ad e-mail sospette**
- **verificare la correttezza del domain www.caribz.it prima di accede all'applicazione ISI**
- **non inserire l'intero codice PIN segreto (l'applicazione ISI richiede max. 2)**
- **verificare che la pagina di inserimento del PIN sia protetta (presenti il lucchetto)**
- **contattare per qualsiasi dubbio o anomalia la Cassa di Risparmio al numero 840 052 052 o via e-mail all'indirizzo: info@sparkasse.it**

CASSA DI RISPARMIO
SPARKASSE