Achtung Phishing!

Mehr Bank.

Phishing ist ein Informatik-Betrugsdelikt mit dem Zweck, die persönlichen Daten eines Benutzers (z.B. Passwort und PIN für den Zutritt zum Internet Banking, Nummer der Kreditkarte usw.) mittels Zusendung von **gefälschten E-Mails** oder mittels **Schadprogrammen bzw. Malware** (Computervirus oder Trojanisches Pferd), die unwissentlich heruntergeladen oder mittels Datenaustausch auf den Computer gelangen, ausfindig zu machen.

Phishing erfolgt durch Betrüger, die **gefälschte E-Mails** verschicken, die augenscheinlich von einer Bank oder einer Kreditkarten-Gesellschaft stammen, wobei das Logo, der Name und das typische Layout der nachgeahmten Gesellschaft sowie ähnliche Domains verwendet werden.
Diese E-Mails fordern den Empfänger auf, sich über einen Link mit einer bestimmten Internetseite zu verbinden, die jener der Bank täuschend ähnlich sieht und sich gewöhnlich über ein Pop-up-Fenster öffnet, um die vertraulichen Informationen einzugeben.

Schadprogramme, wie **Computervirus oder Trojanisches Pferd**, wurden entwickelt, um vom Benutzer unerwünschte und ggf. schädliche Funktionen auszuführen.

Wir bitten unsere ISI Nutzer:
- **keine verdächtigen E-Mails zu beantworten**
- **die Korrektheit des Domains www.sparkasse.it zu überprüfen, bevor auf die ISI Applikation zugegriffen wird**
- **keine persönlichen Daten außerhalb des ISI Bereichs weiterzugeben**
- **eine Antivirus Software auf den PC zu installieren (crimeware)**
- **bei Zweifel oder Unregelmäßigkeiten sich an die Sparkasse unter der Servicenummer 840 052 052 oder über E-Mail: info@sparkasse.it zu wenden**

SPARKASSE
CASSA DI RISPARMIO

Beispiel Phishing

Mehr Bank.

Gefälschte E-mail!

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

Klickt der User auf den Link wird er auf die geklonte Homepage weitergeleitet.

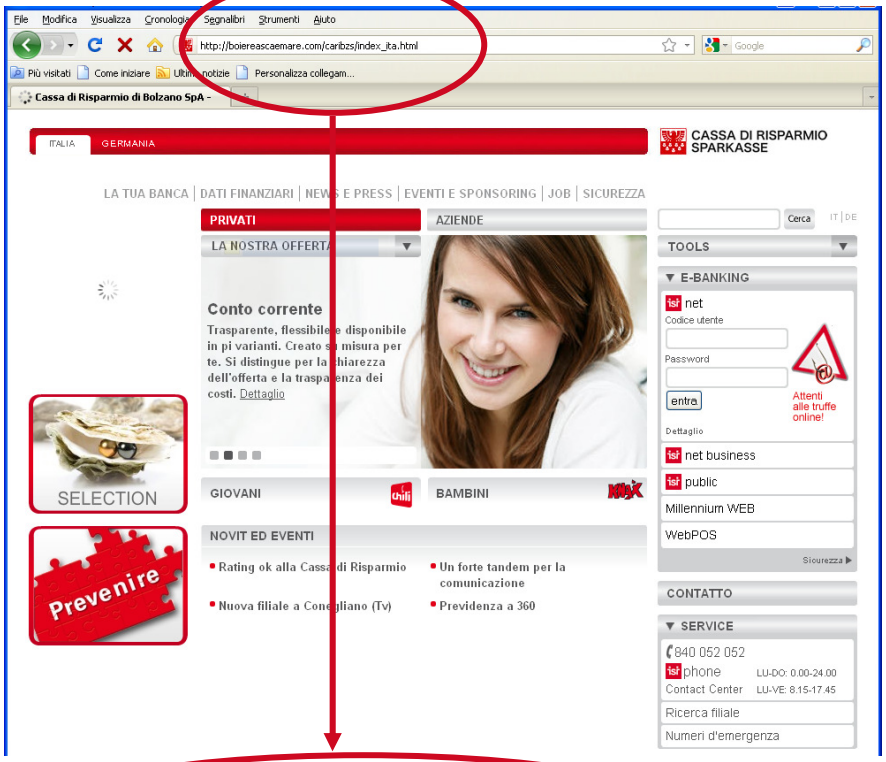
SPARKASSE
CASSA DI RISPARMIO

Beispiel Phishing

Mehr Bank.

Nachdem der Nutzer auf den Link in der gefälschten E-Mail geklickt hat, wird er auf die geklonte Homepage weitergeleitet.

Geklonte Internetseite

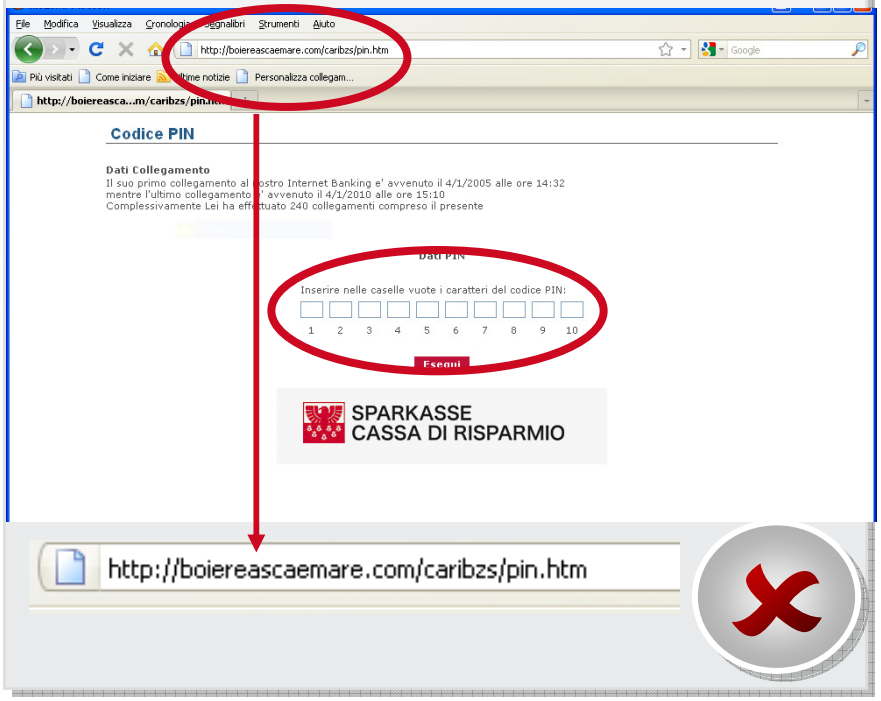


Offizielle Internetseite der Südtiroler Sparkasse www.sparkasse.it

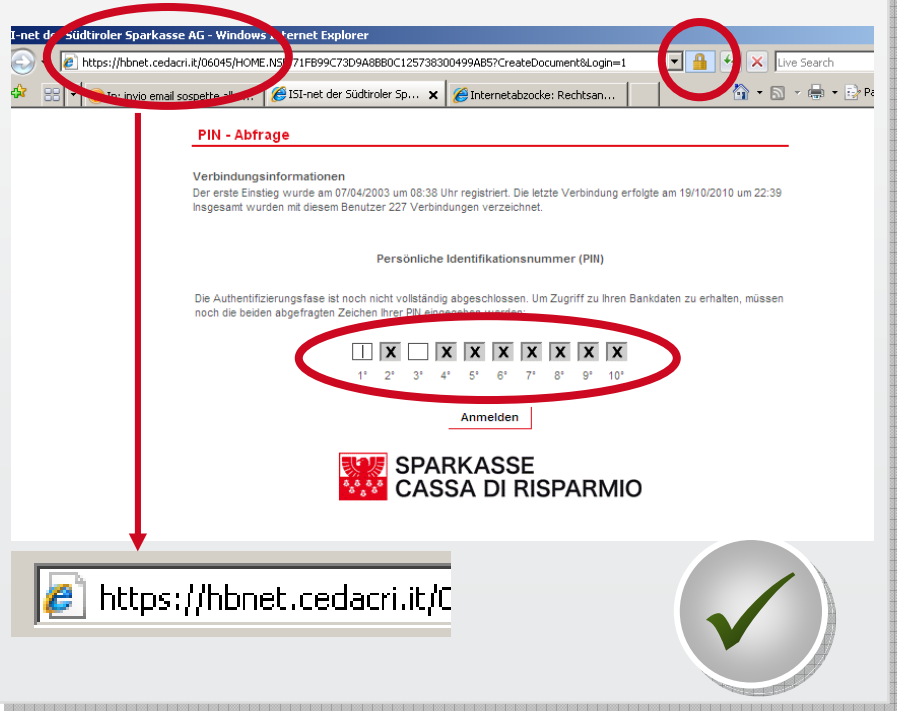
Beispiel Phishing ISI-net

Mehr Bank.

Geklonte Internetseite



Offizielle Internetseite der Südtiroler Sparkasse



Wir weisen unsere ISI Nutzer darauf hin

- **keine verdächtigen E-Mails zu beantworten**
- **die Korrektheit des Domains www.sparkasse.it zu überprüfen, bevor auf die ISI Applikation zugegriffen wird**
- **nicht den vollständigen Geheimcode PIN einzugeben (die ISI Applikation fragt max. 2 Stellen)**
- **darauf achten, dass die Eingabeseite des PIN Codes geschützt ist (Vorhängeschloss ist vorhanden)**
- **sich bei Zweifel oder Unregelmäßigkeiten an die Sparkasse unter der Servicenummer 840 052 052 oder über E-Mail: info@sparkasse.it zu wenden**

SPARKASSE
CASSA DI RISPARMIO