SPARKASSE
CASSA DI RISPARMIO

RATSCHLÄGE UM NICHT IN DIE BETRUGSFALLE DES PHISHING ZU GERATEN

1. **Mißtrauen Sie** jeder Mail, die Sie auffordert, vertrauliche Daten betreffend **Codes von Zahlkarten, Passwords und PIN-Kennziffern** für den Zutritt zum Internet Banking-Dienst oder sonstige persönliche Informationen einzugeben. Die Südtiroler Sparkasse AG fordert diese Informationen nie über E-mail an.

2. E-mail-Betrügereien können mit etwas Aufmerksamkeit in der Regel leicht erkannt werden. Im Allgemeinen sind diese E-mails:
   - nicht persönlich gestaltet und enthalten eine allgemein gehaltene Nachricht, mit welcher aus nicht näher erläuterten Gründen (z.B. Fälligkeit, Verlust, technische Probleme) persönlichen Informationen angefordert werden
   - der Ton des Schreibens ist eher einschüchternd, es wird zum Beispiel gedroht, bei Nichtbeantwortung durch den Benutzer den Account zu löschen
   - sie enthalten kein Fälligkeitsdatum für die Übermittlung der Informationen.

3. Sollten Sie eine E-mail mit diesem Inhalt erhalten, **antworten Sie nicht** , sondern informieren Sie umgehend die Südtiroler Sparkasse AG über den Help-Desk oder indem Sie sich zur Geschäftsstelle begeben.

4. Klicken Sie nicht auf die in verdächtigen E-mails **angeführten Links** , da diese Verbindungen Sie zu einer gefälschten Seite führen könnten, die sich von der originalen Seite kaum unterscheidet. Auch wenn in der Adresszeile des Browsers die richtige Adresse aufscheint, bleiben Sie mißtrauisch: ein Hacker kann nämlich in besagten Feld eine andere Adresse aufscheinen lassen als jene, in der Sie sich tatsächlich befinden. Geben Sie ausdrücklich die Adresse der Webseite ihrer Bank von Hand ein, also „www.caribz.it" oder „www.sparkasse.it".

5. Seien Sie zudem vorsichtig bei E-mails mit sehr langen Adressen, die unübliche Schriftzeichen, aufweisen.

6. Falls Sie vertrauliche Daten in einer Webseite eingeben, vergewissern Sie sich, dass es sich um eine geschützte Seite handelt. Diese Seiten sind leicht zu erkennen, da die Adresse im Browser mit „https://" und nicht mit „http://" beginnt und, je nach dem welchen Browser Sie benutzen, in der Seite ein Schloss aufscheint. Weiters sollten Sie sich vergewissern, dass die Ansicht der Webseite der Bank im einzigen geöffneten Fenster des Browsers erfolgt.

7. Seien Sie vorsichtig, falls sich die Modalitäten für die Eingabe ihrer Zugangscodes zum Internetbanking plötzlich ändern: z.B.: falls diese Daten nicht durch eine Seite, sondern durch ein Pop-up (ein kleineres Zusatzfenster) verlangt werden. Wenden Sie sich in diesem Fall an die Sparkasse, entweder über den Help-Desk oder indem Sie sich direkt zur Geschäftsstelle begeben.

8. **Kontrollieren Sie regelmäßig die Auszüge Ihres Kontos** und der Kreditkarten um sich zu vergewissern, dass die Aufstellung der Geschäftsfälle, den effektiv durchgeführten Geschäftsstellen entspricht. Im gegenteiligen Fall, wenden Sie sich bitte an die Sparkasse und/oder an den Ausgeber Ihrer Kreditkarte.

9. Die Herstellerfirmen der Browser stellen periodisch und zum kostenlosen Herunterladen sogenannte Patch zur Verfügung, durch welche diese Programme zusätzlich abgesichert werden. Auf den Seiten dieser Betriebe können Sie auch feststellen, ob Ihr Browser auf den letzten Stand ist; im gegenteiligen Fall ist es ratsam, die Patch herunterzuladen und zu installieren.

10. Im Internet ist es wie im wirklichen Leben. So wie Sie keinem Unbekannten den Pin-Code Ihrer Bancomat-Karte geben würden, sollten Sie größte Vorsicht walten lassen, bevor Sie Ihre vertraulichen Daten jemandem mitteilen, dessen Identität nicht sicher ist. Im Zweifelsfall wenden Sie sich an die Sparkasse.

    Sie erreichen unser Help-Desk über

    die Telefonnumer **840.052.052**
    über die E-mail-Adresse info@sparkasse.it

    Wir erinnern Sie weiters daran, dass die zuständige Institution zur Bekämpfung von informatischen Betrugshandlungen die Postpolizei ist.