BERGOS

SICHERHEITSHINWEISE FÜR DAS E-BANKING

Die wichtigsten zu beachtenden Grundsätze für einen sicheren Umgang mit dem E-Banking.

1. Grundlegendes zum E-Banking

Login

- Geben Sie die Adresse für den Login in unser E-Banking-Portal («login.bergos.ch») immer manuell in die Adresszeile Ihres Browsers ein oder navigieren Sie via Website der Bergos AG («bergos.ch») auf das E-Banking-Portal. Loggen Sie sich niemals über eine Suchmaschine (z.B. Google) oder über einen Link, der Ihnen beispielsweise per E-Mail zugeschickt worden ist, ein.
- Kontrollieren Sie, ob eine sichere Verbindung zur richtigen Website besteht:
  - Schloss-Symbol in der Adresszeile
  - Richtiger Name der Bergos AG als Zertifikatsbesitzerin (klicken Sie hierzu auf das angezeigte Schloss-Symbol)
  - Korrekte Internetadresse der Login-Seite («login.bergos.ch»)

  Hinweis: Beim sogenannten Echtzeit-Phishing werden Kunden über Werbeanzeigen auf gefälschte E-Banking-Portale geführt. Erfolgt eine Anmeldung auf einem solchen Portal, wird auf das Passwort der Kunden gegriffen, welches nahezu gleichzeitig beim echten E-Banking-Portal zur Anmeldung genutzt wird. Dem Kunden wird auf der Mobile App sodann ein One Time Passcode angezeigt, welcher der Kunde wiederum im gefälschten E-Banking-Portal eingibt. So kann der Angreifer auf den One Time Passcode zugreifen und sich Zugang auf das echte E-Banking-Portal verschaffen. Vor diesem Hintergrund ist es umso wichtiger, sicherzustellen, dass Sie eine sichere Verbindung zum richtigen E-Banking-Portal der Bergos AG hergestellt haben.
- Geben Sie Ihren Benutzername und Ihr individuelles Passwort auf der Login-Seite ein. Ihr Login ist anschliessend mittels Bergos Mobile App zu bestätigen.

Zugangsdaten schützen

- Verwenden Sie komplexe Passwörter, die aus einer Kombination von Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie leicht zu erratende Informationen wie Geburtsdaten oder Namen. Ändern Sie das Passwort, wenn Sie vermuten, dass es anderen Personen bekannt ist.
- Halten Sie Ihre PIN und Passwörter nirgendwo schriftlich fest und geben Sie Ihre persönlichen Zugangsdaten niemals bekannt.
- Loggen Sie sich von unterwegs ein, achten Sie darauf, dass Sie Ihre persönlichen Zugangsdaten verdeckt eingeben und Ihnen dabei niemand über die Schulter schaut. Zudem sollte eine offene E-Banking-Sitzung nie unbeaufsichtigt gelassen werden. So geben Sie Dritten keine Gelegenheit für einen Missbrauch.

Korrekt abmelden

- Beenden Sie die E-Banking-Sitzung ordnungsgemäss, indem Sie auf «Abmelden» klicken und löschen Sie den Browserverlauf. So werden während einer E-Banking-Sitzung zwischengespeicherte Daten entfernt.

Geräte schützen

- Schützen Sie Ihre Geräte mit einer Firewall und einem Antivirenprogramm und achten Sie darauf, dass Sie Ihr Antivirenprogramm, Ihr Betriebssystem sowie weitere installierte Software regelmässig aktualisieren. Aktivieren Sie wann möglich die automatische Update-Funktion.
- Vermeiden Sie die Nutzung von E-Banking-Diensten über öffentliche WLAN-Netzwerke, da diese unsicher sein können.
- Nutzen Sie nur vertrauenswürdige und sichere Geräte für den Zugriff auf Ihr E-Banking-Konto. Vermeiden Sie den Zugriff von öffentlichen Computern oder Geräten.

2. Verhaltensregeln

Vorsicht bei Unregelmässigkeiten

- Wenn ein Systemunterbruch oder eine ungewöhnliche Meldung auftritt sowie falls Sie aufgefordert werden, Bestätigungen auszuführen oder Software zu installieren, brechen Sie den Anmeldevorgang und die Verbindung sofort ab und kontaktieren Sie umgehend den E-Banking-Support.

Unaufgeforderte Kontaktaufnahme

- Hinterfragen Sie unerwartete Kontaktaufnahmen und unerwartete Zahlungsaufforderungen per Anruf, E-Mail oder andere elektronische Nachrichten stets, und geben Sie niemals vertrauenswürdige Informationen bekannt, wenn Ihnen der Anrufer, Absender oder der Grund der Anfrage nicht bekannt ist.
- Insbesondere sind Zahlungsaufforderungen per E-Mail oder andere elektronische Nachrichten, welche Ihnen Bankangaben für eine Zahlung angeben, immer beim Rechnungssteller zu überprüfen. Verwenden Sie hierzu eine offizielle Telefonnummer oder E-Mailadresse und nicht diejenigen, die in der Nachricht aufgeführten sind.

  Hinweis: Bergos AG fordert Sie niemals dazu auf, Ihren E-Banking-Zugang zu testen, Ihre Zugangsdaten oder sonstigen vertraulichen Informationen anzugeben oder eine Testzahlung auszulösen. Weder per Anruf, E-Mail oder andere elektronische Nachrichten. Bei Unsicherheiten kontaktieren Sie bitte den E-Banking-Support.

Verdächtige E-Mails oder andere elektronische Nachrichten

- Betrügerische E-Mails oder andere elektronische Nachrichten, sogenannte Phishing-Mails, sind nicht immer leicht zu erkennen. Achten Sie auf Rechtschreib- und Grammatikfehler, fremde Schriftzeichen, falsche Sprache, ungewöhnliche Tonalität, Haftungsausschlüsse, nicht passende Logos und Design. Phishing-Mails neigen dazu, Dringlichkeit als Taktik einzusetzen, um den Empfänger dazu zu verleiten, schnell zu handeln, ohne ausreichend nachzudenken. Überprüfen Sie die Absenderadresse genau. Oftmals werden ähnlich aussehende Adressen verwendet, um den Anschein von Legitimität zu erwecken. Überprüfen Sie allfällige Links, indem Sie den Mauszeiger darüber bewegen (ohne zu klicken). Phishing-Mails können sich als legitime Seiten ausgeben, indem sie ähnliche klingende Domainnamen verwenden. Klicken Sie in verdächtigen Fällen nicht auf in der Nachricht enthaltene Links, öffnen Sie keine Anhänge und löschen Sie die Nachricht.
- Vertrauen Sie grundsätzlich keinen E-Mails oder sonstigen elektronischen Nachrichten, die Ihnen seltsam erscheinen.
- Bei Unsicherheiten kontaktieren Sie bitte den E-Banking-Support und lassen sich die Echtheit der Nachricht bestätigen. Dies auch, wenn die Nachricht scheinbar von der Bergos AG kommt.

3. E-Banking auf mobilen Geräten

- Geben Sie Ihren Benutzername und Ihr individuelles Passwort in der Bergos Mobile App ein.
- Installieren Sie die Mobile App nur aus den offiziellen Stores.
- Aktivieren Sie stets einen individuellen Sperrcode auf Ihren mobilen Geräten.

4. E-Banking-Support

Bei Ungewöhnlichkeiten oder Unsicherheiten melden Sie sich bitte unverzüglich beim E-Banking-Support.

Telefon: +41 44 284 21 37
E-Mail: ebanking@bergos.ch