Wichtige Information zum Schutz Ihrer PIN und Ihres einmaligen Passcodes

Zum Schutz Ihrer Kontodaten haben wir verschiedene Massnahmen umgesetzt. Um sicherzustellen, dass Ihre Online-Sicherheit nicht beeinträchtigt und Ihr Kontozugang und Ihre Kontodaten nicht unrechtmässig offengelegt oder verwendet werden, empfehlen wir Ihnen, die nachstehenden eService-Sicherheitsrichtlinien zu befolgen.

1. Bevor Sie Ihre WebUserID und PIN eingeben, sollten Sie sich stets vergewissern, dass die aufgerufene Website auch wirklich zu Schroders gehört. Dies können Sie anhand der in Ihrem Browser angezeigten URL (Website-Adresse) sowie anhand des Namens der Bank in ihrem digitalen Zertifikat überprüfen. Dieser Vorsichtsmassnahme gewährleistet, dass Sie Ihren Schroders eService Access Code und Ihre PIN nicht einer Website zugänglich machen, die nicht zu Schroders gehört.
2. Wichtige Tipps zum Schutz Ihrer PIN, Ihres Passcode und Ihrer Kontodaten:
   (a) PINs sollten aus mindestens 6 Ziffern oder 6 alphanumerischen Zeichen bestehen.
   (b) PINs sollten nicht auf einer WebUserID, einer persönlichen Telefonnummer, einem Geburtsdatum oder einer anderen leicht erratbaren persönlichen Information basieren.
   (c) PINs müssen vertraulich gehalten werden und dürfen an niemanden weitergegeben werden.
   (d) PINs sollten Sie sich einprägen – sie dürfen nirgends notiert, aufgezeichnet oder gespeichert werden.
   (e) PINs sind regelmässig zu ändern. Sobald ein Verdacht besteht, dass die PIN offengelegt, unrechtmässig weitergegeben oder verwendet wurde, ändern Sie sie sofort und informieren Sie Schroders.
   (f) Verwenden Sie dieselbe PIN nicht für verschiedene Websites, Anwendungen oder Dienste. Insbesondere dann nicht, wenn sie sich auf verschiedene Dienstleister, Anbieter oder Unternehmen beziehen.
   (g) Bewahren Sie Ihre WebUserID, PIN und/oder Ihr Security Token niemals am gleichen Ort auf.
   (h) Aktivieren Sie niemals die Browsereinstellung für das Speichern oder Aufbewahren von Benutzernamen und Passwörtern.
   (i) Überprüfen Sie, dass die Website-Adresse der Bank sich von «http://» in «https://» ändert und dass ein Sicherheits-Icon angezeigt wird. Dieses sieht (je nach Browser) aus wie ein Vorhängeschloss oder ein Schlüssel und erscheint, wenn eine Authentifizierung oder eine Verschlüsselung zu erfolgen hat.
   (j) Erlauben Sie niemandem, Ihr Security Token zu behalten, zu verwenden oder sich sonstwie daran zu schaffen zu machen.
   (k) Geben Sie niemandem den einmaligen Passcode preis, der vom Security Token generiert wurde.
   (l) Geben Sie die Seriennummer Ihres Security Token an niemanden weiter.
   (m) Überprüfen Sie Ihren Kontostand und die Transaktionen auf Ihrem Bankkonto regelmässig und melden Sie uns jegliche Unstimmigkeiten.

3. Installieren Sie ein Anti-Virus-, Anti-Spyware- und Firewall-Programm auf allen von Ihnen verwendeten Computern.
4. Aktualisieren Sie die Betriebssysteme, Anti-Virus- und Firewall-Programme regelmässig mit den Sicherheitsupdates und neuen Versionen.
5. Deaktivieren Sie alle Datei- und Drucker-Freigabe-Funktionen auf Ihren Computern. Besonders dann, wenn Ihr Internetzugang via Kabelmodem, Breitbandverbindung oder ähnliche Installationen eingerichtet ist.
6. Erwägen Sie die Verwendung von Verschlüsselungstechnologie, um hoch sensible Daten zu schützen.
7. Löschen Sie den Browser-Cache nach jeder Online-Sitzung.
8. Loggen Sie sich aus der Online-Sitzung aus.
9. Installieren Sie keine unbekannte Software und starten Sie keine Programme, deren Ursprung Sie nicht kennen.
10. Löschen Sie Spam- oder Ketten-E-Mails. Diese könnten bösartige Programme enthalten.
11. Öffnen Sie keine E-Mail-Anhänge von Unbekannten.
12. Geben Sie niemals persönliche, finanzielle oder Kreditkarten-Daten auf wenig bekannten oder verdächtigen Websites ein.
13. Verwenden Sie keinen Computer oder anderes Gerät, auf das Sie sich nicht für die Verwendung der Schroders eServices verlassen können.
14. Verwenden Sie für den Zugang zu Schroders eServices niemals öffentlich zugängliche oder in Internet-Cafés installierte Computer.

Die obenstehende Information zu den Sicherheitsvorkehrungen und empfohlenen Vorgehensweisen erhebt keinen Anspruch auf Vollständigkeit und kann jederzeit Änderungen unterliegen.

Bitte zögern Sie nicht, mit uns Kontakt aufzunehmen, wenn Sie Fragen haben oder Unterstützung benötigen.