Informazioni importanti su come proteggere il vostro PIN e il codice temporaneo

Abbiamo messo in atto misure per proteggere le informazioni del vostro conto. Tuttavia, per essere certi che la vostra sicurezza online, l'accesso al conto e le informazioni che vi riguardano non siano compromesse, vi raccomandiamo di adottare le seguenti direttive di sicurezza per eServices.

1. Prima di digitare il vostro WebUserID e il codice PIN, accertatevi sempre che il sito web che state visitando sia quello di Schroders. Questo può essere fatto controllando l'URL che compare nel vostro browser e il nome della Banca nel relativo certificato digitale. Tale precauzione garantirà che non state rivelando a un sito web diverso da quello di Schroders il vostro Codice d'accesso a eServices e il vostro PIN.
2. Suggerimenti importanti per la tutela e la protezione del vostro PIN, passcode e informazioni sul conto:
   (a) I codici PIN devono essere formati da almeno 6 cifre o 6 caratteri alfanumerici.
   (b) I codici PIN non devono basarsi su WebUserID, numero di telefono personale, data di nascita o altre informazioni personali facilmente intuibili.
   (c) I codici PIN sono strettamente personali e non devono essere divulgati a terzi.
   (d) I codici PIN vanno memorizzati e non devono essere mai annotati.
   (e) I codici PIN devono essere periodicamente cambiati. Qualora si sospetti che il codice PIN sia stato compromesso o danneggiato, è necessario cambiarlo immediatamente inviandone notifica a Schroders.
   (f) Lo stesso codice PIN non deve essere utilizzato per differenti siti web, applicazioni o servizi, soprattutto quando fanno capo a organismi/istituzioni diverse.
   (g) Tenete in luoghi separati il vostro WebUserID, codice PIN e/o token di sicurezza.
   (h) Non selezionate l'opzione del browser che consente di memorizzare o archiviare il nome utente e la password sul computer.
   (i) Verificate che l'indirizzo del sito web della banca si modifichi da ‘http://’ a ‘https://’ e che compaia un'icona raffigurante un lucchetto o una chiave nella fase di autenticazione e di crittografia.
   (j) Non permettete a terzi di custodire, utilizzare o manomettere il vostro token di sicurezza.
   (k) Non rivelate a terzi il codice temporaneo generato dal token di sicurezza.
   (l) Non divulgate a terzi il numero di serie del vostro token di sicurezza.
   (m) Verificate frequentemente il saldo del vostro conto bancario e le operazioni effettuate, segnalando eventuali discrepanze.
3. Istallate nei vostri PC software antivirus, anti-spyware e firewall.
4. Aggiornate con cadenza regolare i sistemi operativi, i prodotti antivirus e i firewall con patch di sicurezza o con le versioni più recenti.
5. Disattivate l'opzione di condivisione di file e stampante nei vostri computer, soprattutto quando avete accesso a Internet tramite modem via cavo, connessioni a banda larga o impostazioni simili.

6. Considerate l'utilizzo della tecnologia crittografica per proteggere dati estremamente sensibili.
7. Svuotate la cache del browser dopo la sessione online.
8. Chiudete la sessione online cliccando «esci».
9. Non installate software né utilizzate programmi di origine sconosciuta.
10. Cancellate le e-mail spazzatura o le «catene» perché potrebbero contenere codici maligni.
11. Non aprite allegati a e-mail provenienti da sconosciuti.
12. Non rivelate informazioni personali, finanziarie o relative a carte di credito a siti poco noti o sospetti.
13. Non utilizzate computer o dispositivi inaffidabili per accedere a eServices di Schroders.
14. Non utilizzate computer pubblici o di internet cafè per accedere a eServices di Schroders.

Le informazioni sopra riportate sulle precauzioni e le buone prassi in materia di sicurezza non intendono essere esaustive e si modificano nel tempo.

Non esitate a contattarci per quesiti o per richiedere assistenza.