Información importante para proteger su PIN y su código de acceso de un solo uso

Hemos establecido medidas para proteger la información de su cuenta. No obstante, para no poner en riesgo la seguridad de su conexión, el acceso a su cuenta y su información, le aconsejamos seguir las siguientes recomendaciones de seguridad de eService.

1. Antes de escribir su WebUserID y su PIN, asegúrese siempre de que el sitio web que desea visitar pertenece a Schroders. Para comprobarlo, mire la URL que aparece en su navegador y el nombre del banco en el certificado digital. Esta medida de precaución le ayudará a no revelar su código de acceso y su PIN de eService de Schroders a un sitio web ajeno a la compañía. Sugerencias importantes para proteger su PIN, su código de acceso y la información de su cuenta:

(a) El PIN debe tener al menos 6 dígitos o 6 caracteres alfanuméricos.

(b) El PIN no debe ser igual a su WebUserID, su número de teléfono personal, su fecha de nacimiento ni a ningún otro dato personal que sea fácil de adivinar.

(c) El PIN debe manejarse de forma confidencial y no debe divulgarse a otras personas.

(d) El PIN debe memorizarse y no debe registrarse en ningún lugar.

(e) El PIN debe cambiarse periódicamente. Si sospecha que se ha violado la seguridad de su PIN o que este se encuentra en riesgo, cámbielo inmediatamente y notifique a Schroders.

(f) No utilice el mismo PIN para diferentes sitios web, aplicaciones o servicios, especialmente si pertenecen a diferentes entidades.

(g) No guarde su WebUserID, su PIN y su token de seguridad en el mismo lugar.

(h) No seleccione la opción del navegador para guardar o recordar el nombre de usuario y la contraseña.

(i) Compruebe que la dirección del sitio web del banco cambia de “http://” a “https://” y que aparece un icono de seguridad con forma de candado o llave para la autenticación y el cifrado.

(j) No permita que nadie guarde, utilice o manipule su token de seguridad.

(k) No revele a nadie el código de acceso de un solo uso generado por el token de seguridad.

(l) No divulgue a nadie el número de serie de su token de seguridad.

(m) Compruebe con frecuencia el saldo de su cuenta bancaria y sus transacciones, y comunique cualquier discrepancia.

2. Instale software antivirus, anti-spyware y firewall en sus ordenadores personales.

3. Actualice periódicamente los sistemas operativos y los productos antivirus y de firewall con parches de seguridad o las versiones más recientes.

4. Desactive la opción para compartir ficheros e impresoras en sus ordenadores, especialmente si se conecta a Internet a través de cablemódem, banda ancha o conexiones similares.

5. Considere la posibilidad de utilizar tecnología de cifrado para proteger los datos más confidenciales.

6. Vacíe la memoria caché del navegador cuando finalice su sesión de Internet.

7. Cierre la sesión de Internet.

8. No instale software ni ejecute programas de origen desconocido.

9. Elimine el correo electrónico no deseado o de envío masivo ya que puede contener código malintencionado.

10. No abra los archivos adjuntos a los mensajes de correo electrónico provenientes de remitentes desconocidos.

11. No divulgue datos personales, financieros o de su tarjeta de crédito a sitios web poco conocidos o sospechosos.

12. No utilice un ordenador o dispositivo si no es lo suficientemente fiable para usar Schroders eServices.

13. No utilice ordenadores públicos o de cibercafés para conectarse a Schroders eServices.

La información anterior sobre precauciones de seguridad y prácticas recomendadas no es exhaustiva y es dinámica.

No dude en contactar con nosotros si tiene preguntas o necesita ayuda.