RECOMENDACIONES DE LA SEGURIDAD DE INFORMACIÓN

Por haberse hecho más frecuentes los casos de operaciones fraudulentes de transferencia de recursos monetarios con el empleo de sistemas de servicio bancario a distancia a través de la red Internet y a efectos de prevenir el acceso desautorizado a las Cuentas del Cliente por parte de malechores el Banco recomienda con insistencia a las personas físicas – usuarios del Sistema – cumplir las siguientes medidas de seguridad de información:

- Usar permanentemente el software antivirus con la última versión actual de las bases.
- Realizar regularmente la comprobación antivirus para detectar oportunamente los programas maliciosos.
- Instalar regularmente las actualizaciones del sistema operativo y del navegador Internet (mediante el cual se realiza el acceso al Sistema).
- Es necesario realizar la entrada en el Sistema tecleando directamente el enlace https://elf.faktura.ru/?site=evrofinance en el navegador o pulsando el enlace en el sitio oficial del Banco, comprobando siempre que la conexión se realice por el protocolo seguro https. La barra de direcciones del navegador al pasar al sitio auténtico del Sistema debe cambiar el color al verde, o en la barra de direcciones aparecerá el icono de cerradura cerrada.
- No usar el Sistema desde puestos de trabajo de invitado (cibercafés etc.).
- No instalar actualizaciones del software de sistema o del navegador de Internet recibidas en nombre del Banco por correo electrónico o de cualquier otro modo, no abrir enlaces en tales mensajes postales. Al recibir tal mensaje comunicarlo inmediatamente al Banco.
- Una vez al día o más a menudo recibir la información de las Disposiciones registradas y del estado de cuentas.

El Banco recomienda al Cliente tener en cuenta los riesgos durante el trabajo con el Sistema a través de la red Internet y comprender que el empleo del software antivirus no da el 100% de la garantía de protección contra las operaciones fraudulentas en el Sistema por un malechor.

Hay que tener en cuenta los sistemas de fraude en la red Internet que son las más difundidas actualmente:

- "Ingeniería social" – los malechores envían mensajes SMS en nombre del Banco y bajo pretextos diferentes tratan de recibir del Cliente Nombres de usuario, Contraseñas, apellidos, nombres y patronímicos, números de cuentas, tarjetas, códigos pin etc.
- "Phishing" – se envía al Cliente por correo o de otro modo un enlace a un sitio falso, que puede no distinguirse visualmente del auténtico, con la instrucción de introducir el Nombre de usuario, la Contraseña para el acceso al Sistema y otros datos bajo cualquier pretexto (ha expirado el plazo de la contraseña, necesidad de pasar una autorización adicional, desbloquear el acceso bloqueado etc.).
- Contagio con un código malicioso – pasa a través de difundir programas maliciosos a través de los recursos de Internet, por ejemplo, sitios de las redes sociales, o mediante el envío de correo basura. Después de que el Sistema del Cliente se contagia con el virus o un "troyano" el malechor recibe el control total del Sistema.

Usando el Sistema hay que recordar que:

El Banco no envía mensajes mediante SMS o correo electrónico solicitando datos del Cliente o datos del Sistema.

En caso de que el Cliente detecte operaciones sospechosas en el Sistema es necesario contactar inmediatamente el Servicio de atención al cliente por los teléfonos publicados en el sitio oficial del Banco.