INFORMACIÓN AL INVERSOR

La CNMV alerta de nuevas estrategias informáticas de los *chiringuitos financieros*

19 de noviembre de 2020

- No comparta con terceros las claves de acceso a sus cuentas bancarias y de valores
- No permita el acceso remoto a sus dispositivos informáticos
- No inicie una sesión para operar con sus cuentas bancarias y de valores con un tercero conectado
- No recurra a servicios VPN para ocultar su IP y entrar en páginas web bloqueadas a IPs procedentes de España

En los últimos meses se están recibiendo en la CNMV testimonios de inversores españoles sobre el uso de nuevas herramientas informáticas por parte de los conocidos como chiringuitos financieros —entidades que prestan servicios de inversión sin autorización, no inscritas en los registros de este organismo—, que les ha provocado importantes pérdidas en el patrimonio invertido, como resultado de las operaciones realizadas o por lo infructuoso de sus intentos por recuperar el saldo de sus cuentas de valores.

Los testimonios recibidos se centran en el recurso a dos herramientas que las condiciones derivadas de las medidas adoptadas con motivo de la Covid-19 han popularizado: el software de acceso remoto (como AnyDesk, LogMeIn, TeamViewer, etc.) y las redes privadas virtuales (servicios de VPN).

Software de acceso remoto

Este tipo de herramientas permite conectarse de forma remota a los diferentes dispositivos de los usuarios (ordenadores, teléfonos móviles, etc.) para, entre otros servicios, poder acceder los propios usuarios a sus dispositivos a distancia, desde otro terminal, o para gestionar, por parte de terceros, problemas informáticos detectados.

Se ha detectado que los chiringuitos financieros están recurriendo a estas herramientas para conectarse al dispositivo de un inversor y apropiarse de datos (como códigos de acceso o contraseñas) que les permiten, posteriormente, operar sobre las cuentas de valores del inversor, sin contar con la autorización expresa de este.

En ocasiones, es el propio chiringuito financiero el que invita al inversor a instalar previamente una aplicación de acceso remoto específica, pero a veces puede utilizar alguna de las disponibles en el ordenador del propio inversor.

Una vez que el chiringuito financiero está conectado de forma remota al dispositivo del inversor, le solicita a este que inicie una sesión en la página web a través de la que presta indebidamente sus servicios de inversión, captando los códigos de acceso necesarios para operar posteriormente en la cuenta de valores del inversor. Otras veces, de forma más directa, le solicita al inversor que aporte sus claves de acceso a las cuentas de valores.

El uso indebido de este software de acceso remoto, además de las consecuencias que pueden derivarse para los inversores —comunes al resto de herramientas que utilizan los chiringuitos financieros—, dificulta las investigaciones que se pudieran realizar, en sede policial o judicial, en relación con la identificación del ordenante de las operaciones realizadas.

Lo anterior vienen a ser nuevas modalidades de una práctica que, pese a su sencillez e ingenuidad, sigue provocando víctimas en el entorno de los chiringuitos financieros, la de facilitar a terceros las claves de acceso a las cuentas bancarios o de valores, sobre cuyos riesgos es necesario insistir.

Red privada virtual (Servicios VPN)

Los servicios VPN se pueden utilizar para, entre otras funciones, ocultar la dirección de Internet (conocida como IP), que actúa a modo de un identificador público de cada dispositivo informático en Internet. Este identificador es único para cada dispositivo y permite conocer, entre otros elementos, su ubicación geográfica.

Algunas entidades, para no ser caracterizadas como chiringuitos financieros que ofrecen servicios de inversión a inversores españoles, bloquean el acceso a sus páginas web a IP procedentes de España. No obstante, se han recibido testimonios de inversores a los que algunos chiringuitos financieros, por vía telefónica, han propuesto utilizar servidores VPN, lo que permite ocultar o simular la IP de sus dispositivos informáticos, de forma que las páginas web a través de la que los chiringuitos financieros ofrecen sus servicios no identifiquen la procedencia real del inversor y pueda eludir el bloqueo mencionado, que se convierte en solo aparente.

Finalmente, se insiste en la recomendación de no operar más que con las entidades autorizadas para prestar servicios de inversión que figuran en la página web de la CNMV (www.cnmv.es), en la sección "Consultas a los Registros Oficiales". Asimismo, en dicha página web se pueden consultar las entidades que han sido objeto de una advertencia, por parte de la CNMV u otro regulador extranjero, por haberse detectado que prestaban servicios de inversión de carácter reservado sin contar con la autorización preceptiva.