OCF
Oficina del Consumidor Financiero

Tips Contra Estafas

1. Sea desconfiado: Si recibe una llamada telefónica de un número “desconocido” o privado, póngase en guardia. Ser desconfiado es la mejor defensa.

2. No caiga en la trampa de la conversación amable: Si atiende y lo primero que le dicen es “estamos hablando con”, y con especial amabilidad mencionan su nombre completo, cuélguele de inmediato. Ni siquiera espere que le hablen nada más. Si se trata de una llamada legítima, lo volverán a llamar.

3. Exija datos que confirmen que se trate de un funcionario real: En caso de presentarse como funcionario público o bancario, exija de inmediato datos que no se espera, por ejemplo, su número de carné, departamento y nombre de su jefe, número de teléfono y extensión. Responda que usted lo va a llamar, o que pasará más tarde a una sucursal. Lo más seguro es que le darán datos incorrectos, o no se los darán del todo.

4. Por lo general, le ofrecerán desde el inicio algo muy atractivo: las estafas buscan que el consumidor se interese, por lo que le ofrecerán el trámite del bono Proteger, la devolución de unos impuestos o algo similar. Cuelgue la llamada, de inmediato; es una trampa.

5. Jamás brinde datos confidenciales: El supuesto funcionario le dirá desde el principio que no requieren información confidencial, ese será el “gancho”, pero sin que se dé cuenta, es lo primero que buscará; le sugerirá que instale un programa en su dispositivo electrónico, o que ingrese a una página que solo el consumidor puede ver. Cuélguele de inmediato, es otra trampa. Ninguna entidad financiera ni institución, le pedirá nunca nada de eso.

6. Ingreso seguro: Cuando vaya a ingresar al sitio web de su entidad financiera, por medio de su computadora o de su celular, hágalo desde una red segura (de su operador de internet o de la wifi de su casa), pero ante todo que no sea de acceso público. Es muy fácil que le puedan copiar los datos importantes.

7. Verifique que sea la página oficial: Ingrese directamente la dirección web de la entidad financiera en la barra de navegación; nunca lo haga a través desde un buscador, ya que existen páginas clonadas incluso idénticas a la verdadera. Usted no logrará notar la diferencia. Tampoco acceda a la página de la entidad financiera desde vínculos (links) que le hayan enviado, ya que pueden direccionarlo a páginas falsas, que le copiarán todo lo que usted escriba.

8. Descarte correos electrónicos: Nunca responda correos electrónicos donde le soliciten datos personales o confidenciales (contraseñas, tokens, códigos de seguridad). Incluso si el correo viene de una dirección que usted cree que es de un familiar o un amigo.

9. Programas informáticos: No instale programas informáticos que no conozca, porque pueden robarle información confidencial y sensible. Antes de hacerlo, consulte.

10. Cierre inmediato: Cuando deje de utilizar el servicio virtual, cierre de inmediato la sesión y asegúrese que se cerró.