POR UNA BANCA CIBERSEGURA: ¿OFERTÓN? NO, GRACIAS

«Sé cauto y no hagas en internet lo que no harías en el entorno físico»

PILAR CLAVERÍA
ASESORA DE LA ASOCIACIÓN ESPAÑOLA DE LA BANCA (AEB)

Si cuando estás tranquilamente descansando o afanosamente haciendo algo, recibes una llamada de teléfono diciendo que es una de tus empresas de suministros para informar de que, por ser cliente, tienes una oferta muy interesante, desconfía. Si para dar credibilidad a la llamada, comienzan a citar datos que tienen sobre tu persona, desconfía. Si para acceder a la oferta, solo tienes que aceptarla y darles para ello unos datos que te van a enviar al móvil para confirmarla, desconfía.

Si la empresa real de suministros te fuera a aplicar un descuento lo haría sin más y te informaría de ello, pero probablemente no tendrías que hacer ninguna confirmación. Si disponen de ciertos datos es porque probablemente los han recabado de manera irregular. Si compartes los datos que llegan a tu teléfono, probablemente les estás dando los códigos de seguridad de acceso a tu banca electrónica, en cuya puerta están esperando para entrar con muy malas intenciones.

Si recibes tal llamada, deja claro que no les puedes atender y que llamarás con posterioridad a la compañía en cuestión para concretar la oferta. Por supuesto, si quieres comprobar la veracidad de la llamada, localiza los datos oficiales de contacto en las facturas periódicas de la compañía y dirígete a ellos, pero nunca uses un número que te faciliten para devolver la llamada. Si atiendes la llamada por curiosidad o porque resulta creíble, nunca des ningún consentimiento. Y jamás, ¡jamás! compartas con terceros claves de seguridad que te envíe el banco; son eso, claves de seguridad, sería como entregar las llaves de acceso a los amigos de lo ajeno que acechan a la puerta con insanas intenciones.

Y si a estas alturas te preguntas cómo es posible que tengan tanta información y tan precisa hay varias respuestas posibles: han podido acceder a esos datos personales de manera ilegítima, mediante brechas de seguridad en empresas que legítimamente los custodiaban, que se trafican en el mercado negro. O piensa que puede tratarse simplemente de información que has compartido por internet, ya sea en redes sociales o al rellenar formularios para darte de alta en alguna web o servicio en respuesta a ofertas tentadoras, en los que se requie-

ren datos personales, datos telefónicos, direcciones, etc...

Si te das cuenta después de que todo esto haya ocurrido, contacta con tu banco, que te aconsejará sobre cómo proceder. Y recuerda, los bancos, al igual que en las sucursales tienen medidas de seguridad para evitar accesos indeseados, también custodian los fondos y datos de los clientes en el mundo virtual. Están preparados para contener incursiones no permitidas, pero si el malo llega a la puerta con las llaves para entrar porque se las hayamos entregado incautamente, será difícil detener su acceso. Sé cauto y no hagas en internet lo que no harías en el entorno físico.