



---

## ¿Qué es la suplantación de identidad (Phishing)?

El término suplantación de identidad se refiere a mensajes de correo electrónico que se envían para engañar al receptor y hacer que proporcione información privada o personal. Usualmente la información requerida será suficiente para obtener acceso a las cuentas financieras personales o abrir cuentas nuevas fraudulentamente.

Los mensajes se diseñan de modo inteligente para que luzcan como si la fuente oficial los hubiera enviado. Te pueden preguntar algo como “verifica tu información de cuenta”, “actualiza tu perfil de cuenta”, o pueden usar alguna otra táctica para que ingreses tu información confidencial. El mensaje puede especificar que es importante hacer esto rápidamente. Puede hacer referencia a alguna actividad sospechosa en la cuenta o decir que la cuenta se cerrará si no se ingresa la información rápidamente. Algunos de estos mensajes pueden incluso usar gráficos sacados del sitio web de la fuente auténtica. No obstante, cuando ingresas la información o haces clic en el botón para entrar en el sitio, eres llevado a otro lugar. Cualquier información que ingreses se puede usar para propósitos ilegítimos, tales como retiro de dinero, compras fraudulentas o más robo de identidad. Los que envían estos mensajes son inteligentes y buscan constantemente nuevas formas de hacer que los mensajes parezcan genuinos y oficiales.

Lincoln Automotive Financial Services nunca te enviará un correo electrónico para pedirte información personal como número de cuenta, de seguro social, de licencia de conducir, etc.

## ¿Qué debo hacer si recibo un correo electrónico sospechoso de Lincoln Automotive Financial Services?

Si recibes un mensaje así, no ingreses ninguna información ni hagas clic en ningún botón o enlace.

1. Guarda el correo electrónico como un documento de Word en tu computadora.
2. Envía el correo electrónico como documento adjunto a [abuse@ford.com](mailto:abuse@ford.com) , y en el asunto escribe **“phishing”**
3. Dinos cómo te gustaría que te contactemos después de finalizar la investigación. Incluye al menos tu nombre y número de teléfono en el correo electrónico o responderemos a la dirección de correo electrónico con los resultados de la investigación.
4. No elimines el correo electrónico sospechoso hasta que finalicemos la investigación.
5. Si se necesita más información para completar la investigación, Ford Security se comunicará contigo por teléfono/correo electrónico.

Te responderemos en dos días hábiles con los resultados de la investigación.

Ten en cuenta que Lincoln Automotive Financial Services envía correos electrónicos a los clientes que inscribieron sus cuentas en el Administrador de Cuenta. Estas notificaciones por correo electrónico te brindan información sobre tu cuenta en línea (es decir, estados de cuenta disponibles, pagos registrados, cambios de dirección, etc.). Siempre se te pedirá que inicies sesión en el sitio web seguro del Administrador de Cuenta para ver información personal o hacer cualquier transacción.

Si tienes alguna pregunta, no dudes en [Contactarnos](#).