¿Estoy en peligro tras un intento de estafa a través de AnyDesk?

Hoy en día, las estafas a través de aplicaciones de acceso remoto como AnyDesk son un problema creciente. Si has estado en una situación similar a la descrita, es importante actuar con rapidez y tomar precauciones adicionales para proteger tus datos personales. En el caso presentado, tu amigo fue contactado por un estafador que supuestamente representaba a su banco. A menudo, estos estafadores pueden manipular a las personas para que descarguen software de acceso remoto, permitiendo el acceso a su computadora sin que lo noten.

En primer lugar, al desconectar tu computadora de Internet y desinstalar AnyDesk, has tomado medidas inteligentes que minimizan el riesgo de que el estafador obtenga acceso a información sensible. No obstante, es fundamental comprender que simplemente desinstalar el software podría no ser suficiente para proteger tus datos.

Aquí hay algunas recomendaciones:

1. **Cambia tus contraseñas**: Si sospechas que tu información podría estar en riesgo, cambia todas las contraseñas relacionadas con cuentas vinculadas a tu computadora, especialmente las de servicios financieros.
2. **Revisa tu información bancaria**: Mantente alerta sobre cualquier actividad sospechosa en tus cuentas. Si notas algo inusual, contacta a tu banco inmediatamente.
3. **Considera una reinstalación completa**: Realizar una instalación limpia del sistema operativo puede eliminar cualquier posible malware o software malicioso que el estafador pudo haber instalado. Además, asegúrate de respaldar tus datos críticos antes de realizar cualquier reinstalación.
4. **Montar una vigilancia**: Usa software de seguridad para escanear tu computadora en busca de amenazas y mantenerte informado sobre las mejores prácticas de seguridad.

Recuerda, la prevención y la vigilancia constante son esenciales para protegerte de posibles estafas. Si alguna vez sientes que tu seguridad está en riesgo, no dudes en buscar ayuda profesional.