

Usurpación de Cuentas de Correo de Voz

Si usted no cambia la clave de fábrica de todas sus cuentas de correo de voz, usted o su empresa podrían exponerse a una cara sorpresa. Los piratas informáticos (*hackers*, en inglés) saben cómo poner en peligro los sistemas de correo de voz y cómo efectuar llamadas internacionales por pagar, sin su conocimiento ni autorización.

Cómo funciona la estafa

Primero un pirata informático llama a un sistema de correos de voz, en busca de cuentas de correo de voz que aún tengan activas las claves originales de la empresa proveedora o que tengan combinaciones fáciles de adivinar, como 1-2-3-4. Cuando las encuentra, el pirata cambia la grabación de saludo a algo así como “si, si, si, si, operadora voy a aceptar los cargos”. Los sistemas automáticos de llamadas por cobrar están programados para reaccionar a palabras y frases como esas. Entonces el pirata informático efectúa una llamada por cobrar a ese teléfono. Cuando el operador automatizado escucha el mensaje de la cuenta de correo de voz, la llamada se conecta. Entonces el pirata puede usar la misma conexión por largos periodos de tiempo, para efectuar otras llamadas internacionales.

En otra versión de esta estafa, un pirata ingresa ilegalmente a un sistema de derivación de llamadas; programa el sistema para derivar llamadas a un número internacional y entonces utiliza dicho número para efectuar otras llamadas.

Típicamente, los piratas atacan los sistemas de correos de voz de empresas. Pero los usuarios de correos de voz residenciales también deben mantenerse alertas.

Lo que usted debe saber

- Por lo general, los piratas informáticos ingresan ilegalmente a los sistemas de correo de voz durante días festivos o fines de semana, cuando es más probable que los cambios a los mensajes de voz pasen inadvertidos.
- Lo típico es que los piratas informáticos residan en el extranjero, y sus llamadas se originen y se dirijan desde y a muchos países del mundo.
- Las compañías que caen presas de esta estafa generalmente descubren que han sido víctimas cuando su compañía telefónica les informa que sus cuentas han observado una actividad anormal. Pero es posible que las víctimas de teléfonos residenciales no sean alertadas hasta que reciban sus cuentas telefónicas, con cargos mucho más altos que lo acostumbrado.

Consejos para minimizar su riesgo

Para evitar ser víctima de esta estafa, siga los siguientes consejos:

- Siempre cambie la clave original otorgada por su proveedor para su correo de voz telefónico.
- Elija una clave de correo de voz compleja y compuesta por lo menos de seis dígitos.
- Cambie su clave de correo de voz con frecuencia.
- No use claves obvias, como direcciones, fechas de nacimiento, números telefónicos, números repetidos (como 000000) o sucesivos, como 123456.

- Examine su grabación de salud con regularidad, para asegurarse de que sigue siendo lo que usted dispuso.
- Considere bloquear las llamadas internacionales.
- Inhabilite la notificación remota, la contestadora automática, la derivación de llamadas y las funciones de servicios de búsqueda que no utilice.
- Consulte al proveedor de su correo de voz para obtener opciones de resguardo adicionales.

Si piensa que ha sido víctima de piratas informáticos, alerte edl hecho a su proveedor de servicios y a la policía.

Presentación de quejas

Usted tiene múltiples opciones para presentar una queja ante la FCC:

- Presente una queja en línea: <https://consumercomplaints.fcc.gov> (en inglés).
- Por teléfono: 1-888-CALL-FCC (1-888-225-5322); TTY: 1-888-TELL-FCC (1-888-835-5322); ASL: 1-844-432-2275
- Por correo postal (por favor, incluya su nombre, dirección, información de contacto y tantos detalles como pueda respecto a su queja):

Federal Communications Commission
Consumer and Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
45 L Street NE
Washington, DC 20554

Formatos accesibles

Para solicitar este artículo en formato accesible - Braille, letra grande, Word o documento de texto o de audio - escribanos o llámenos a la dirección o teléfonos de más arriba o envíenos un correo electrónico a fcc504@fcc.gov.

Última edición: 22 de septiembre de 2016

