General

Mensajes de correo electrónico solicitando claves (phising)

El phising es una forma de ataque en la que un delincuente suplanta la identidad de un tercero de confianza (empresa, institución, responsable del Servicio) para adquirir información confidencial, como por ejemplo claves de correo electrónico o claves bancarias.

Los mensajes suelen hacer referencia a la necesidad de confirmar alguna clave, debido a algún problema o por mantenimiento en el servicio. En ocasiones facilitan algún enlace (link) a una página web con el mismo aspecto que la entidad que suplantan.
Pero en la mayoría de los casos los mensajes están mal traducidos y a pesar de ello muchos usuarios siguen respondiendo y enviando los datos solicitados al atacante.

Una vez conseguida la información, el atacante suele utilizarla para:
- suplantar a la víctima en otro ataque
- acceder con sus credenciales a opciones privilegiadas.
Por ejemplo: en Campus Virtual están disponibles las actas de notas, nóminas, etc...

El Servicio de Informática nunca le solicitará que le envíe por correo electrónico ningún tipo de clave. Recuerde que usted ya puede cambiar su clave con la opción disponible en Campus Virtual.

Igualmente, ninguna otra institución externa le solicitará que confirme sus claves por correo.

Cualquier mensaje en este sentido debe considerarse sospechoso.

Más información:
- Reconocer Mensajes fraudulentos
- Protégete en el correo electrónico

Solución única ID: #1422
Autor: Jefe Editor de la Sección de Redes
Última actualización: 2010-01-12 13:44