**¿Qué es el Phishing?**

Phishing se uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador.

¿Qué funciona el phishing?

 

Consejos para protegerse del phishing:

1. Evita abrir correos electrónicos no solicitados (o los que se encuentran en spam).
2. No hagas clic a enlaces en correos electrónicos no solicitados.
3. Protege tus contraseñas y no las reveles a nadie.
4. No des información confidencial a nadie, menos por correo electrónico. Cuando las empresas reales necesitan contactarnos tienen otras formas de hacerlo.
5. Comprueba la URL del sitio (dirección web). En muchos casos de phishing, la dirección web puede parecer legítima, pero la URL puede estar mal escrita o el dominio puede ser diferente (.com cuando debería ser .gob).
6. Si se trata de entidades bancarias o comerciales revisa que la dirección web comience con https y no http, como es la costumbre. La S final, nos da un alto nivel de confianza que estamos navegando por una página web segura.
7. Mantén Si aún desea ingresar, no haga clic actualizado tu navegador y aplica los parches de seguridad.
8. Mantén tu antivirus actualizado.
9. Cuando ingreses a páginas de entidades financieras, es preferible que digites la dirección directamente en la barra de búsqueda. Evita los enlaces de otros sitios.
10. Si tienes dudas sobre la legitimidad de un correo, llama por teléfono a la compañía y comprueba la información solicitada.
11. Nunca le entregue sus datos por correo electrónico. Las empresas y bancos jamás le solicitarán sus datos financieros o de sus tarjetas de crédito por correo.
12. Si duda de la veracidad del correo electrónico, jamás haga clic en un link incluido en el mismo.
13. Compruebe que la página web en la que ha entrado es una dirección segura ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.
14. Cerciórese de  escribir correctamente la dirección del sitio web que desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.
15. Si sospecha que fue víctima del Phishing, cambie inmediatamente todas sus contraseñas y póngase en contacto con la empresa o entidad financiera para informarles.

Todos los usuarios del correo electrónico corremos el riesgo de ser víctimas de estos intentos de ataques. Cualquier dirección pública en Internet (que haya sido utilizada en foros, grupos de noticias o en algún sitio web) será más susceptible de ser víctima de un ataque debido a los spiders que rastrean la red en busca de direcciones válidas de correo electrónico. Éste es el motivo de que exista este tipo de malware.

Es realmente barato el realizar un ataque de este tipo y los beneficios obtenidos son cuantiosos con tan sólo un pequeñísimo porcentaje de éxito.

La mejor manera de protegerse del phishing es entender la manera de actuar de los proveedores de servicios financieros y otras entidades susceptibles de recibir este tipo de ataques.

 Prof. Farneti Alejandra y Barciocco María José

Información extraída de

[**https://www.infospyware.com/articulos/que-es-el-phishing/**](https://www.infospyware.com/articulos/que-es-el-phishing/)

[**https://elconsejosalvador.com/que-es-el-phishing-como-evitarlo/**](https://elconsejosalvador.com/que-es-el-phishing-como-evitarlo/)