Dirección General de Sistemas

# Cómo protegerse del phishing

El fraude informático mediante correo electrónico, comúnmente denominado **phishing**, es un proceso fraudulento de la rama de la ingeniería social cuyo objetivo es adquirir información sensible como nombres de usuario, claves o datos de cuentas o tarjetas de crédito, a través de una comunicación electrónica, fingiendo ser una entidad de confianza, tal como un banco o una entidad gubernamental.

El término *phishing* proviene de la palabra en inglés “fishing” (pesca) y hace alusión al acto de “pescar” usuarios mediante “anzuelos” (trampas) cada vez más sofisticados para obtener contraseñas e información financiera.

## CARACTERISTICAS DEL PHISHING

- El campo De: del mensaje muestra una dirección de una empresa real. No obstante, es sencillo para el estafador falsificar la dirección del remitente.
- Normalmente el texto del mensaje presenta errores gramaticales o palabras cambiadas, que no son usuales en las comunicaciones de la entidad auténtica.
- El mensaje contiene logotipos e imágenes que han sido obtenidas del sitio web real al que el mensaje fraudulento hace referencia.
- El enlace que se muestra parece apuntar al sitio web original de la empresa, pero en realidad lleva a un sitio fraudulento donde se solicitarán los datos de usuario.
- El defraudador buscará conseguir una respuesta rápida por parte de la víctima, por ello el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido.

## RECOMENDACIONES ANTE EL PHISHING

**1. Evite el correo basura (SPAM) ya que es el principal medio de distribución de mensajes engañosos.**

Los mensajes de phishing se distribuyen mediante el correo electrónico de la misma forma que los mensajes de correo basura, por lo cual toda acción que contribuya a disminuir el SPAM que se recibe, contribuirá también en reducir los mensajes de phishing que reciba en su casilla.

**2. Ninguna entidad responsable le solicitará datos confidenciales por correo electrónico, teléfono o fax.**

La Dirección General de Sistemas nunca le enviará un correo electrónico solicitando el ingreso de alguna clase de datos, que usted no haya concertado previamente. Todo mensaje en el que se solicite su clave de acceso es falso y constituye un engaño al usuario.

**3. Verifique la fuente de la información.**

No conteste correos que soliciten información personal o financiera. Si duda, comuníquese telefónicamente con la empresa en cuestión mediante los números que figuren en la guía telefónica (no llame a los números que aparecen en el mensaje recibido).

**4. Si el correo electrónico contiene un enlace a un sitio web, escriba usted mismo la dirección en su navegador de Internet, en lugar de hacer clic en dicho enlace.**

De esta forma sabrá que accede a la dirección que aparece en el mensaje y que no está siendo redirigido a un sitio falso. Adicionalmente, si el sitio le solicita información personal, verifique que el envío y la recepción de datos se realiza sobre un canal seguro (la dirección web debe comenzar con https:// y debe aparecer un pequeño candado cerrado en la esquina inferior derecha de la pantalla del navegador).

Para poder dar tratamiento a los casos de Phishing es necesario que al reenviar los mensajes en el estado original, es decir tal y como los tratan los servidores de correo.

Muchos programas de correo adaptan la presentación de los mensajes y pueden acabar ocultando información decisiva para la investigación como son las cabeceras de los mensajes en las que figuran las direcciones IP de los servidores etc.

Las cabeceras de mensajes incluyen una lista de detalles técnicos como, por ejemplo, la dirección IP de la computadora desde la que se envía, el programa utilizado para su redacción y los servidores por los que se ha transmitido hasta llegar a su destino. Esta información es **imprescindible** para la identificación de problemas con el correo electrónico y para identificar fuentes de mensajes de correo electrónico comercial no deseado y fraudes.

Para reenviar un correo electrónico, conservando los encabezados originales del mensaje, es necesario realizar un reenvío especial en el programa de correo electrónico.

### Thunderbird / Icedove

Si utiliza el programa Thunderbird o Icedove, para reenviar un mensaje como adjunto, manteniendo los encabezados originales:

- En la ventana del mensaje, haga clic en el menú **Mensaje**, opción **Reenviar como**, y seleccione **Adjunto**.
- Complete con la dirección de destino `seguridadinformatica@unlu.edu.ar`

### Webmail Roundcube

Si utiliza el Webmail de la Universidad, para reenviar un mensaje como adjunto, manteniendo los encabezados originales:

- En la ventana del mensaje, haga clic la **flecha hacia abajo** que figura en el botón Reenviar y del menú que aparece, seleccione **Reenviar como adjunto**.
- Complete con la dirección de destino `seguridadinformatica@unlu.edu.ar`

### The Bat

Si utiliza el programa The Bat, para reenviar un mensaje como adjunto, manteniendo los encabezados originales:

- En la ventana del mensaje, haga clic en el menú **Especial** y seleccione **Reenvío Alternativo**.
- Complete con la dirección de destino `seguridadinformatica@unlu.edu.ar`

### Correo Gmail

- En la ventana del mensaje, haga clic en la **flecha hacia abajo** al lado del botón Responder, y del menú que aparece, seleccione **Mostrar original**.
- Copie todo el contenido de la pestaña que aparece en el portapapeles.
- Cree un mensaje nuevo pulsando en el botón **Redactar** y pegue allí el texto copiado.
- Complete con la dirección de destino `seguridadinformatica@unlu.edu.ar`

Recuerde que los mensajes que recibamos sin las cabeceras completas no nos serán útiles para combatir el Phishing. Su ayuda es decisiva para combatir el fraude.

**Si Ud. ha recibido un correo electrónico que sospecha puede tratarse de phishing repórtelo al Departamento de Seguridad Informática al teléfono 02323 42-3171 / 42-3979, interno 1312, y reenvíe el mensaje (como adjunto, con los encabezados completos) y toda otra información que considere que puede ser de utilidad a la dirección**

**seguridadinformatica@unlu.edu.ar**