

ALERTA POR CORREOS FALSOS PHISHING

El término phishing proviene de la palabra en inglés "fishing" (pesca) y hace alusión al acto de "pescar" usuarios mediante "anzuelos" (trampas).

El fraude informático mediante correo electrónico, comúnmente denominado phishing, se vale de técnicas de ingeniería social para adquirir información personal y sensible como: nombres de usuario, claves o datos de cuentas o tarjetas de crédito. Para ello el estafador finge que el correo proviene de una entidad de confianza, tal como la Universidad, una entidad bancaria o un organismo gubernamental. Luego utiliza la información obtenida para enviar correo SPAM desde las cuentas de mail de las víctimas del engaño, o para efectuar fraudes monetarios.



CARACTERÍSTICAS

1 PARECE ENVIADO POR LA UNIVERSIDAD

El campo De: del mensaje puede mostrar una dirección de correo electrónico de la Universidad o de una empresa real. No obstante, es sencillo para el estafador falsificar la dirección del remitente.

El cuerpo del mensaje puede contener logotipos e imágenes que han sido obtenidas del sitio web real al que el mensaje fraudulento hace referencia.

2 SOLICITA INFORMACIÓN CONFIDENCIAL

La Universidad nunca le enviará un correo electrónico solicitando el ingreso de datos personales. Todo mensaje en el que se solicite su clave de acceso es falso y constituye un engaño.

3 ENLACES A SITIOS FRAUDULENTOS

El enlace que se muestra parece apuntar al sitio web original de la Universidad, pero en realidad lleva a un sitio fraudulento con un formulario donde se solicitarán los datos de usuario.

4 CARÁCTER DE URGENCIA

El defraudador buscará conseguir una respuesta rápida por parte de la víctima, por ello el mejor incentivo es amenazar con un perjuicio, ya sea económico o de pérdida o cierre de la propia cuenta de correo, si no se siguen las instrucciones indicadas en el e-mail recibido.



RECOMENDACIONES

- Si recibe un mensaje con estas características NO lo responda.
- Reenvíe el correo a seguridadinformatica@unlu.edu.ar para poder advertir de la estafa.
- Si sospecha que su clave de acceso a alguno de los servicios que presta la Universidad ha sido vulnerada, por favor cámbiela de inmediato y contáctese con el Departamento de Seguridad Informática.