www.mexis.net

SEÑALES DE ADVERTENCIA DE ATAQUES DE INGENIERÍA SOCIAL

Todos los intentos de ingeniería social tienen algunas cosas en común.
A continuación, se indican algunas de las señales más comunes que pueden indicar que alguien está intentando un ataque de ingeniería social:

Llamadas telefónicas inesperadas.

Si recibes una llamada que no esperabas, especialmente **si la persona que te llama dice ser de un banco, una compañía de seguros o una empresa de informática, es probable que se trate de un intento de phishing.** No facilites ningún dato personal y evita responder afirmativamente a cualquier pregunta.

Dirección de correo electrónico sospechosa del remitente.

Si algo le parece extraño en un correo electrónico que ha recibido, **compruebe siempre la dirección de correo electrónico del remitente.** Si no coincide con el nombre del remitente y la línea de asunto del correo electrónico, contiene números o símbolos y, en general, parece sospechosa, es posible que se trate de un correo electrónico no deseado.

Solicitudes inusuales de alguien que quizás conozcas.

Si el director ejecutivo de tu empresa te contacta con solicitudes urgentes de dinero, credenciales, documentos y otra información, aunque nunca lo haya hecho antes, podría tratarse de un intento de phishing. **Confirma siempre con la persona que quizás conozcas si es ella quien envió el correo electrónico o el mensaje.**

Solicitudes o demandas urgentes.

Los intentos de phishing siempre tienen un sentido de urgencia, como **“pague ahora” o “actúe rápidamente”** y similares, diseñados para hacer que se sienta presionado, distraído y abrumado. **No tome medidas inmediatas e intente evaluar la situación con calma.** Las organizaciones legítimas se comunicarán de maneras que sean fáciles de entender, en un tono neutral y que no evoquen sentimientos de urgencia o miedo.

Enlaces o archivos adjuntos inesperados.

No abra archivos adjuntos ni haga clic en enlaces incluidos en correos electrónicos que no esperaba. Pueden ser maliciosos y dirigirlo a sitios maliciosos. Antes de hacer clic en los enlaces, pase el cursor sobre el texto y, si los enlaces no coinciden con el texto, es posible que se trate de una falsificación. **Los estafadores también pueden acortar las URL para ocultar el verdadero destino del enlace.**

Diseño y ortografía inusuales.

La gramática y la ortografía incorrectas, la estructura de oraciones extrañas y el formato inconsistente son indicadores claros de un intento de phishing. **Las organizaciones legítimas cuentan con personal dedicado a producir, corregir y aprobar cualquier correspondencia, incluidos correos electrónicos, mensajes, boletines informativos y otros.**

Saludos/firmas genéricos.

Los saludos que no incluyen su nombre, como "Señor/Señora", y las firmas sin información de contacto (o información de contacto que no tiene sentido) **son fuertes indicadores de un correo electrónico de phishing.** Las organizaciones legítimas, como bancos, compañías de seguros, servicios de entrega de paquetes y otros, incluirán saludos personales e información de contacto.

Ofertas que parecen demasiado buenas para ser ciertas.

Si una oferta parece demasiado buena para ser cierta, **como grandes cantidades de dinero a cambio de información aparentemente discreta, podría tratarse de un intento de phishing.**

Solicitudes en las redes sociales de personas que no conoces.

Los actores maliciosos recurren a las redes sociales para hacerse pasar por cuentas de empresas e influencers. Ten cuidado con este tipo de mensajes, especialmente si provienen de alguien que no conoces.

Medidas defensivas contra ataques de ingeniería social

Cualquiera puede ser víctima de un ataque de ingeniería social, ya que están diseñados para aprovecharse de las vulnerabilidades humanas. La mejor forma de defenderse de este tipo de ataques es actuar con una mentalidad de "confianza cero": no confiar en nadie y comprobar siempre las fuentes, los mensajes, los archivos adjuntos y demás. Sin embargo, existen algunas **medidas técnicas e interpersonales de defensa** que se pueden adoptar para reducir el riesgo de ingeniería social.

Habilitar filtros de spam

En la actualidad, **la mayoría de los servicios de correo electrónico ofrecen filtros antispam que marcan los correos electrónicos sospechosos como tales,** le advierten antes de abrir un archivo o correo electrónico sospechoso o envían los correos electrónicos previamente marcados como spam directamente a la papelera. Sin embargo, **no confíe únicamente en los filtros antispam y ejerza un pensamiento crítico, desconfíe y adopte una mentalidad de confianza cero.**

Fuente de información: cybernews.com