BOLETÍN DE CALIDAD

UNPHU
Universidad Nacional Pedro Henríquez Ureña

Universidad Nacional Pedro Henríquez Ureña / Vicerrectoría de Desarrollo Institucional, Aseguramiento de la Calidad y Proyectos / Número 29/ Enero 2024

PHISHING

DESCRIPCION GENERAL

El correo electrónico y los servicios de mensajería, como (Skype, Twitter, Snapchat, entre otros) han llegado a ser fundamentales en nuestras vidas como formas primordiales de comunicación. Más allá de su empleo cotidiano en el ámbito laboral, desempeñan un papel crucial al permitirnos mantener vínculos con amigos y familiares. Sin embargo, debido a la extensa dependencia global en estas tecnologías, se han convertido en objetivos primarios de los ciberdelincuentes, dando origen a una táctica de ataque conocida como "phishing". Es fundamental comprender en qué consiste el phishing, así como aprender a identificar y contrarrestar, tales ataques, ya sea en el contexto laboral o en el entorno personal.

¿QUÉ ES EL PHISHING?

El phishing constituye una forma de ataque que se vale del correo electrónico o servicios de mensajería, para engañar al destinatario e inducirlo a realizar acciones inapropiadas. Estas acciones pueden abarcar desde hacer clic en enlaces perjudiciales, compartir contraseñas hasta abrir archivos adjuntos infectados.

RECUERDE

Ante cualquier duda sobre la autenticidad de un mensaje, es preferible comunicarse directamente con la persona u organización utilizando información confiable, en lugar de interactuar directamente a través del mensaje sospechoso. En última instancia, el sentido común es tu mejor defensa.

¿COMO PROTEGERSE?

En la mayoría de las situaciones, no hay inconvenientes en abrir y leer un correo electrónico o un mensaje. Para que un ataque de phishing tenga éxito, los perpetradores necesitan inducirlo a realizar una acción específica. Afortunadamente, existen señales reveladoras que pueden indicar la presencia de un mensaje malicioso.

A continuación mostramos las señales más comunes a tener en cuenta:

- **Urgencia extrema:** Cuando el mensaje demanda una "acción inmediata" bajo amenaza de consecuencias negativas, como el cierre de una cuenta o problemas legales, el atacante busca generar precipitación para que cometas un error.
- **Errores gramaticales u ortográficos:** Mensajes de organizaciones oficiales con mala gramática, ortografía defectuosa o direcciones de correo electrónico personales (@gmail.com) son indicadores de que algo no está bien.
- **Curiosidad excesiva o promesas excesivamente atractivas:** Si el mensaje despierta una curiosidad intensa o promete algo que parece demasiado bueno para ser cierto (como ganar una lotería que no recuerdas haber jugado), es probable que sea un intento de engaño.
- **Saludos genéricos:** Si el saludo del mensaje es genérico, como "Estimado cliente", es sospechoso. La mayoría de las comunicaciones legítimas personalizan el saludo con tu nombre.

CALENDARIO

Capacitación: Norma ISO 21001:2018
Fecha: 12/01/2024
Modalidad: Presencial
Facilitador: Edward Nouel
Dirigido a: Personal Administrativo

CONTACTOS

Vicerrectoría de Desarrollo Institucional, Aseguramiento de la Calidad y Proyectos Ext.2200
Dirección de Aseguramiento de la Calidad Ext. 1025
Correo Electrónico: calidad@unphu.edu.do