SEÑALES DE ALARMA EN UN

Correo de Phishing

REMITENTE

- **Verifica la dirección de correo electrónico:** Los correos de phishing pueden parecer legítimos pero presentan pequeñas variaciones.
- **Dominios sospechosos:** Dominios extraños o que no coinciden son una señal de alerta.

GRAMÁTICA Y SALUDO

- **Saludo personalizado:** Las empresas legítimas usan tu nombre real; un saludo genérico puede indicar phishing.
- **Errores:** Los correos de phishing suelen tener errores gramaticales y ortográficos, a diferencia de comunicaciones oficiales.

De: Microsoft 365 (micros0ft@outlook.com)
Para: usuario@tuempresa.com

Verifica tu cuenta hoy o será bloqueada con fines de privacidad.

Estimado usuario, hemos detectado una actividad inusual en tu cuenta. Es necesario que confirmes tu cuenta con un proceso de verificación para que sigas haciendo uso de nuestros servicios. Haga clic en el siguiente boton para confirmar cuenta:

Confirma tu cuenta

http/verificocinat.ksgw.745382.094udh.com

URGENCIA O AMENAZA

- **Sensación de urgencia**: En correos de phishing con mensajes como "¡Tu cuenta será suspendida!".
- **Amenazas:** De consecuencias si no se actúa de inmediato.

DISEÑO DEFICIENTE

- **Diseño:** Correos mal diseñados pueden ser señal de phishing. Logos y gráficos de mala calidad pueden indicar un correo falso.

DIRECCIONES WEB NO COINCIDEN

- **Desajustes de URL:** Recuerda pasar tu cursor por encima del botón y visualizar la URL en la parte inferior de tu pantalla. Pequeñas variaciones pueden indicar un sitio de phishing.

RECUERDA REVISAR BIEN EL CORREO; ANTE CUALQUIER DUDA, NO HAGAS CLIC EN ENLACES NI DESCARGUES ARCHIVOS Y ¡REPORTA!

TU LOGO AQUÍ

Grupo Smartekh | Security Culture Management

#CybersecurityAwareness