BOLESTIC
Especial Fraude del CEO
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

¿Qué es el fraude del CEO?

El fraude del CEO cae dentro de la categoría del phishing, pero en vez de suplantar a una web conocida, al que se **suplanta es al director general (CEO) de la organización**, o a otro ejecutivo de alto nivel.

Algunos fraudes del CEO usan la ingeniería social, pero la mayoría de los ataques consisten en un compendio de métodos, en vez de uno solo. El objetivo de esta estafa es **convencer a un empleado de que le envíe dinero o información confidencial al atacante,** como propiedad intelectual o credenciales.

Para que la suplantación tenga posibilidades de éxito lo normal es que los ciberdelincuentes hayan **recopilado datos de la organización, de sus correos, utilicen datos de proveedores, etc.** Esta información pueden haberla conseguido mediante ataques previos, comúnmente de phishing, o en fuentes abiertas de Internet. Así, una vez obtenidos algunos datos que les permitan ofrecer credibilidad, tratan de completar el engaño.

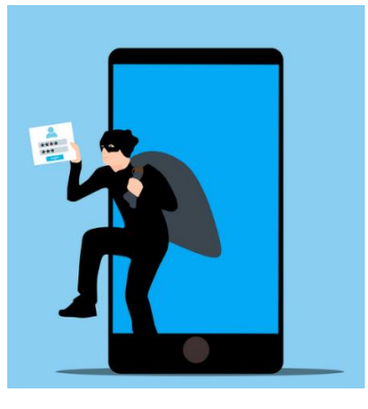
Principales métodos de ataque

La suplantación de identidad en **Correos Electrónicos, SMS** o **WhatsApp,** son los principales métodos de ataque en el fraude del CEO, pero la ingeniería social suele incorporarse a la estrategia para lograr una mayor rentabilidad. Las actividades de reconocimiento que usan las páginas web corporativas y LinkedIn les brindan a los atacantes una gran cantidad de información acerca de la organización, los empleados, nombres y direcciones de correo electrónico de los ejecutivos, así como de sistemas de facturación. Por lo general, los correos electrónicos de phishing se enfocan en empleados en departamentos específicos, como RR. HH. y cuentas por pagar.

Los delincuentes utilizan fotos del alto cargo para hacerse pasar por él, estas imágenes las obtienen de las publicaciones en webs corporativas o redes sociales.

En los casos de ataques más sofisticados, pueden utilizar WhatsApp para enviar mensajes de voz trucados que suplantan la identidad del directivo. Es decir, un deepfake de audio, que es muy complicado de detectar excepto que exista un contacto directo y frecuente con este responsable de la organización.
Os recordamos que en la Administración pública, **no se debe comunicar nada** relacionado con el trabajo mediante ese canal **(WhatsApp)**.

Normalmente, los atacantes insisten mucho en que se trata de algo **confidencial** y, sobre todo, **urgente**; alegando que es importante transferir el dinero para cerrar una operación. Sin embargo, no se debe olvidar que pueden utilizar cualquier otro pretexto, como el pago de facturas de un proveedor o a cualquier regularización de pagos.



Comprueba si tu cuenta de correo está comprometida, https://haveibeenpwned.com/. Si es así, **cambia la contraseña**.

¿Cómo detectar y hacer frente al fraude?

El principal truco para cualquier ataque de phishing es **crear una sensación de urgencia.** Si a la víctima se le da demasiado tiempo para pensar acerca de lo que está ocurriendo, es posible que se dé cuenta de que es una estafa. El atacante usará una dirección de correo electrónico suplantada o creará una dirección legítima que se parezca a la oficial. A causa de la sensación de urgencia, el **usuario objetivo podría obviar las señales de alerta.**

Pasos que puedes seguir para protegerte de este fraude:

- Evitar hacer clic en enlaces o archivos adjuntos en correos electrónicos sospechosos hasta que se verifique que son auténticos.
- Utilizar, siempre que sea posible, autenticación multifactor en las cuentas.
- Disponer de un software de seguridad de correo electrónico avanzado que detecte ataques de ingeniería social por correo electrónico.

Notifica siempre cualquier tipo de actividad sospechosa y comportamientos inusuales que observes.

Puedes usar los siguientes canales de notificación:

- Correo: incidentes.soc@juntadeandalucia.es
- Teléfono: 955 060 974

Ejemplos campañas de fraudes CEO