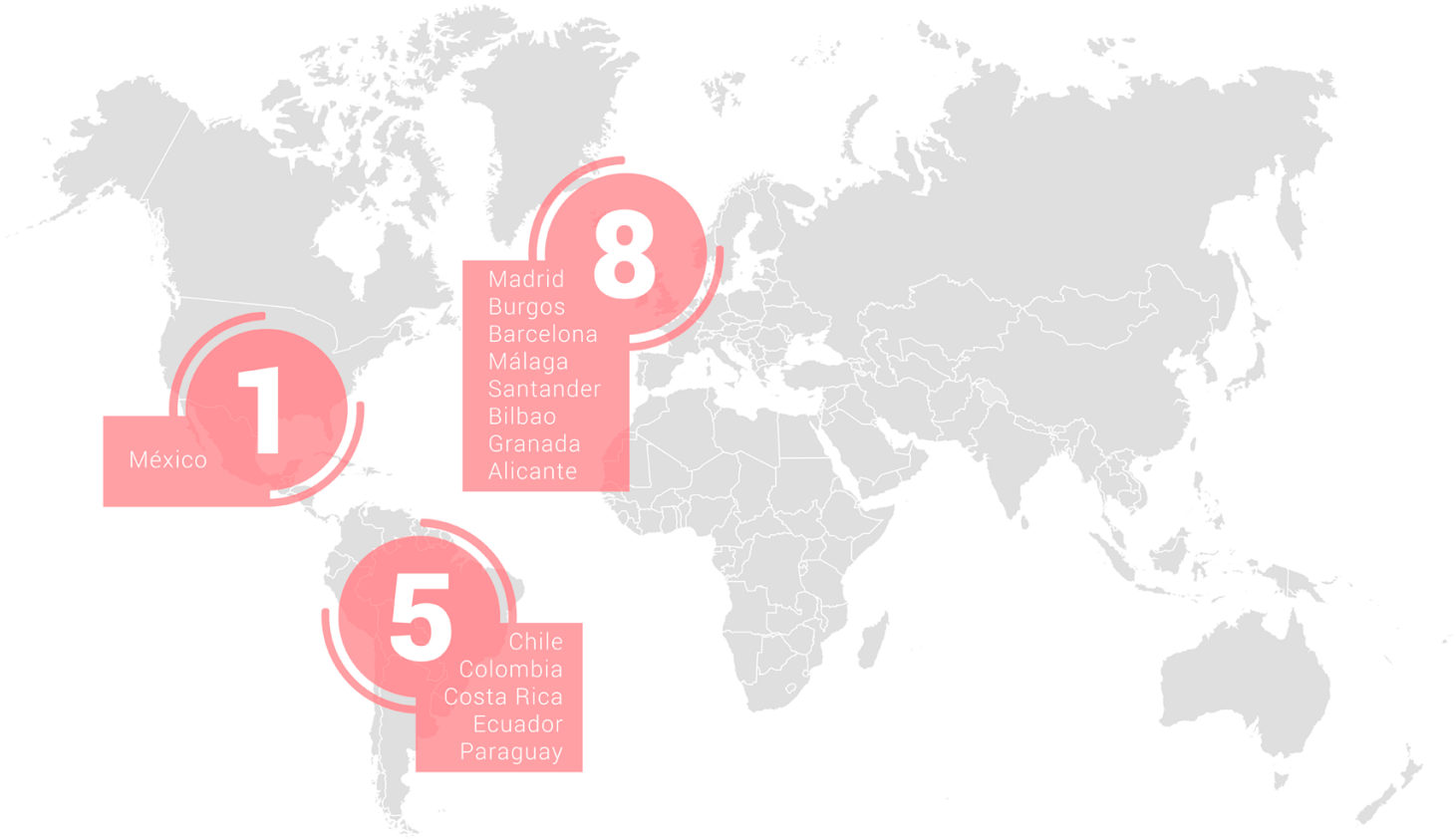
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Qué es Phishing: Tips para protegerse del Fraude



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicado el 10/11/2020 - Actualizado el 21/01/2022

Índice de Contenidos

1. ¿Qué es el Phishing?

Hoy en día recibimos tanto Spam en nuestros correos electrónicos que podemos llegar a abrirlos sin dedicarles previamente unos segundos para comprobar su autenticidad. Hay varios tipos de fraudes electrónicos que se utilizan como elvishing, smishing o phishingpara estafar al usuario pero es posible detectarlos si somos prudentes y conocemos sus formas de actuación.

El Phishing es un tipo de fraude donde el ciberdelincuente finge ser una entidad legítima con el objetivo de intentar robar información privada del usuario,claves de acceso, contraseñas privadas y acceder a datos confidenciales.

Para el engaño se utilizan mensajes de correo electrónico o mensajes de texto que simulan provenir de sitios de total confianza.

2. ¿Cómo funciona este fraude?

El funcionamiento es muy simple pero a la vez ingenioso. La víctima recibe del estafador un email o un SMS que pretender convencerlo para que realice una acción, como puede ser pinchar en un enlace, descargar un pdf, poner claves privadas?

El atacante puede presentarse como una red social que suele visitar, una entidad bancaria, una institución pública con el fin de crear confianza y que el usuario no dude lo más mínimo en realizar lo que se le solicita.

Una vez hemos realizado la acción de incluir nuestra credenciales, el usuario puede aterrizar en un sitio web malicioso que es falso o descargar adjuntos que contienen malware, descargar una aplicación, etc.

3. Estar alerta para detectar la estafa

¿Es posible descubrirlo? El fin último es conseguir nuestra información privada, teniendo eso como premisa, será fácil detectar si el email o SMS es auténtico o es falso.

El hacker intentará atacar a través de diferentes tipos de engaño y para protegerse lo único que tiene que hacer es estar atento a los siguientes puntos:

- Desconfiar de notificaciones que le soliciten sus datos bancarios en pasarelas de pago online,

- Comprobar si los emails tienen urls acortadas, o urls con nombres mal escritos donde suele faltar una letra.

- No atender a emails que contengan amenazas o impliquen sanciones de cualquier tipo.

- No pinchar en enlaces a premios y sorteos donde debe de poner sus datos para que se los manden.

- Vigilar el tipo de emails que contengan urgencia y se deban responder de forma inmediata ya sea descargando un archivo adjunto o visitando un enlace que le dirigirá a una web falsificada por los timadores.

- Sospechar de la promoción de nuevos servicios si debe entrar en su área privada.

- Desconfiar de ofertas de trabajo falsas si ha de poner credenciales.

- No hacer caso a los emails que le informan de que debe cambiar claves de alguna de sus redes sociales (facebook, pinterest, tiktok,tuenti, instagram, linkedln,etc.)

- Sospechar de los emails que informan sobre fallos de seguridad cuando va a ingresar en juegos online.

Las formas de engañar basadas en el Phishing cada vez son más complejas y más convincentes y, a veces, es bastante complejo detectarlas pero no imposible. Recuerde: Siempre que tenga que poner sus datos personales no lo haga a través de un link de un mensaje, vaya directamente a su área de cliente. Pondremos nosotros mismosen el navegador la url del sitio seguro, ya sea su entidad bancaria, la aseguradora, empresas de asistencia en carretera, empresas de telefonía? y accederemos únicamente desde allí.

Para aprender a detectar estos tipos de emails engañosos tendrá que prestar una gran atención antes de responder y descargar archivos.

4. ¿Cómo nos protegemos?

- Instale un Antivirus en su dispositivo para que detecte las posibles amenazas. Estos programas detectan enlaces y archivos maliciosos.

- Bloquee correos no deseados y utilice filtros antispam.

- Verifique que la web que visita es realmente la oficial y no una suplantación.

- Realice acciones de compra en lugares que aporten confianza. Sitios web seguros (https)

- Revise cuentas bancarias a menudo y observe si hay irregularidades o pagos que no realizó.

- Sea prudente siempre que decide abrir un email.

- Es necesario ser consciente de que podemos ser victimas, en cualquier momento, de un fraude en las telecomunicaciones.

5. ¿Ha sido víctima del fraude?

Póngase en contacto con el Soporte de incidencias a través del Instituto Nacional de Ciberseguridad (INCIBE) y el Centro de información y documentación de consumo.

También es posible interponer una denuncia ante la Policíay la Guardia Civil

Consulte a Grupo ACMS si necesita asesoramiento sobre la norma ISO 20000, RGPD, ISO 22301, Hacking ético profesional, Análisis forense informático (Ciberseguridad), certificado ISO 33000, Esquema nacional de seguridad, Protección de infraestructuras técnicas, etc.

Grupo ACMS Consultores implanta Sistemas de Seguridad de la información bajo la Norma ISO 27001. Si deseaadaptar su empresa a la Ley de Protección de Datos LOPDGDDconsúltenos sin compromiso.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com