FREMM
Federación Regional de Empresarios del Metal Murcia

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

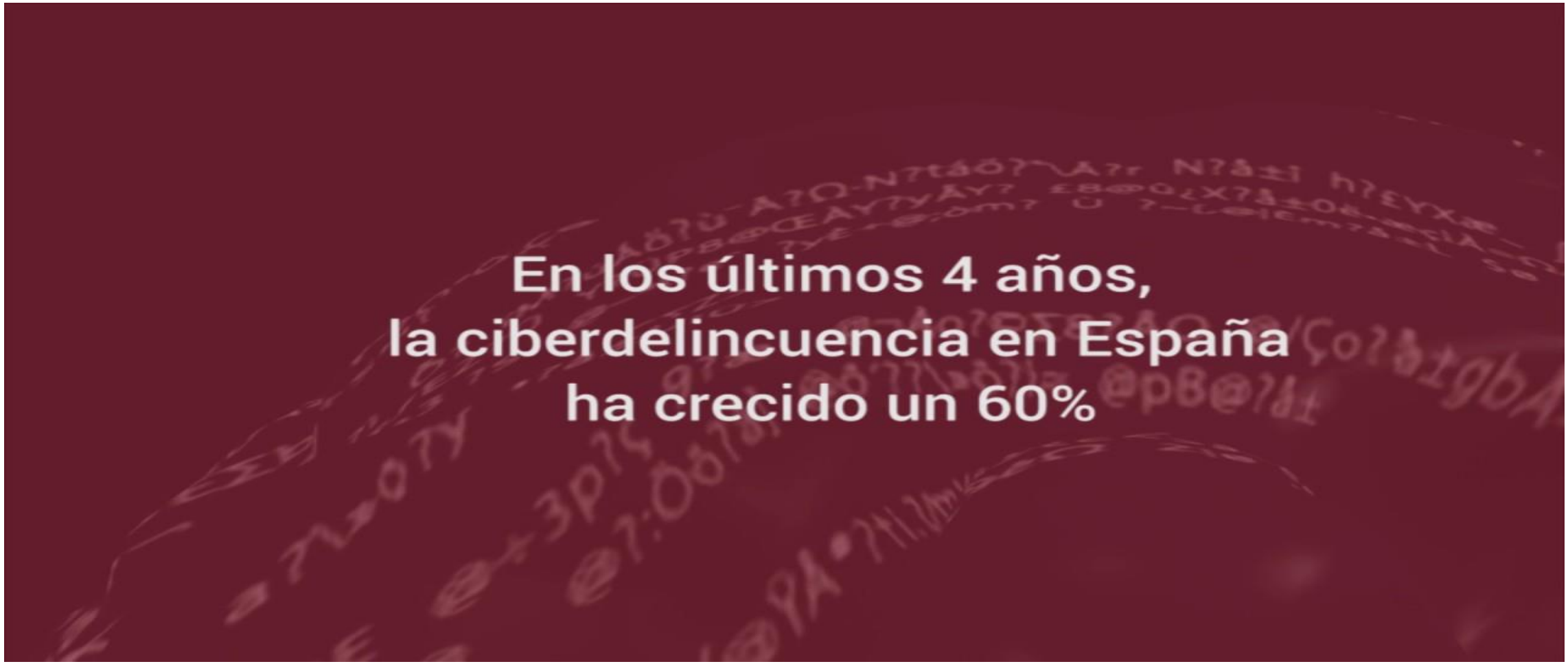
Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

"Cómo proteger a tu empresa del "fraude del CEO"
Elaboración de un plan de seguridad informática

23 DE JULIO DE 2021


LAS CONTRASEÑAS
son como
LA ROPA INTERIOR
5 7 2 5 3
NO
puedes dejar
que nadie la vea
NO
debes compartirla
con extraños
y
debes cambiarla
REGULARMENTE


En los últimos 4 años,
la ciberdelincuencia en España
ha crecido un 60%

EL PAN NUESTRO DE CADA DÍA …

La Policía alerta del último caso de Phishing : un SMS de CaixaBank intenta robar tus datos

ALERTAS POLICÍA NACIONAL

Policía Nacional
@policia

¡ALERTA! #PHISHING

Si recibes un #SMS como este en tu teléfono móvil👉
IGNÓRALO Y BÓRRALO

Ni tu cuenta ha sido desactivada ni tienes que poner tus datos personales para verificarla

#NoPiques

Estafas online

- **Modalidades más frecuentes y formas de prevención**
  - **Phishing**
  - SIM Swapping
  - Tiendas online fraudulentas
  - **Estafa del CEO**
  - Estafa romance
  - Estafas en alquileres de viviendas
  - Falsas ofertas de empleo
  - Fraude online (venta de productos en portales de anuncios)

PHISHING

- La palabra phishing deriva de la palabra inglesa fishing que significa pescar.
- El término en este caso no se refiere a la **pesca** de peces, si no de **datos personales muy sensibles.**
- Por ejemplo, los **números de cuenta bancaria, tarjetas de crédito y contraseñas.**
- Este tipo de **ataques son muy frecuentes en pequeñas y medianas empresas**.

- Su procedimiento es sencillo y se pueden dar **dos escenarios de entrada**:
  - Recibimos un **correo electrónico pidiéndonos realizar una acción**.
    - Si lo hacemos, nos "pescan" los datos.
  - **La web corporativa es atacada y es utilizada como base para enviar e-mails de phishing a nuestros clientes.**
    - Si lo consiguen, tu web se convierte en la "caña" del pescador.

CON ESTO YA NO CAE NADIE …

"El Príncipe Nigeriano te ha dejado en herencia 200 000 euros. Para cobrarla tendrás que hacer un aporte de 3000 euros para cubrir los gastos de envío y de traspaso"

FREMM
Federación Regional de Empresarios del Metal Murcia
OFICINA Acelera pyme
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

INGENIERÍA INFORMÁTICA COMO HERRAMIENTA PARA EL FRAUDE

- X es la gerente de una pequeña empresa en la ciudad de Murcia.
- Al ser una estructura familiar, ella misma es quien realiza los pagos a clientes y proveedores.
- De esta manera, tiene en todo momento el control de la tesorería.
- Es una tarea delicada y prefiere hacerlo ella misma.

ESTAFAS MÁS ELABORADAS …

- Un día, recibe un **correo de su proveedor de e-mail** (Gmail, Hotmail o similar) **diciéndole que su contraseña había sido expuesta públicamente, y que debería cambiarla de inmediato para garantizar su seguridad**.
  - El correo tenía toda la estética de un e-mail oficial (logotipos, tipo de letra, forma del mensaje, color de los botones…) y se fió.
  - Hizo clic y cambió su contraseña.

- A estas alturas, **el hacker ya tiene su contraseña de correo electrónico y accede a su bandeja de entrada con total libertad.**
- Después de investigar, detecta **un correo electrónico legítimo pendiente por leer de un proveedor**.
- Este le solicita el pago de 10.000€, y el mismo e-mail, le indica el número de cuenta donde hacer la transferencia.

- Esta situación es habitual en muchas pymes, pero…
- **¿Qué hace el hacker?**
  - Abre el correo del proveedor, lo edita y modifica el número de cuenta.
  - Lo coloca de nuevo en la bandeja de entrada y lo marca como "no leído".

- Al día siguiente, X accede a su correo y empieza a contestar los correos pendientes.
- Entre ellos, está hacer el pago de 10.000€ a Y, que es el dueño de la empresa de transportes que envía los productos a los clientes de X.
- La factura es el pago mensual de su servicio

- X hace la transferencia con total normalidad, pero al día siguiente…
- Y le escribe reclamando (de nuevo) el pago.
- X le confirma que está procesado, pero él no ha recibido nada.
- Al comprobar los números de cuenta… sorpresa, no coinciden.

- X ha enviado 10.000€ al número de cuenta del hacker de manera voluntaria, lo que complica mucho su recuperación.
- Detectada la estafa, X nos avisa y nos cuenta lo ocurrido.
  - Le indicamos que cambie la contraseña de su correo electrónico de inmediato, siempre a través de la web oficial del proveedor.
  - De esta manera, el hacker deja de tener acceso a su número de cuenta.
- El siguiente paso, es notificar la incidencia al banco y a nosotros.

¿Como podemos detectar un ataque de phishing?

- A pesar de que X disponía de un antivirus legal y actualizado, este no detectó la fraudulencia del correo electrónico.
- Este es uno de los motivos por los cuales la Policía Nacional, informa de lo importante que es **invertir en materia de ciberseguridad**.

FREMM
Federación Regional de Empresarios del Metal Murcia
OFICINA Acelera pyme
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

BUENAS PRÁCTICAS PARA DETECTAR UNA ESTAFA DIGITAL:

- **1. Antivirus instalado y actualizado**
  - Que disponga del módulo de antiphising para correo electrónico y páginas web.
- **2. Sistema operativo legal y actualizado**
  - La falta de actualizaciones son agujeros de entrada para todo tipo de ataques.

- **3. Activa la verificación de dos pasos**
  - Siempre que sea posible en todos tus servicios online.
  - Es una de las mejores maneras para prevenir la intrusión ajena a tu correo.
  - Activar la verificación en dos pasos
    - Abre tu cuenta de Google.
    - En el panel de navegación, selecciona Seguridad.
    - En "Iniciar sesión en Google", selecciona Verificación en dos pasos. Empezar.
    - Sigue los pasos que aparecen en pantalla.

- **4. Adopta una actitud de desconfianza**
  - Ante todo mensaje que te pida contraseñas o datos bancarios (a menudo con urgencia o cuentas atrás).
  - Muchos provienen de grandes y conocidos servicios de compra o pagos online como eBay, PayPal, Amazon o entidades bancarias.
  - Estos suelen ser los grandes preferidos de los atacantes…

- **5. No hagas clic en los enlaces**
  - Sin antes situar el ratón encima y ver la URL exacta y verificar su legitimidad.
  - Un correo electrónico puede parecer legítimo con sus logotipos y colores idénticos a la marca original, pero contener botones que llevan a otros dominios.
  - Además, desconfía de los acortadores de enlaces ya que no sabes donde pueden dirigirte.

- **6. Verifica la validez del certificado SSL**
  - En todas las webs donde introduzcas una contraseña o realices una compra.
  - Encripta los datos para que viajen seguros por la red.

- **7. Comprueba el aviso legal y política de privacidad**
  - En la parte inferior de una web para ver la legitimidad de la propiedad.

Carrefour

Estimado cliente,

La tarjeta Pass (Carrefour) es un servicio ofrecido por la cadena de hipermercados Carrefour, con el cual, podrá optar a realizar sus pagos en la cadena de supermercados cómodamente, en más de 28 millones de establecimientos adheridos, en sus más de 800.000 cajeros con el distintivo VISA, así como beneficiarse de ofertas exclusivas dirigidas a los titulares de la tarjeta Pass (Carrefour).

Tu tarjeta esta desactivada por las nuevas normas de seguridad. Para activar la tarjeta nº .

5499 **** **** **** ****

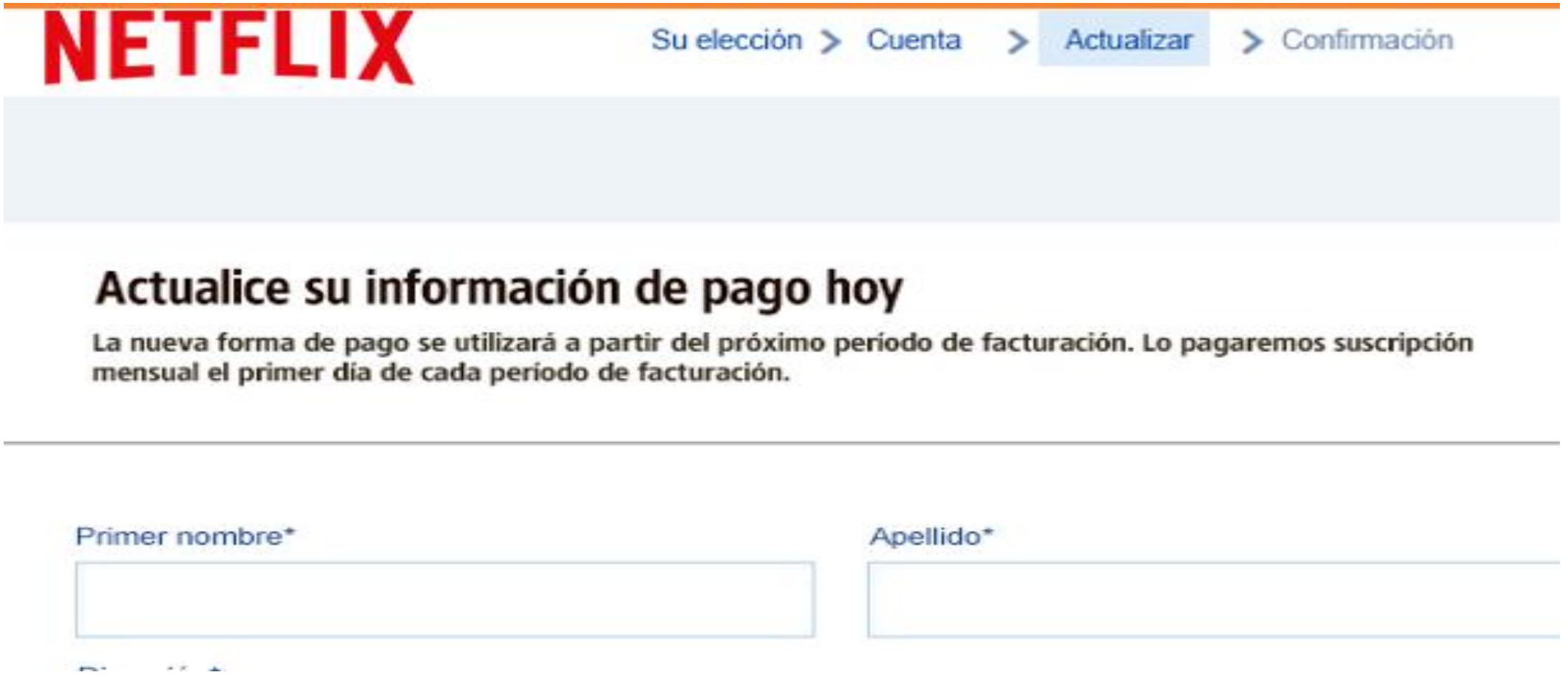
tiene que seguir 2 pasos.

1. Hacer click en el siguiente link
2. Responder al cuestionario

Activar servicios

Saludos,

Carmen Maria Marchal Basalo.


NETFLIX
Su elección > Cuenta > Actualizar > Confirmación
Actualice su información de pago hoy
La nueva forma de pago se utilizará a partir del próximo periodo de facturación. Lo pagaremos suscripción mensual el primer día de cada periodo de facturación.
Primer nombre*
Apellido*

CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

FREMM
Federación Regional de Empresarios del Metal Murcia

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

Estafa del CEO

Hay once detenidos

Roban 2,4 millones de euros con la estafa del CEO que puede arruinar una empresa

Esta organización criminal realizaba fraudes a través de las nuevas tecnologías valiéndose de métodos de ingeniería social.

La estafa del CEO: el coronavirus resucita el timo que puede arruinar a una empresa

El caso de Murcia

Durante los meses de abril y mayo, en plena pandemia del **coronavirus**, una empresa comercializadora de **productos sanitarios** solicitó a un proveedor la adquisición de **4 millones de mascarillas** efectuando para ello un primer pago a una cuenta bancaria.

Fue días más tarde, y a través de un correo electrónico, cuando se intentó llevar a cabo el fraude. La empresa que había llegado a un acuerdo con el proveedor para la adquisición de las **mascarillas** durante la crisis del **coronavirus** recibía un nuevo correo en donde se solicitaba el cambio de número de cuenta para efectuar un nuevo pago que ascendía a 870.000 euros.

Era la estafa por el método del **fraude del CEO o BEC**, los **ciberdelincuentes** habían **suplantado la identidad** del proveedor original para solicitar una transferencia bancaria.

La empresa víctima se dio cuenta de que habían sido estafados al comprobar por otro medio que la transferencia nunca había llegado al proveedor y rápidamente, se puso en contacto con la **Policía Nacional.**

- **Proceso :**
  - 1.-**'Hackear' la cuenta de correo electrónico** de altos directivos/proveedores de la empresa/AAPP, para acceder a sus datos confidenciales, monitorizar y analizar sus gestiones económicas y suplantar su identidad.

- 2.- Envío de uno o varios correos (del **suplantador del CEO/proveedor al contable**), con el **objetivo final**: generar un traspaso de dinero o modificar cuentas bancarias para una operación en curso (a una cuenta fraudulenta).

- El motivo de la transferencia es hacer frente a un **pago urgente y muy necesario** de la asociación/AAPP o de bien de una factura pendiente de pago de una empresa.
- La transferencia se hace por contables de empresas o tesoreros de ONG/AAPP que caen en la "trampa" a **cuentas**, normalmente **extranjeras**.
- Hecha la transferencia, el dinero se **mueve rápidamente por muleros** (criptomonedas, de bancos nacionales a bancos extranjeros, etc.)

Prevención

- **Revisar en el correo recibido** las mínimas diferencias de dirección respecto del contacto y el posible **distinto trato del habitual** con el que la persona se relaciona habitualmente.
- **Comprobar SIEMPRE, física o telefónicamente**, con el requirente de transferencia, la **cuenta de destino, su importe y motivo.**

- Tratar de establecer un **sistema de doble firma** para hacer pagos, que imponga la aceptación de, al menos dos personas, para que una empresa autorice transacciones (**protocolo interno de pagos)**.
- Atención a la falsificación de **facturas**: se modifica ésta, **con otro número de cuenta**.
  - Comprobar que las transferencias **nacionales comienzan por ES**.
  - Falsificación **exclusivamente del número** de cuenta en la factura. Lo demás suele ser correcto.

FREMM
Federación Regional de Empresarios del Metal Murcia

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

CONTACTAR EN CASO DE DUDAS

- **Jefe Sección Unidad Delincuencia Especializada y Violenta (UDEV)**
  - Miguel Marcos Castro Martín
  - 652 544 238
  - marcos.castro@policia.es

FREMM
Federación Regional de Empresarios del Metal Murcia

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

DUDAS

MUCHAS GRACIAS POR SU ATENCIÓN

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE LA POLICÍA