¡ Maldito Phishing !

Últimamente cada vez nos encontramos más correos conocidos como phising sobre todo este 2020 que parece que existe un aumento en este tipo de estafas en internet. En este artículo analizamos este problema.

¿ Qué es el Phising ?

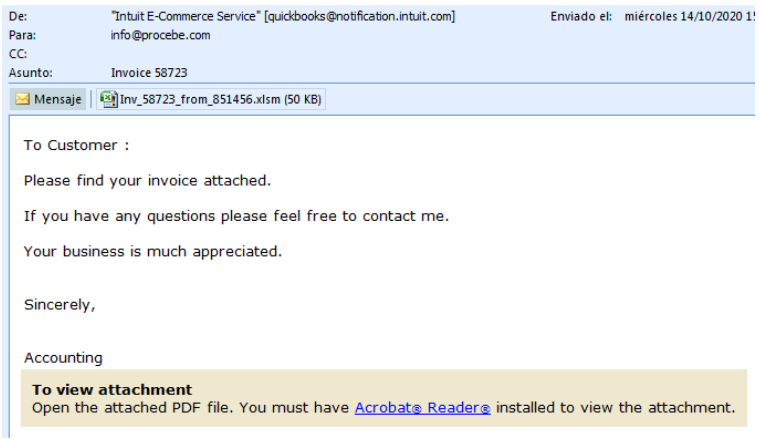
Si citamos a la wikipedia podemos definir el Phising como ***término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace…..***

El contacto más habitual que tenemos con el phising son esos correos electrónicos que recibimos con frecuencia con mensajes de **entidades de confianza** (bancos conocidos, empresas de suministro eléctrico, correos, empresas de mensajería, etc e incluso organismos oficiales) que nos hacen referencia a algún tema que tenemos pendiente. Puede coincidir con alguna empresa con la que verdadera relación y que en un primer momento salven la barrera de desconfianza mediante técnicas conocidas como de ingeniería social.

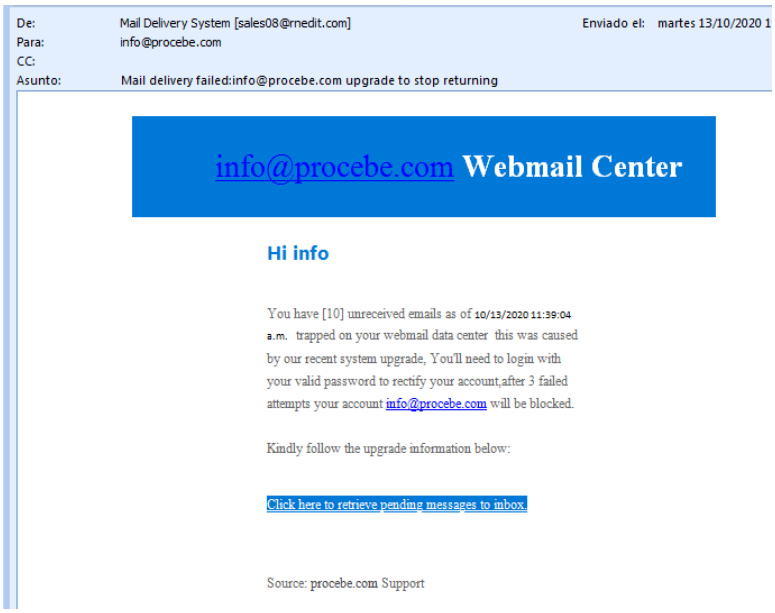
En este artículo nos centraremos en este último caso. Los **email suplantadores** de una identidad que nos llevan a realizar alguna acción

Me gusta establecer una **clasificación** muy personal

- Email en inglés, email en español latino (si eres español), emails pobremente estructurados. Estos los solemos descartar automáticamente, salvo que, efectivamente, mantengamos relación con proveedores o suministradores de servicios de otros países. Entre los latinos podemos notar que no corresponde el tono o lenguaje al habitual de la empresa e incluso nos encontramos con faltas graves de ortografía.



- **Mensajes de email rechazado** . Mail Delivery System. Aunque son en inglés, los pongo aparte. Porque es algo que podemos recibir habitualmente de forma lógica y pueden confundirnos, relajando nuestra vigilancia. En el mensaje tipo Phising vemos que el diseño puede no corresponde a nuestro proveedor de correo habitual. Normalmente en estos correos (los verdaderos) ya solemos en el texto saber a qué destinatario corresponde el error de envío. No necesitaríamos acceder a ningún adjunto o enlace


De: Mail Delivery System [sales08@rnedit.com] Enviado el: martes 13/10/2020 1
Para: info@procebe.com
CC:
Asunto: Mail delivery failed:info@procebe.com upgrade to stop returning

info@procebe.com Webmail Center

Hi info

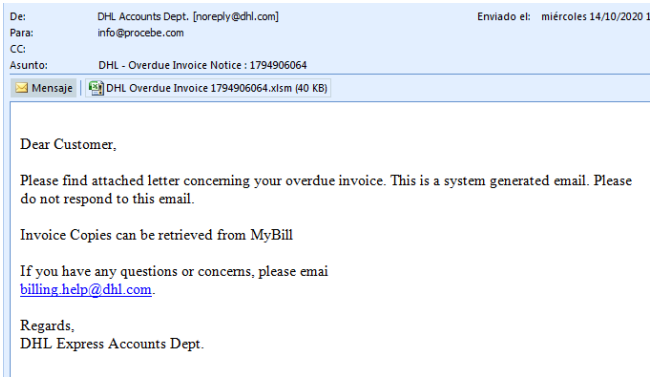
You have [10] unreceived emails as of 10/13/2020 11:39:04 a.m. trapped on your webmail data center this was caused by our recent system upgrade, You'll need to login with your valid password to rectify your account,after 3 failed attempts your account info@procebe.com will be blocked.

Kindly follow the upgrade information below:

Click here to retrieve pending messages to inbox

Source: procebe.com Support

- Email de empresas con las que **no mantenemos relación** pero que parecen verdaderos. Están bien estructurados (buen diseño, logos corporativos, etc). Pueden ser comunicaciones, por ejemplo de un banco, una operadora telefónica, empresas de fuera de nuestro sector o localicad, etc pero sabemos que no tenemos relación con ellos lo cual debe ser motivos para sospechar que sean phising


De: DHL Accounts Dept. [noreply@dhl.com] Enviado el: miércoles 14/10/2020 1
Para: info@procebe.com
CC:
Asunto: DHL - Overdue Invoice Notice : 1794906064
Mensaje | DHL Overdue Invoice 1794906064.xlsm (40 KB)

Dear Customer,

Please find attached letter concerning your overdue invoice. This is a system generated email. Please do not respond to this email.

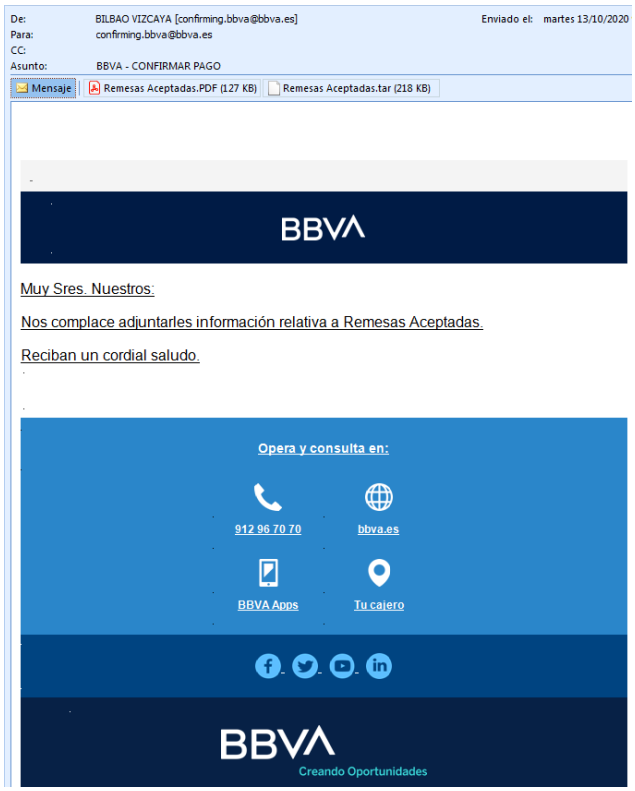
Invoice Copies can be retrieved from MyBill

If you have any questions or concerns, please emai
billing.help@dhl.com.

Regards,
DHL Express Accounts Dept.

- Email de empresas con las que podríamos tener **relación esporádica**: mensajerías, bancos que comunican transferencias a nuestro favor, etc. Aquí debemos ser cautos y garantizarnos que en el texto del mensaje tenemos confirmación de identificación del agente de confianza (proveedor, cliente, etc) que nos haga creer con **absoluta seguridad** que el mensaje tiene relación con él

- Email de las empresas con las que nos relacionamos: nuestros proveedores, clientes, bancos, etc. Esto se pone interesante. Debemos sospechar si no es el canal de comunicación habitual de este interlocutor. **Ser muy prudentes** si es algo no esperado y en caso de duda no abrir adjuntos ni pinchar enlaces del mensaje.



Este sería un buen ejemplo. El mensaje está bien diseñado copiado de un correo verdadero e incluso los enlaces incluidos y el remitente son correctos. Cualquiera, repito cualquiera puede mandar un correo con la dirección de otro remitente de forma muy fácil (no es garantía de legitimidad). El daño viene en los adjuntos uno es inofensivo, el pdf (hace ganar legitimidad) pero el otro es un archivo comprimido que al abrirlo….bueno, mejor ni probarlo

- Email de organismos públicos, suministradores. Estos los veo los más peligrosos. A lo largo de los años me he encontrado en mis clientes este tipo de mensajes. Los definiría como mensajes que **nos remueven las tripas**. Nos mueven los sentimientos y anulan nuestra razón. Es sabido que cuando nuestro cerebro está sometido a una emoción nuestra razón se ver perturbada (ver el libro Inteligencia Emocional de Daniel Coleman. Pondré algunos ejemplos.

    - Correos de un suministrador habitual: compañía eléctrica, compañía de telecomunicación, de alojamiento, etc. Recibimos un mensaje con aparente estética de la compañía en cuestión. Y tenemos en el texto el aviso de que se nos va a cargar una cantidad económica desorbitada en nuestra próxima factura y nos pone un enlace para descargar la factura en cuestión o incluso un archivo adjunto. Nuestra primera reacción es de ira, nos agarramos un cabreo monumental y pulsamos en el enlace **cegados por la rabia**. Ya está, ya hemos caído.

    - Mensaje de una institución pública: Hacienda, Ministerio de Trabajo, etc. En este caso se nos avisa de un cargo de hacienda, una sanción o apertura de expediente, Una inspección de trabajo, etc. En este caso movidos por el **miedo** nuestra razón se manda a mudar y pinchamos en la trampa

    - Email de premio, recompensa, etc. Aquí es la **codicia** la responsable a veces la necesidad. Se nos anuncia un ingreso, un cheque regalo o alguna clase de

recompensa. Y allí se va de nuevo nuestro raciocinio de vacaciones. Más canalla me parece el que, aprovechándose de la necesidad de la víctima, ofrece ofertas laborales fraudulentas.

Consecuencias del phising

Ya sea por un seguir un enlace del correo o por abrir un archivo adjunto podemos encontrarnos varios tipos de daño:

Infección vírica: Ejecutamos inconscientemente un virus que puede infectar nuestro ordenador. Generalmente de tipo ramsonware que provoca el encriptamiento de nuestros archivos solicitándonos un rescate para recuperar nuestros datos.

Robo de identidad. Un enlace nos lleva a una supuesta pantalla de acceso de la empresa remitente (banco, organismo público, etc) lo que si tecleamos nuestras auténticas credenciales procederán a utilzarlas fraudulentamente

Robo de información sensible. Acceso a nuestro ordenador consecuentemente a nuestros datos almacenados en él.

Resumiendo, tengamos en cuenta lo siguiente:

1. **Ingenuidad cero**, Analizar cada correo con cautela, leer el mensaje con detenimiento. Nadie da duros a cuatro pesetas. Hoy en día es raro no recibir a diario correos de este tipo

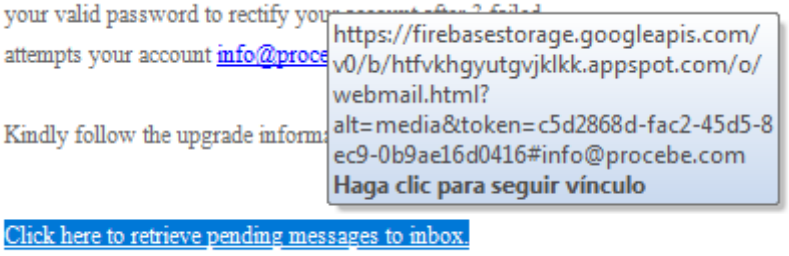
2. Nuestro banco o proveedor **nunca nos pedirá credenciales de acceso vía email**

3. Las comunicaciones de organismos oficiales suelen llegar por otro canal para garantizarse **el acuse de recibo** si bien en verdad que con las notificaciones electrónicas nos puede llegar el aviso de llegada de notificación que siempre se recibirá en la página web del organismo correspondiente.

4. Tener la sana costumbre de que para **conectarnos a cualquier sitio que requiera credenciales** (usuario, contraseña): bancos, tarjetas de créditos, organismos oficiales, etc, hacerlo usando el **navegador** a ser posible con enlaces almacenados en nuestros favoritos no a través de enlaces en emails

5. Recordar que está vigente la nueva **ley de protección de datos** y sólo deberíamos recibir correos de empresas a las que les hayamos dado la autorización correspondiente.

6. Si pasamos el puntero del ratón por encima de los enlaces propuestos en el mensaje nos encontraremos con **direcciones extrañas** que no corresponden al remitente de forma inequívoca o muy sospechosas



7. En caso de duda **contactemos con el remitente** para garantizarnos su autenticidad

Para cualquier consulta sobre el tema o si te ves afectado puedes contactactar libremente con un servidor: jcebollero@procebe.com