UNIDAD DE PARTICIPACIÓN CIUDADANA POLICÍA NACIONAL JEREZ

PREVENCIÓN CONTRA DELITOS A TRAVÉS DE INTERNET CRISIS COVID 19

OCTUBRE de 2020

La Policía Nacional informa de las características básicas de algunos tipos de delitos de los que se ha detectado un fuerte incremento durante la presente crisis Covid 19, **CONCRETAMENTE CIBERDELITOS**; **estafas, timos, engaños y difusión de virus informáticos,** que se han reproducido en **INTERNET** utilizando en su mayoría como vía de difusión el **correo electrónico,** pero también las **aplicaciones de mensajería instantánea.**

ESTOS DELITOS CONSISTEN EN:

Los delincuentes **suplantan la identidad corporativa** de entidades públicas como el **Ministerio de Trabajo y Economía Social, la Dirección General de Tráfico, Agencia Tributaria, Ministerio de Seguridad Social, etc...,** y privadas de reconocido prestigio como **empresas de telefonía, empresas de suministros, etc...**, y realizan un envío masivos de e-mails, haciéndose pasar por estas instituciones con la intención de engañar a los destinatarios para obtener sus datos personales y bancarios.

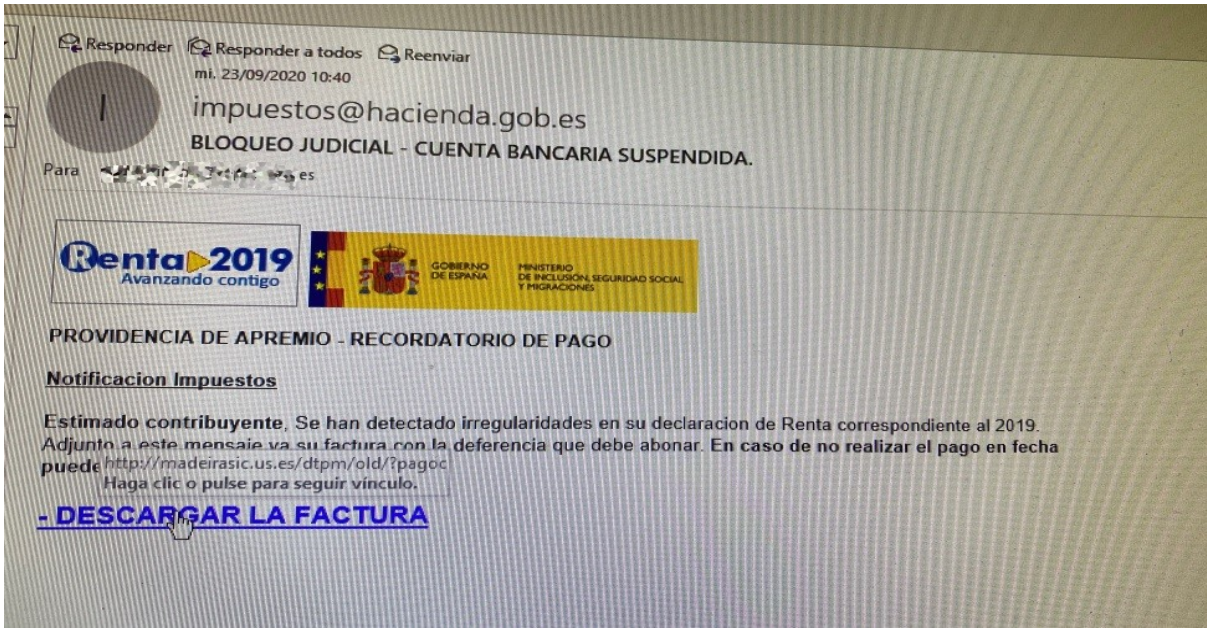
Estos envíos masivos afectan en mayor medida a empresas, empresarios, autónomos, profesionales liberales de todo tipo, tanto en sus e-mails de empresa como personales y privados.

También afecta a otros ciudadanos particulares de todo ámbito.

El engaño siempre consiste en asustar o amenazar veladamente o abiertamente al destinatario con situaciones o problemas irreales, por ejemplo: **indican bloqueo de cuantas bancarias por error o deuda de la víctima, supuestas deudas con hacienda, con la agencia tributaria, etc...**

En la gran mayoría incluyen en el mail malicioso un enlace "link" (texto en azul que permite con solo click redirecionar a otra página o comenzar una descarga) con tan solo la intención de descargar software malicioso, por todos conocidos como virus (malware) o te llevan a páginas falsificadas donde piden rellenar datos personales o bancarios.

EJEMPLO 1.



En este caso suplantan a Hacienda y al Ministerio de Inclusión, Seguridad Social y Migraciones alegando una supuesta deuda del receptor e incluyen un enlace (link) para descargar una falsa factura.

EJEMPLO 2.

En este otro caso se hacen pasar por la Agencia Tributaria y alegan una ***"denuncia contra su empresa por una deuda"*** adjuntando de igual forma un "link" malintencionado que indica: ***"haga click aquí para ver los documentos en línea"***

EJEMPLO 3.

En este tercer ejemplo de e-mail falso avisan de **un falso bloqueo de la cuenta bancaria de la víctima**, y de igual forma, incluyen un enlace para, de forma falsa, descargar un supuesto comprobante fiscal digital.

EJEMPLO 4.

En este caso **simulan la identidad de la DGT para comunicar una supuesta multa de tráfico** a la víctima y un "link" para que pueda visualizarla, de nuevo es otra falsedad y excusa para que el receptor descargue el virus en el enlace.

EJEMPLO 5.

Envían a las víctimas un correo email suplantando la identidad de su entidad bancaria, en el mismo exponen la excusa falsa de **"...se ha producido un error y es necesario realizar una "*actualización de seguridad*",** en el que le redirecionan a una página web falsa que simula la aplicación de banca on line de la entidad bancaria de la víctima y en la que le solicitarán sus datos bancarios, incluidos números *pin* de accesos o numero de tarjeta de crédito o débito, con fecha de caducidad y número de control.

Si las víctimas caen en el engaño se les realiza una transferencia inmediata a otra cuenta donde el dinero desaparece en escasos minutos.

PARA EVITARLO SE RECOMIENDA:

- NO CREER ESTAS COMUNICACIONES, NINGUNA EMPRESA PÚBLICA O PRIVADA PEDIRÁ DATOS PERSONALES O DE LA EMPRESA A TRAVÉS DE MEDIOS INFORMÁTICOS O TELEFÓNICOS.

Pero.... **¿cómo podemos detectar que se trata de una comunicación maliciosa?**

1. ¿Esperaba un mail de esa entidad? Si no es así, desconfíe.

2. Compruebe que el email corresponda con la entidad que dice y alega ser. Busque en las páginas oficiales de estas entidades.

3. ¿Es un tema impactante y alarmante? Si es así desconfíe, la mayoría de estas estafas usan temas muy llamativos para captar la atención de sus víctimas.

4.¿Cuál es el objetivo del correo? Ninguna entidad le pedirá datos personales, si es un texto que transmite urgencia, que es amenazador o vende ofertas muy atractivas....desconfíe.

5. Fíjese en la redacción. Si observa faltas ortográficas o gramáticas, mala sintaxis o formas de componer las frases que no corresponden con el castellano, también fíjese en las instituciones que menciona, si no existen o no corresponden con las españolas (Ej: en la estafa donde suplantan a la DGT se refieren a un supuesto *"tribunal de faltas"* que no existe en España.

6. Mucho cuidado con los enlaces "links" y las páginas a las que redirigen. Tan sólo con poner el cursor encima de estos enlaces, sin llegar a clickar, se puede ver el dominio web de destino, en muchas ocasiones el usuario ya se puede percatar que no corresponden con lo que dicen.

7. Nunca bajo ningún concepto descargar ningún archivo adjunto a estos "links", en su 99% contienen virus malware tipo gusano troyano.

¿QUÉ HAGO SI YA HE DESCARGADO ESTOS VÍRUS Y TENGO EL SISTEMA INFECTADO?

Si ya ha descargado y ejecutado el archivo malicioso, es posible que su dispositivo se haya infectado. **Para proteger tu equipo debe escanearlo con un antivirus actualizado o seguir los pasos que encontrará en páginas web especializadas como INCIBE,** o en su caso que le indiquen profesionales de la informática los pasos a seguir para la desinfección de dispositivos.

Si no ha ejecutado el archivo descargado, posiblemente su dispositivo no se habrá infectado. Lo único que debe hacer es **eliminar el archivo que encontrará en la carpeta de descargas**. También **deberá enviar a la papelera el correo de tu bandeja de entrada y eliminarlo de la propia papelera.**

¡USE SU SENTIDO COMÚN!,

HABLE CON SUS FAMILIARES, COMPAÑEROS DE TRABAJO, EMPLEADOS, ETC... PARA ACORDAR FORMAS DE ACTUACIÓN CONJUNTAS Y SIMILARES ANTE CORREOS SOSPECHOSOS

Los cuatro ejemplos son estafas recibidas por empresas y ciudadanos de Jerez (Cádiz)

Ante cualquier duda, sospecha o incidencia, contactar con la Unidad de Participación Ciudadana en los teléfonos 956326986/856305780, o al 091 ante cualquier incidente de carácter urgente.

PARTICIPACIÓN CIUDADANA
POLICÍA NACIONAL

DELEGACIÓN DE PARTICIPACIÓN CIUDADANA
JEREZ DE LA FRONTERA

Comisaría Local de Jerez de la Frontera

JEFATURA SUPERIOR DE POLICÍA DE ANDALUCÍA OCCIDENTAL

Avenida de la Universidad nº 10,
11406 Jerez de la Frontera (Cádiz)

jerezfrontera.participacion@policia.es
956326986 / 856305780