somos digital

Día de Internet

17 DE MAYO DE 2022

#diadeinternet

Seguridad y protección ante los fraudes más comunes

Dédalo FUNDACIÓN

Webinar impartida por: Salvador Real

"Por un uso seguro, responsable y respetuoso de la tecnología".

QUÉ VAMOS A VER...

Contenido

- Precauciones y consejos para protegerse.
- Tipos de fraudes.
- Phishing.
- Compras online.
- Alquiler de viviendas.
- Búsqueda de empleo.
- ¿Qué puedo hacer?

PRECAUCIONES Y CONSEJOS

Dispositivo actualizado y protegido. Todo el software instalado en el dispositivo debe estar **actualizado.** También es recomendable tener instalado en el dispositivo un **antivirus** para evitar algunas clases de malware que son capaces de recolectar información personal y bancaria.

Utilizar una red segura. Cuando vayamos a realizar una visita web, indistintamente de la tienda sea cual sea, es importante hacerlo desde una red confiable como por ejemplo la de nuestra casa. No es recomendable efectuar una compra desde una **RED WIFI PÚBLICA** como la de un bar ya que alguien podría estar interceptando las comunicaciones y con ello posiblemente nuestros datos personales y bancarios.

Evitar el uso de ordenadores, tabletas y teléfonos inteligentes públicos o compartidos para realizar compras online. Generalmente no podemos conocer su estado de seguridad o la finalidad de su uso (las páginas por las que se ha navegado), y podrían contener virus o cualquier otro tipo de código malicioso.

Revisar los programas y las apps instaladas y eliminar todas aquellas que no se estén utilizando. Cuantas más tengamos, más difícil será mantener nuestro equipo actualizado y protegido, además de ralentizar y entorpecer su rendimiento.

PRECAUCIONES Y CONSEJOS

HTTPS. Aunque en las tiendas online no es necesario que todas las páginas de la web comiencen por HTTPS, es decir, que la información que se transmite esté cifrada, sí que tienen que contar con cifrado o https en algunas partes. En el formulario de contacto o cuando tengamos que **introducir información bancaria,** como el número de tarjeta.

Certificado de seguridad. Además de que la dirección comience por https, el certificado de seguridad que tiene, debe coincidir con el sitio donde estamos navegando, de esta manera se identifica inequívocamente que el sitio web es el que debería ser y no uno ilegítimo.

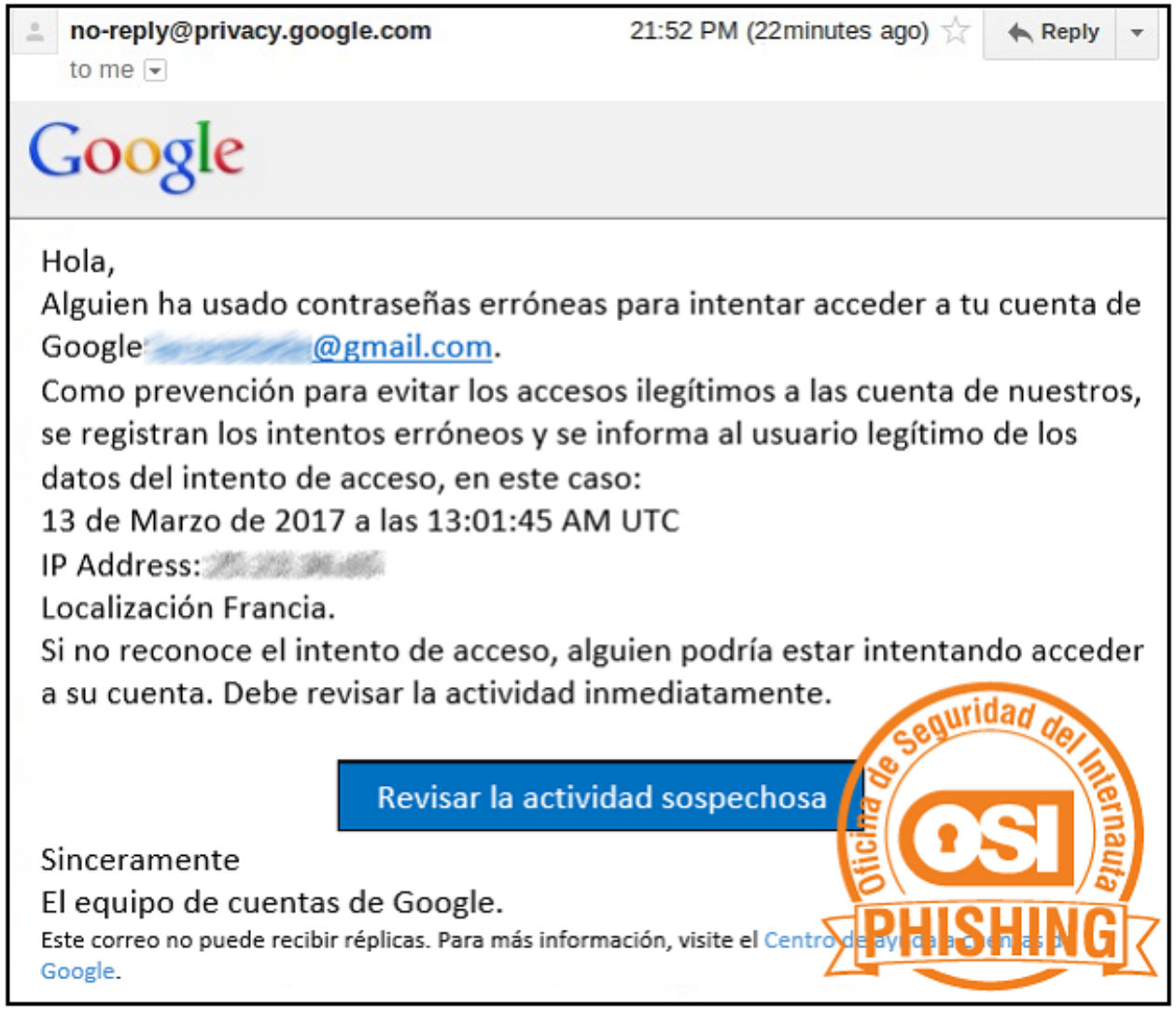
Teclados virtuales al introducir datos bancarios. Un teclado virtual es un tipo de *software* que simula ser un teclado convencional y su funcionamiento se hace por medio del ratón, su uso es muy común en banca online. Algunas clases de *malware* son capaces de capturar las teclas que presionamos en el teclado y enviar ese texto a los ciberdelincuentes. **Windows** incorpora un teclado virtual como complemento en su sistema operativo aunque también es posible utilizar otro tipo de *software* como por ejemplo extensiones para los navegadores.

TIPOS DE FRAUDES

FRAUDES

- **Filtración de datos**: se filtra información confidencial (personal o financiera) desde una locación segura a un entorno no confiable.
- **Programa malicioso o malware**: software diseñado para dañar computadoras y sistemas informáticos.
- **Phishing o spoofing**: estafadores utilizan correos electrónicos falsos, mensajes de texto o un sitio web de imitación para intentar robar su información personal o su identidad.
- **Fraude en subastas por internet:** implica la tergiversación de un producto anunciado en un sitio de subastas por Internet.
- **Fraude con tarjeta de crédito**: los estafadores obtienen dinero o bienes de manera fraudulenta, a través del uso no autorizado del número de una tarjeta de crédito o débito.

PHISHING



no-reply@privacy.google.com 21:52 PM (22minutes ago) Reply

to me

Google

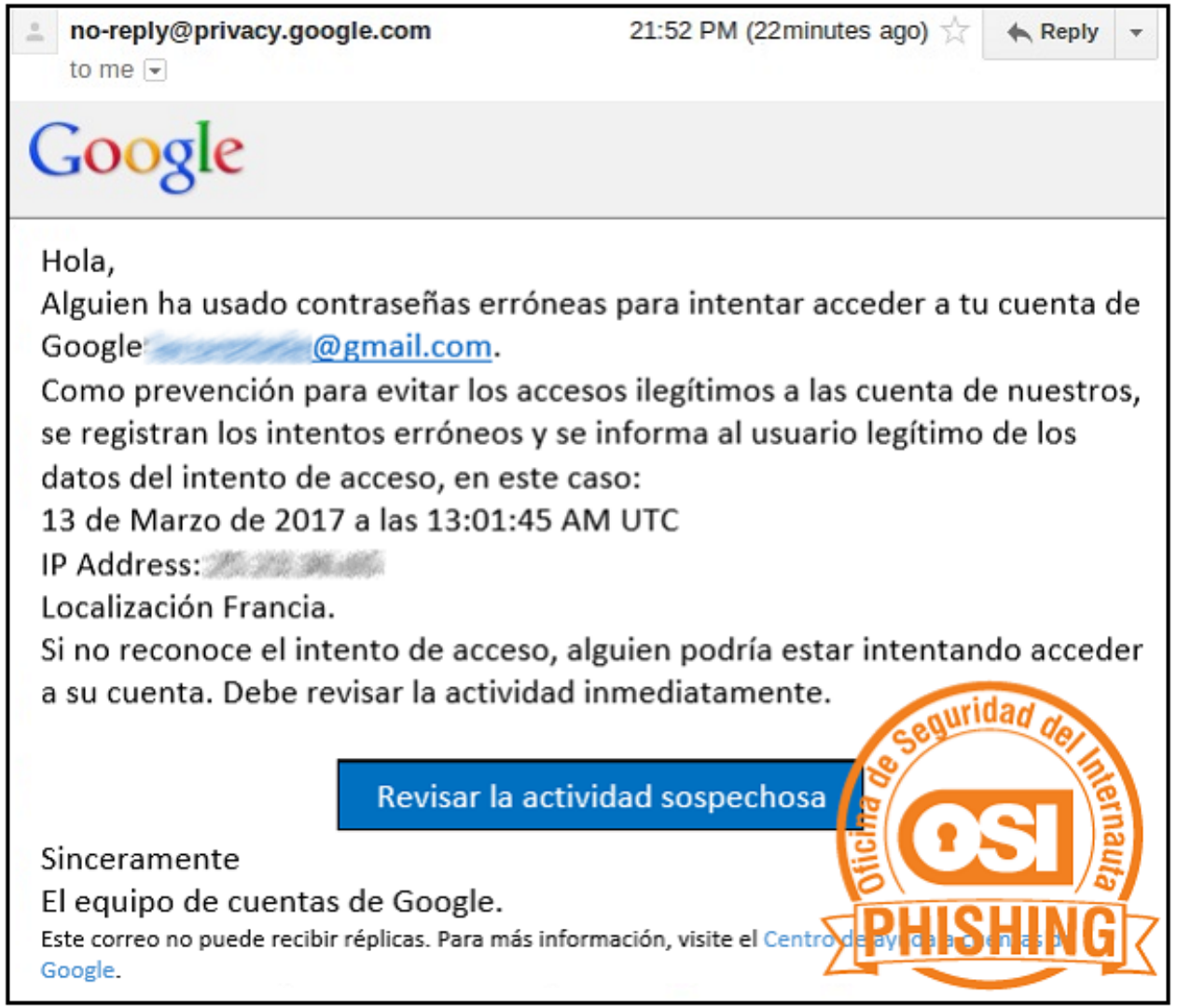
Hola,
Alguien ha usado contraseñas erróneas para intentar acceder a tu cuenta de Google [redacted]@gmail.com.
Como prevención para evitar los accesos ilegítimos a las cuenta de nuestros, se registran los intentos erróneos y se informa al usuario legítimo de los datos del intento de acceso, en este caso:
13 de Marzo de 2017 a las 13:01:45 AM UTC
IP Address: [redacted]
Localización Francia.
Si no reconoce el intento de acceso, alguien podría estar intentando acceder a su cuenta. Debe revisar la actividad inmediatamente.

Revisar la actividad sospechosa

Sinceramente
El equipo de cuentas de Google.
Este correo no puede recibir réplicas. Para más información, visite el Centro de ayuda a [redacted] de Google.

El primer paso es valorar el **contenido del mensaje**. Como hemos mencionado anteriormente, el intento de suplantación puede ser a un banco, una plataforma de pago, una red social, un servicio público, etc.

PHISHING



no-reply@privacy.google.com 21:52 PM (22minutes ago) Reply

to me

Google

Hola,
Alguien ha usado contraseñas erróneas para intentar acceder a tu cuenta de Google [redacted]@gmail.com.
Como prevención para evitar los accesos ilegítimos a las cuenta de nuestros, se registran los intentos erróneos y se informa al usuario legítimo de los datos del intento de acceso, en este caso:
13 de Marzo de 2017 a las 13:01:45 AM UTC
IP Address: [redacted]
Localización Francia.
Si no reconoce el intento de acceso, alguien podría estar intentando acceder a su cuenta. Debe revisar la actividad inmediatamente.

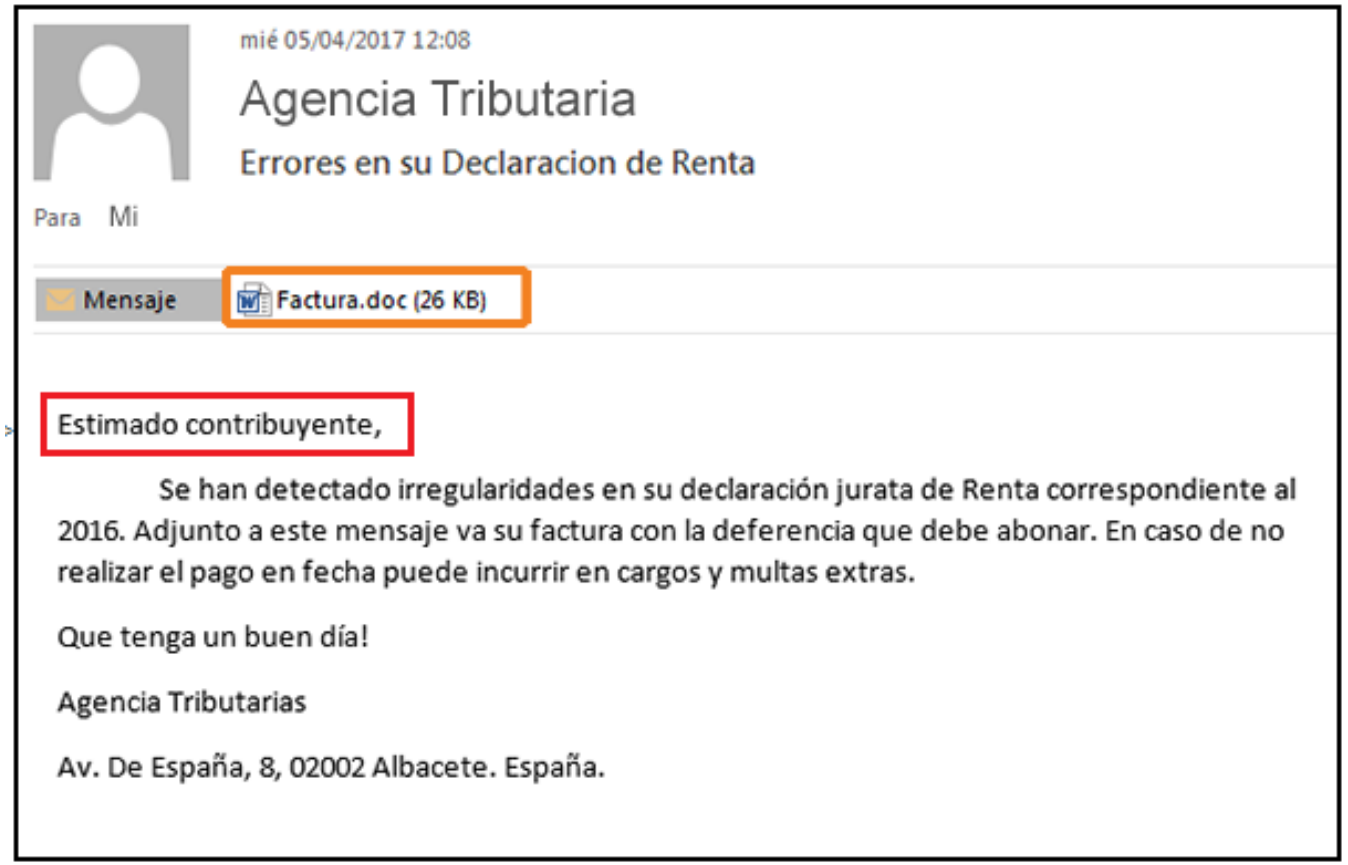
Revisar la actividad sospechosa

Sinceramente
El equipo de cuentas de Google.
Este correo no puede recibir réplicas. Para más información, visite el Centro de ayuda [illegible] Google.

Si detectamos que el correo tiene una ortografía pobre y su escritura es informal, debemos estar alerta.

- **Fallos semánticos**: artículos “el” o “la” intercambiados.
- **Palabras con símbolos extraños**: donde deberían estar palabras acentuadas como por ejemplo: “DescripciÃ?n”. Este caso aparece al intentar escribir vocales acentuadas en un teclado no español.
- **Frases mal construidas**.

PHISHING



mié 05/04/2017 12:08

Agencia Tributaria

Errores en su Declaracion de Renta

Para Mi

Mensaje Factura.doc (26 KB)

Estimado contribuyente,

Se han detectado irregularidades en su declaración jurata de Renta correspondiente al 2016. Adjunto a este mensaje va su factura con la deferencia que debe abonar. En caso de no realizar el pago en fecha puede incurrir en cargos y multas extras.

Que tenga un buen día!

Agencia Tributarias

Av. De España, 8, 02002 Albacete. España.

Si un delincuente quiere estafar a cientos de miles de personas, es muy complicado saber el nombre de todas esas personas.

Por ello, utilizan fórmulas genéricas como “Estimado cliente”, “Hola”, “Hola amigo”, etc. para evitar decir un nombre.

PHISHING

De LaCaixaBank@admin.lacaixa.es

Asunto Información de seguridad LaCaixa

A

CaixaBank | Particulares, Empresas "la Caixa"

Aviso Urgente"la Caixa"

-Le notificamos que su cuenta y tarjeta esta bloqueada temporalmente debido a que su ultima consulta de cajero o banca en linea no finalizo de manera corecta

-Para poder desbloquear la tarjeta es necesario afiliar y hacer una pequena verificacion de identidad. Para verificar su identidad AQUI

-Su Tarjeta Visa/Master debe ser sincronizada y reactivada de acuerdo a su usuario de acceso.

-Una vez emitido este correo electronico tendra un plazo de 8 horas para llevar acabo dicha accion de lo contrario y por medidas de seguridad su tarjeta XXXX sera descontinuada.

-Luego terminando el proceso solicitado,presiona Continuar. A partir de aqui,podras seguir realizando sus tranzacciones de la manera acostumbrada

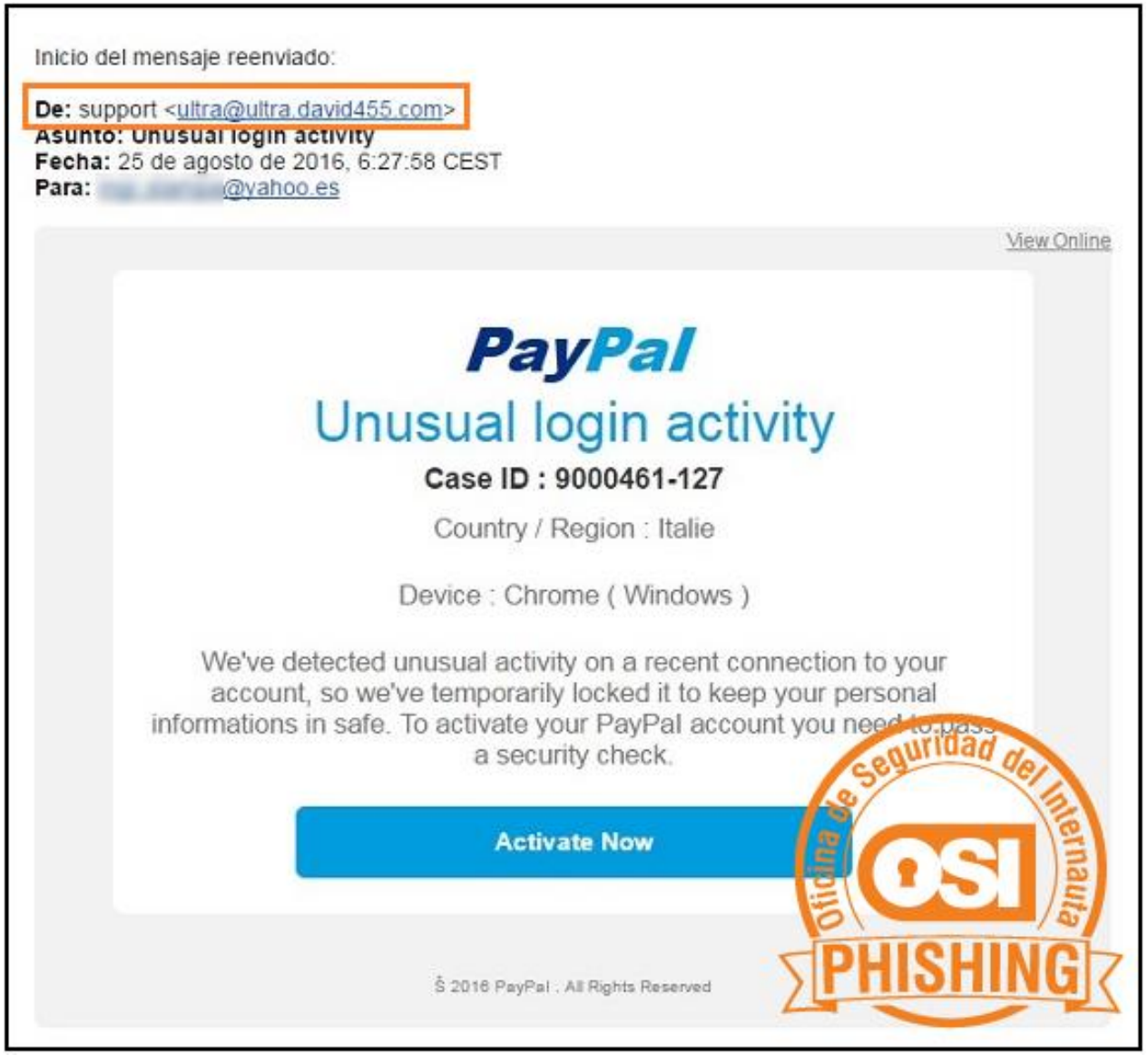
Entre aqui para realizar la sincronizacion :

CaixaBank | Particulares, Empresas "la Caixa"

Activar Tarjeta AQUI

Otra técnica utilizada por los delincuentes es la de pedir la realización de una acción en un período de tiempo muy corto.

PHISHING



Inicio del mensaje reenviado:

De: support <ultra@ultra.david455.com>
Asunto: Unusual login activity
Fecha: 25 de agosto de 2016, 6:27:58 CEST
Para: [redacted]@yahoo.es

View Online

PayPal

Unusual login activity

Case ID : 9000461-127

Country / Region : Italie

Device : Chrome (Windows)

We've detected unusual activity on a recent connection to your account, so we've temporarily locked it to keep your personal informations in safe. To activate your PayPal account you need to pass a security check.

Activate Now

Ŝ 2016 PayPal . All Rights Reserved

Oficina de Seguridad del Internauta OSI PHISHING

Debemos sospechar si el remitente es una dirección de correo que no pertenece a la entidad, como sucede en el siguiente ejemplo, que el mensaje hace referencia a **PayPal** y el email del remitente no hace ninguna alusión a dicho servicio.

PHISHING Frases comunes

Acceda al siguiente **enlace** para conocer sus adeudos.

Presione **clic aquí** para **descargar** su estado de cuenta.

Multa por incumplimiento de obligaciones fiscales.

Evite sanciones, revise por favor el **documento anexo**.

UNAM

PHISHING

- ✓ **Sé precavido** ante los correos que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- ✓ **Sospecha** si hay errores gramaticales en el texto, pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- ✓ Si recibes **comunicaciones anónimas** del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”, es un indicio que te debe poner en alerta.
- ✓ Si el mensaje te obliga a tomar una **decisión de manera inminente** o en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: **la OSI, Policía, Guardia Civil, etc**.
- ✓ Revisa si el texto del **enlace** que facilitan en el mensaje coincide con la dirección a la que apunta, y que ésta corresponda con la URL del servicio legítimo.
- ✓ Un servicio con cierto prestigio **utilizará sus propios dominios** para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.

FRAUDE COMPRA ONLINE

El **carding** es una actividad delictiva consistente en la utilización fraudulenta de numeraciones válidas de tarjetas de crédito/débito para efectuar compras por internet en comercios virtuales.

Consejos y recomendaciones

- Realizar una revisión periódica de los movimientos de nuestras cuentas a las que tengamos asociadas tarjetas por si vemos algún cargo sospechoso y, en su caso, poder reclamar.
- Es imprescindible anular las tarjetas en caso de pérdida o sustracción.

DETECCIÓN: CONSEJOS

- Realizar preferentemente las compras en **páginas oficiales** o con reputación y prestigio consolidado.
- No se recomienda comprar si no aparece en la web **información** sobre:
  - **Datos reales y físicos** de la empresa: titular, NIF/CIF, domicilio fiscal, etc.
  - **Condiciones de venta**, devoluciones o reclamaciones.
  - **Textos legales**: aviso legal, políticas de privacidad, etc.
- Sospechar de tiendas con **precios muy por debajo** del precio de mercado, o si todos los productos se venden al mismo precio, independientemente del modelo.
- En cuanto al **diseño** de la web, desconfiar:
  - Si no transmite homogeneidad (varios tipos de letra en la misma ventana)
  - La foto de portada puede encontrarse en otros lugares de internet.
  - La calidad de las imágenes no es buena: pixeladas, de baja calidad o incluyen marcas de agua.
  - La web aparenta ser la página legítima de una determinada marca.
  - Aparecen textos mal traducidos. Por ejemplo, aparece traducida la sección “Home” como “Casa”, en lugar de “Inicio”, que es lo comúnmente utilizado.
- Descartar la compra si la web anuncia varias **formas de pago**, pero finalmente sólo acepta tarjeta de crédito.


SALE

COMPRAS SEGURAS

Son muchos los que desconocen las distintas **alternativas** disponibles y qué ventajas o inconvenientes aporta cada una.

Por tanto, es importante conocer qué opciones hay disponibles para saber cuál es la que más interesa utilizar para cada tipo de compra y la que ofrece una mayor seguridad.

Plataformas de Pago

Servicios de **intermediarios entre nosotros y el vendedor** (PayPal, Apple Pay, Google Pay, etc.). Protegen nuestros datos y actúan de mediadores ante posibles fraudes.

Tarjetas Prepago/E-Wallet

Estas **tarjetas virtuales** permiten realizar pagos **sin que estos estén asociados a nuestra cuenta bancaria**.

Tarjetas de Crédito o Débito

La mayoría de las plataformas las aceptan, pero **corremos el riesgo de exponer nuestros datos**.

Transferencia Bancaria

En caso de **sufrir alguna incidencia con el envío** o el producto, podría ser **difícil de demostrar.** En especial, si se trata de una transferencia al extranjero.

ESTAFAS EN PISOS DE ALQUILER

- ✓ Sé precavido ante alquileres a **precios muy bajos**. Si te interesa una ubicación concreta, haz una comparativa con el resto de alquileres de la zona.
- ✓ Sospecha si detectas que las **fotos** de la vivienda son **copiadas** de otra web (contienen marcas de agua) o si son las mismas que las vistas en otros anuncios.
- ✓ No te fíes de propietarios que residen en el **extranjero** y por algún motivo no pueden enseñarte el piso en persona.
- ✓ Desconfía si te sugieren hacer uso de **intermediarios** para la entrega de las llaves o el contrato.
- ✓ Las **prisas** deben ponerte en alerta.
- ✓ Si te solicitan pagos a través de **servicios de envío de dinero** de forma anónima como MoneyGram o Western Union, no continúes con el proceso.

ESTAFAS EN BÚSQUEDA EMPLEO ONLINE

- Cuando encuentres una oferta de empleo por Internet, asegúrate que la información que contiene es coherente.
- Si la oferta de empleo la recibes por Internet sin haberla solicitado o haberte apuntado a ningún proceso de notificación de estas características, duda sobre su veracidad.
- Los anuncios de trabajo que están mal redactados o contienen faltas de ortografía hay que ponerlos en cuarentena.
- Si tras enviar una solicitud para optar a un puesto de trabajo te solicitan dinero o efectuar un pago bajo algún pretexto, no accedas a las peticiones sin más.
- Sospecha de anuncios que publiciten trabajos desde casa o en el extranjero, muy bien remunerados, en los que no se pide ningún tipo de experiencia previa.

Dédalo FUNDACIÓN

GRACIAS POR SU ASISTENCIA !!!

somos digital