HISTÓRICO DE ALERTAS DE SEGURIDAD

2026

--

Se están recibiendo en los buzones de la UBU correos fraudulentos intentado suplantar la identidad de Microsoft.

Cuando lo recibas, márcalo como SPAM o correo no deseado.

Más información en: https://www.ubu.es/servicio-de-informatica-y-comunicaciones/informacion-general/seguridad-de-la-informacion/como-distinguir-evitar-y-denunciar-correos-fraudulentos.

25/03/2026

--

Se ha detectado una campaña de phishing que suplanta a la Agencia Estatal de Administración Tributaria (AEAT), sobre la cual ha alertado el Instituto Nacional de Ciberseguridad (INCIBE).

La campaña se basa en el envío de correos electrónicos fraudulentos que informan falsamente de la existencia de una nueva notificación electrónica pendiente revisión. Dichos correos redirigen a las víctimas a páginas web falsas que imitan la Dirección Electrónica Habilitada Única (DEHú).

El objetivo principal del ataque es la sustracción de credenciales de acceso, solicitando a la víctima que introduzca sus datos personales y de autenticación en los formularios fraudulentos.

Los mensajes presentan una apariencia visual legítima, pero proceden de dominios no oficiales.

Para más información, consulte el comunicado oficial de INCIBE.

19 de marzo de 2025

--

2025

--

Durante el día de hoy, 19 de marzo de 2025, se están recibiendo correos intentando suplantar la identidad de personal de la UBU con el asunto "**Informe financiero importante y los estados financieros correspondientes a marzo de 2025 están disponibles para su revisión**". En caso de haber facilitado tus datos, cambia tu contraseña inmediatamente en UBUNet y abre una incidencia en https://cau.ubu.es para que podamos valorar el alcance de los daños.

19 de marzo de 2025

--

Los días 5 y 12 de febrero de 2025 se recibieron varios correos maliciosos en algunos buzones de la UBU con el asunto "**Adjunto el recibo 202502xxxxxx**". Solo existió riesgo si abriste el PDF adjunto y pinchaste en el enlace incluido en el fichero. En tal caso, abre una incidencia en https://cau.ubu.es para que podamos valorar el alcance de los daños.

--

2024

--

Están llegando a la UBU correos con información falsa intentando suplantar de identidad del Vicerrectorado de Estudiantes. En dichos correos se indica de forma incorrecta que se cancelan las clases de hoy martes.

29 de octubre de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notificación de caducidad de contraseña**" o similar, de suplantación de identidad. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

17 de julio de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**UBU**", de suplantación de identidad. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

24 de junio de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**JEFE DE DEPARTAMENTO**", de suplantación de identidad. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

12 de junio de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Administrador de sistema**" e "**información urgente**", intentando suplantar la identidad soporte del correo de la UBU. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

6 de mayo de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Convocatoria: Responder a la recepción ●**", con un PDF adjunto sospechoso intentando suplantar la identidad de la Guardia Civil. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

4 de marzo de 2024

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Convocatoria: Respuesta inmediata**", con un PDF adjunto sospechoso intentando suplantar la identidad de la Guardia Civil. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

30 de enero de 2024

--

El CCN-CERT, del Centro Criptológico Nacional, informa que Apple, empresa estadounidense de equipos electrónicos, software y servicios en línea, ha publicado **cinco avisos de seguridad** relacionados con **seis vulnerabilidades** de severidad **alta y crítica**, y que afectan a sus productos con sistemas operativos macOS Sonoma, macOS Monterey, watchOS, iOS, iPadOS y tvOS

25 de enero de 2024

--

Programada para el martes 23 de enero una actualización de los servidores cloudpaging de UBULabs, entre las 14:00h y las 15:00h, que implicará que durante ese periodo no funcionen las aplicaciones de UBULabs.

Actualización: tendrás que acceder de nuevo a UBULabs (ubulabs.ubu.es) para ejecutar las aplicaciones a las que accedías previamente a la actualización.

23 de enero de 2024

2023

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Coordinador de Decisiones Estrategicas Informa - 54904645**" y "**Cumplimiento de Normas Tributarias – 974452**", con un intento de suplantación de identidad. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

18 de diciembre de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Tu Informe Médico está listo !!**", con un intento de suplantación de identidad. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

12 de diciembre de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: " **New Document** ", intentando suplantar la identidad de la Univerisidad de Burgos. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

15 de noviembre de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Your Universidad de Burgos Mailbox Notice**", intentando suplantar la identidad de la

Univerisidad de Burgos. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

15 de septiembre de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**REMITTANCE Ubu -July 01, 2023**", con un adjunto malicioso. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

04 de julio de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: PAGO**", intentando suplantar la identidad de una persona de una universidad de México. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

26 de junio de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**FW: HOLA**", con un PDF adjunto. Si has abierto el PDF o pinchado en algún enlace, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

22 de junio de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Tu cuenta de Amazon.es**", intentando suplantar la identidad de Amazon. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

12 de abril de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: PAG0**", intentando suplantar la identidad de una persona de la UCV. Si has

facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

20 de marzo de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**FACTURAS PENDIENTES DE PAGO**", intentando suplantar la identidad de una empresa privada de construcción. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

02 de marzo de 2023

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notificación de sanción por infracción del reglamento general de circulación**", intentando suplantar la identidad de la Dirección General de Tráfico. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

08 de febrero de 2023

2022

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notification: RE: factura**", intentando suplantar la identidad de Microsoft. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

16 de noviembre de 2022

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**REQUEST: Password Update (Tuesday, September 27, 2022)**", intentando suplantar la identidad de Microsoft. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

28 de septiembre de 2022

--

Actualización de seguridad en Apple.

Desde el CCN-CERT nos informan de una vulnerabilidad en productos Apple y recomiendan aplicar las actualizaciones correspondientes en los dispositivos afectados.

Tienes más información en: **https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12036-actualizacion-de-seguridad-en-apple.html**.

20 de septiembre de 2022

--

Llamadas fraudulentas

13 de septiembre de 2022

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Confirm Request Access**", intentando suplantar la identidad de Microsoft. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (**https://cau.ubu.es**).

27 de julio de 2022

--

Detectada otra campaña de correos fraudulentos de phishing usando la técnica de ingeniería social conocida como "sextorsión".

Estas campañas buscan extorsionar a las víctimas para que paguen una determinada cantidad en bitcoins o por el contrario se hará público un supuesto vídeo íntimo. Es un engaño: **nadie ha tenido acceso a tus dispositivos ni ha grabado un vídeo íntimo**.

Mas información sobre este tipo de correos en: **https://www.osi.es/es/actualidad/avisos/2021/04/nadie-ha-copiado-los-datos-de-tu-dispositivo**

Instrucciones de cómo proceder en: **https://www.ubu.es/servicio-de-informatica-y-comunicaciones/informacion-general/seguridad-de-la-informacion/instrucciones-para-informar-sobre-correos-fraudulentos-phishing-o-correo-no-deseado-spam-en**

Información relevante sobre seguridad en **https://www.ubu.es/servicio-de-informatica-y-comunicaciones/informacion-general/seguridad-de-la-informacion**

30 de junio de 2022

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: **Comprobante fiscal digital - MINISTERIO DE HACIENDA Y FUCION PUBLICA**", intentando suplantar la identidad de la UBU. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

23 de marzo de 2022

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**[Scanned document:##362073#Ubu#]**", intentando suplantar la identidad de la UBU. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

23 de marzo de 2022

2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**File: (2) Documents**", intentando obtener datos de los usuarios. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

12 de noviembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Dating and Friend Zone**", intentando obtener datos de los usuarios. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

8 de noviembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: ubu**", intentando suplantar la identidad de estudianttes de la UBU. Si has facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

26 de octubre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Buen días**", intentando suplantar la identidad de Office 365. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

29 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Pago realizado con éxito.**", con un fichero ".zip" malicioso como adjunto. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

22 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**RE: Buen día**" y "**RE: Tema del TFG**", intentando suplantar la identidad de personas de la Universidad. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

13 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**RE: Buen día**" y "**RE: Nota**", intentando suplantar la identidad de personas de la Universidad. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

9 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**RE: Buenos días**", intentando suplantar la identidad de personas de la Universidad y con el asunto: "**Validación**", intentando suplantar la identidad de Office 365. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

8 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: UBU..**", intentando suplantar la identidad integrantes de la Comunidad Universitaria y otro con el asunto: "**Carta postal - Citación I64059**" intentando suplantar la identidad de la Administración de Justicia. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

7 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**ubu.es Expiration/Request=49**", intentando suplantar la identidad de Office 365. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet y ponte en contacto con el Centro de Atención a Usuarios (https://cau.ubu.es).

6 de septiembre de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Después del último cálculo sobre las actividades fiscales**", intentando suplantar la identidad de la Agencia Tributaria. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet, y si has facilitado algún dato bancario, ponte inmediatamente en contacto con tu entidad bancaria.

También están llegando correos solicitando un pago Bitcoins a cambio de no revelar información comprometida. Este tipo de correos no es ninguna amenaza, simplemente hay que marcarlo como "Correo no deseado".

1 de julio de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: UBU**" y "**Re: Correo**", intentando suplantar la identidad de estudiantes de la Universidad de Burgos. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

21 de junio de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**ADMINISTRADOR: Información**", intentando suplantar la identidad de la Universidad de Burgos. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

10 de junio de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**IMPORTANTE: Servicio de Internet.**", intentando suplantar la identidad de la Universidad de Burgos. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

9 de junio de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notification: Password Update 5/26/2021**", intentando suplantar la identidad de Office 365. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

26 de mayo de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Última advertencia - Envio de Burofax Online**". Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

25 de mayo de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**MANDATE PASSWORD: Wednesday, April 28, 2021**", intentando suplantar la identidad de Office 365. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

28 de abril de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Re: UBU**", intentando suplantar la identidad de estudiantes de la UBU. Si has facilitado tus credenciales, cambia tu contraseña inmediatamente en UBUNet.

21 de abril de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Agarre seguro para [usuario] en 16, Apr 2021**", intentando suplantar la identidad de Office365.

16 de abril de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con los asuntos: "**Pago desde su cuenta**" e "**Inicio de sesión completado con éxito, todos los datos de su dispositivo fueron**

copiados. Lea las instrucciones en el interior.", amenazando con la publicación de información personal a cambio de un pago con bitcoins.

12 de abril de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Sede Electónica - acción fiscal**", intentando suplantar la identidad de la Agencia Tributaria.

7 de abril de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notificación.**" intentando suplantar la identidad de estudiantes de la UBU. Si has pinchado en el enlace y has facilitado tus datos, cambia inmediatamente tu contraseña en UBUNet.

12 de marzo de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**CONFIRMA TU CÓDIGO PROMOCIONAL AHORA [1H11S...] ..**" intentando suplantar la identidad de **AMAZON**. Si has facilitado tus datos, cambia inmediatamente tu contraseña en UBUNet.

25 de febrero de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Coresponde un reembolso del impuesto en valor de 469,00 euro**" intentando suplantar la identidad de la Agencia Tributaria.

29 de enero de 2021

--

Están llegando a la UBU correos fraudulentos "phishing" que distribuyen el **malware Emotet.** Dichos correos hacen referencia a conversaciones con usuarios habituales y adjuntan un fichero con contraseña.

A continuación, le mostramos un ejemplo de los correos relacionados con esta campaña:

13 de enero de 2021

2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Reembolso del impuesto en valor de 469,00 euro"** intentando suplantar la identidad de la Agencia Tributaria**.**

17 de diciembre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Notification**" intentando suplantar la identidad de estudiantes de la UBU.

16 de noviembre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Confirmation Request**" intentando suplantar la identidad de Office 365.

30 de octubre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Direccion General de Trafico España (sede.dgt.gob.es) - Registro de multa 13239.**" intentando suplantar la identidad de la Dirección General de Tráfico.

8 de octubre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Orden Devuelta - [id 761259099]**" intentando suplantar la identidad de Correos.

5 de octubre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Devolucion De Impuestos**" intentando suplantar la identidad de la Agencia Tributaria.

24 de septiembre de 2020

--

Están llegando a la UBU correos fraudulentos "phishing" con el asunto: "**Los hackers piratearon tu cuenta. Cambie los datos de acceso inmediatamente.**"

20 de junio de 2020

--

Estamos observando un considerable incremento de cuentas de estudiantes que están enviando SPAM. Esto significa que alguien ha conseguido la contraseña de estas cuentas y ha podido acceder a ellas, enviando correos de phishing a la libreta de direcciones de la universidad, que pretenden conseguir otras credenciales de acceso. Estos correos tienen como asunto: **Anuncio y Notificación**.

A aquellos que tengan sus cuentas comprometidas, se les están bloqueando, de forma que no podrán acceder al correo ni a las aplicaciones corporativas hasta que se sigan las instrucciones enviadas por el Centro de Atención a Usuarios del Servicio de Informática y Comunicaciones (CAU).

Las causas más probables del robo de contraseñas son:

-Haber caído en alguna campaña de phishing

-Usar la misma contraseña para el acceso a la UBU y a otras páginas externas.

-Tener malware instalado en el equipo.

Como medida preventiva recomendamos a todos los miembros de la comunidad universitaria que cambien la contraseña utilizando la aplicación de UBUNet.

¿Sabes lo que es el phishing? Es una técnica de suplantación de identidad. Alguien se hace pasar por quien no es, ya sea una empresa o una persona de confianza, para conseguir datos como tus claves de acceso.

¿Cómo puedes protegerte del phishing?

-Presta atención a la dirección de email del remitente.

-Presta especial atención al dominio (lo que viene después de la @, como por ejemplo, @ubu.es).

-Fíjate en el destino de los enlaces. Presta especial atención a la barra de direcciones y asegúrate de que es la correcta (por ejemplo: *.ubu.es).

-Presta atención a la redacción del email o de la página web. Muchas veces tienen faltas graves o redacciones confusas.

-Esta clase de correos habitualmente te piden que entres en tu cuenta de forma urgente.

-Navega a través de conexiones cifradas (utilizando https en lugar de http).

-Asegúrate de que tienes instalado en tu equipo un antivirus actualizado.

-Si tienes dudas de lo que estás haciendo o de la identidad de la persona que te envía el email, no hagas clic.

-Recuerda no utilizar la misma contraseña de la UBU en otras páginas web externas.

Recomendamos realizar este test, para ver si eres capaz de detectar el phishing: **https://phishingquiz.withgoogle.com/?hl=es**

2 de junio de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento intentando suplantar la identidad de Office 365 con el "Asunto": "**Notification Thursday 17, 2020**". Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber descargado un fichero o haber facilitado tus datos, ponte en contacto de inmediato con el C.A.U.

18 de junio de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**11 June, 2020**". Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber descargado un fichero o haber facilitado tus datos, ponte en contacto de inmediato con el C.A.U.

12 de junio de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento intentando suplantar la identidad de Office 365. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber descargado un fichero o haber facilitado tus datos, ponte en contacto de inmediato con el C.A.U.

4 de junio de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Su factura 30928.0092 para pagar hoy. SNN03029898318:10**". Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber descargado un fichero o haber facilitado tus datos, ponte en contacto de inmediato con el C.A.U.

22 de mayo de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Action Required- B1955B490**", intentando suplantar la identidad de Office 365. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber descargado un fichero o haber facilitado tus datos, ponte en contacto de inmediato con el C.A.U.

20 de mayo de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Factura ay disponible - 54VIK**". Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

14 de abril de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Facturación – D0JFD**". Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

1 de abril de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Informe de resultados - 37C7763B**", suplantando la identidad de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

17 de marzo de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Re: Notificación**", suplantando la identidad de estudiantes de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus

credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

5 de marzo de 2020

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**E-Fact ay disponible - I87UR**", para obtener datos de forma ilícita. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

3 de marzo de 2020

--

La Universidad de Burgos ha sido víctima de un ataque perpetrado por hackers a la seguridad de la información.

Más información: https://www.ubu.es/noticias/hackers-en-la-ubu

17 de enero de 2020

2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Acción requerida**", suplantando la identidad de Office 365. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

17 de diciembre de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Re: notificación**", suplantando la identidad personal de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

8 de noviembre de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Re: notificación**", suplantando la identidad de estudiantes de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

17 de septiembre de 2019

--

Se están enviando desde cuentas de la UBU correos fraudulentos. Comprueba en tu carpeta de "enviados" que no tienes correos sospechosos. En el caso de que detectes alguna anomalía, ponte en contacto con el Centro de Atención a Usuarios en el 947259505 o abre una incidencia en https://cau.ubu.es.

12 de septiembre de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Important Software Maintenance for Student/Staff**", suplantando la identidad de estudiantes de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

16 de julio de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Suspension Alert for Office Account**", suplantando la identidad del administrador del correo. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

19 de junio de 2019

--

Se han detectado llamadas de teléfono donde el interlocutor se hace pasar por un técnico de Microsoft que informa de la detección de un virus informático en vuestro ordenador. Se ofrecen a solucionar el problema indicando que, de no hacerlo, está en riesgo la integridad de tu sistema operativo y tu información personal.

Se trata de un ataque de tipo "Ingeniería Social", intentan que les deis acceso a vuestro ordenador para controlarlo, sustraer información sensible o insertar código dañino.

30 de mayo de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "Undeliverable Email:.", suplantando la identidad del administrador del correo. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

28 de mayo de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Verifique su correo electrónico**", suplantando la identidad del administrador del correo. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber

facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

7 de mayo de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Notificación por correo electrónico (Tratar urgente)**", suplantando la identidad de una administración. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

7 de marzo de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Ubu.es**", suplantando la identidad de la Universidad de Burgos. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

6 de febrero de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Actualización de la cuenta de correo electrónico (tratar urgente**", "**Su buzón está lleno**", o "**Subscription confirmation**", suplantando diferentes identidades. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

24 de enero de 2019

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Acceso a cuenta de correo**", suplantando la identidad de personal de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el

caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

14 de enero de 2018

2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**[Account-Deactivation]**", suplantando la identidad del administrador del correo de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

23 de octubre de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Reconfirm your Ubu Password**", suplantando la identidad del administrador del correo de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

4 de octubre de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con tu usuario y tu contraseña en el "asunto". Ante este tipo de correos, en primer lugar, cambia tu contraseña en UBUNet y en segundo lugar, marca el correo como "no deseado". Más información sobre este tipo de ataques en: https://www.genbeta.com/seguridad/no-black-mirror-nueva-estafa-que-amenaza-filtrar-tus-videos-masturbandote-no-pagas-bitcoin

3 de octubre de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Account Verification**", suplantando la identidad del administrador del correo de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de

identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

25 de septiembre de 2018

--

Se ha detectado una campaña de phishing a nivel global de phishing contra universidades y centros de investigación. Esta campaña tiene como particularidad que tiene capacidades de autopropagación, por lo que el impacto potencial puede ser muy alto.

Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

13 de septiembre de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **“informe evaluación doctorando (nombre y apellidos)”**, suplantando la identidad del administrador del correo de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

11 de septiembre de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Action Required: Mail Box Failed - ***@ubu.es**", suplantando la identidad del administrador del correo de la Universidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

29 de agosto de 2018

--

Están llegando a las cuentas de la UBU correos fraudulentos con los asuntos: "**Finalmente está AQUÍ**" y "**Anuncio Del Administrador De La Escuela**", el primero es un phishing y el segundo intenta suplantar la identidad del administrador del correo de la Universidad. Ante este tipo de

correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

20 de agosto de 2018

--

Están llegando a las cuentas de la UBU correos fraudulentos con el asunto: **" Habilite Su Archivo (ID: usuario@ubu.es-23/7/2018)"** suplantando la identidad de Microsoft Office 365. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

23 de julio de 2018

--

Parada programada en el **Servidor de Incidencias** prevista para el próximo **miércoles 27 de junio de 8:30 a 9:00.**

Disculpad las molestias.

23 de mayo de 2018

--

Están llegando a las cuentas de la UBU correos fraudulentos con el asunto: **"Account Confirmation"** suplantando la identidad de Office 365. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

23 de mayo de 2018

--

Están llegando a las cuentas de la UBU correos fraudulentos con los asuntos: "**Actualizar**" y **“Tiene dos (2) mensajes”** suplantando la identidad de la gestión del correo de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación

de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

12 de abril de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: "**Actualizar**" suplantando la identidad de la gestión del correo de la UBU. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

11 de abril de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **"Suspensión : Errσr de sesiσn"** suplantando la identidad del Banco Santander. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

5 de abril de 2018

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **"Aviso : Nueva actualización !"**. suplantando la identidad del Banco Santander y otro con un texto obsceno suplantando la propia identidad. Ante este tipo de correos, accede al portal de Office 365 (portal.office.com), selecciona la aplicación de correo y marca el mensaje. Una vez marcado desde el menú de la parte superior hay que seleccionar el desplegable que hay en correo no deseado y elegir la opción "Suplantación de identidad". En el caso de haber facilitado tus credenciales, cambia tu contraseña en UBUNet y ponte en contacto de inmediato con el C.A.U.

19 de marzo de 2018

2017

--

De: Macdonald, Rachael M <rmm7@hw.ac.uk>
Enviado: viernes, 24 de noviembre de 2017 11:23
Asunto: Status code: 550 5.0.350

Inactivity response is due to bunch of unresponded and unread mails, you need to resolve in attachment.

24 de noviembre de 2017

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **Vuelva a validar su cuenta ahora!**. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

20 de noviembre de 2017

--

De: Shihui YAO [mailto:syaoab@connect.ust.hk]
Enviado el: sábado, 16 de septiembre de 2017 16:00
Asunto: Administrateur de courriel scolaire

Nous avons remarqué certaines activités inhabituelles sur votre compte de messagerie ces derniers jours pour empêcher votre compte de messagerie contre le vol, nous avons temporairement suspendu votre compte pour prouver qu'il s'agit de votre compte, veuillez cliquer sur le lien **http://administradorweb.weebly.com** pour vérifier vos informations et débloquer Ton compte

Notez que vous avez moins de 24 heures pour vérifier vos informations et débloquer votre compte ou qu'il soit suspendu en permanence

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **Banco Sabadell. (27722)**. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

7 de septiembre de 2017

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **Seguridad Banco Santander. (17627)**. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

4 de septiembre de 2017

--

Asunto: rdpino will shut down soon!

30 de junio de 2017

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: **Final Warning: Microsoft Office 365 security alert**. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

19 de junio de 2017

--

16 de mayo de 2017

Aviso importante sobre "ciberataque" de ramsonware

Configurar

Cómo sabrás por los medios de comunicación, este fin de semana se ha producido un ataque masivo por medio de un virus tipo ransomware.

¿De qué se trata?

Desde el pasado viernes 12 de mayo un malware (virus) se está difundiendo a nivel mundial. Esto es algo que, por desgracia, ocurre a diario, pero en esta ocasión, por diferentes motivos, ha tenido mayor repercusión de la habitual.

Una vez que este malware entra en la red de una organización, se puede transmitir entre sus ordenadores con sistema Windows a través de una vulnerabilidad para la que existe una solución (una actualización del sistema).

Si un equipo se infecta, se cifrarán y quedarán inutilizables tanto sus ficheros como los de los dispositivos (pendrives, disco duros externos, carpetas de red compartidas, …) a

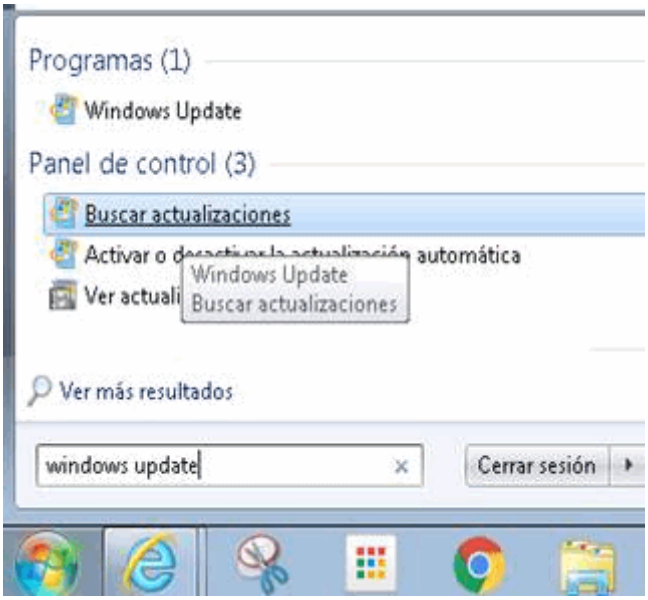
los que tengas acceso. Actualmente no se conoce una forma de recuperar esta información salvo a partir de una copia de seguridad.

¿Qué debo hacer para prevenir?

Este problema sólo afecta a equipos con sistema operativo Windows. Si es tu caso, sigue estas indicaciones:

1. No abras ningún correo de remitentes desconocidos con ficheros adjuntos sospechosos.
2. Se especialmente cuidadoso con la navegación web. Navega solo por sitios web fiables y necesarios para el desempeño de tu trabajo.
3. Comprueba que tu sistema está actualizado, especialmente si eres administrador del sistema.
4. Si tu equipo se lo ha entregado e instalado el Servicio de Informática, ya estará configurado de forma que las actualizaciones importantes del sistema se descargan de forma automática cuando Microsoft las publica y, por tanto, no estaría en riesgo. No obstante, realice esta comprobación, ya que, es posible que dado que Vd. es administrador de su sistema, en algún momento haya modificado esta configuración o bien, no haya querido o podido instalar estas actualizaciones.

En Windows: Teclee “Windows Update” en el control de búsqueda y, después, pulse sobre “Buscar actualizaciones”



Si tiene todas las actualizaciones importantes instaladas verá lo siguiente:

Si no fuera así, pulsa sobre “buscar las actualizaciones” importantes disponibles e instálalas.

5. Comprueba que tienes el antivirus actualizado.
6. Recuerda que si tu equipo se infecta y los ficheros son cifrados, la única solución posible actualmente de recuperar la información es a partir de una copia de seguridad. En cuanto puedas, realiza una copia de seguridad de tu información en un dispositivo externo y desconéctalo del equipo una vez realizada la copia.

Más información

- CCN-CERT: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- Microsoft: https://blogs.technet.microsoft.com/microsoftlatam/2017/05/13/orientacion-al-cliente-para-ataques-wannacrypt/

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: seguridad banco santander. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

7 de abril de 2017

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: administrador de sistema. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

27 de febrero de 2017

2016

--

Está llegando a las cuentas de la UBU un correo fraudulento con el asunto: UBUNet. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta

"Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

16 de noviembre de 2016

--

Está llegando a las cuentas de la UBU un intento de phishing con el asunto: Alerta en linea BancoSantander. (73291). No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

24 de octubre de 2016

--

Está llegando a las cuentas de la UBU un correo fraudulento (sin asunto) que avisa de que se ha superado el tamaño del buzón de correo. No contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

21 de octubre de 2016

--

Están llegando correos fraudulentos con el asunto "Le adjunto también, para su información, las instrucciones aclarativas" Recuerda, no contestes ni pinches en los enlaces de este tipo de correos. Muévelo a la carpeta "Correo no deseado" y, en el caso de haber facilitado tus credenciales, ponte en contacto de inmediato con el C.A.U.

8 de septiembre de 2016

--

En las últimas semanas están llegando una serie de correos en los que aparece como remitente ENDESA y se trata de un virus muy peligroso que causa importantes daños en los sistemas informáticos. El virus engaña al usuario aparentando ser una factura de Endesa, haciendo que la descargue y haciéndose con todos los datos del ordenador del usuario.

Se recibe un mail desde la dirección “endesa-clientes.com” con un enlace para consultar una factura es un enlace falso para tomar el control de su ordenador, hacerse con sus

datos y pedir un dinero a cambio devolverle los datos del su ordenador. Por favor, no abras ningún correo de Endesa sin estar completamente seguro de su autenticidad.

En este caso la campaña de los “piratas informáticos” es utilizando el nombre de Endesa, pero existen muchas otras campañas parecidas utilizando Correos, Agencia Tributaria, incluso Policía…, etc. Antes de acceder a ningún enlace debes comprobar la dirección del remitente, la forma de escribir el correo y su estructura, el asunto, y pensar si ese tipo empresas tiene acceso a su correo (personal y de empresa) para ese tipo de comunicaciones. Ante cualquier duda es mejor no pinchar ningún enlace.

9 de junio de 2016

--

Os informamos de un nuevo intento de correo fraudulento que ha estado llegando a cuentas de la UBU con el asunto "Ocupacion parcial"

13 de mayo de 2016

--

Os informamos de un nuevo intento de correo fraudulento que ha estado llegando a cuentas de la UBU suplantando la identidad de Eurocopia con el asunto [SPAM] Documento

27 de abril de 2016

--

Os informamos de un nuevo intento de phising/cryptolocker que ha estado llegando a cuentas de la UBU suplantando la identidad de Correos

25 de abril de 2016

--

Os informamos de un nuevo intento de phising/cryptolocker que ha estado llegando a cuentas de la UBU suplantando la identidad de Correos

13 de abril de 2016

--

Con fecha 20 de agosto de 2015 Microsoft envió un correo informando sobre la carpeta "Otros correos". Este era el texto:

Manténgase al día de su correo electrónico

Hemos agregado una nueva e increíble característica que ayuda a filtrar el correo electrónico de baja prioridad, lo que le ahorra tiempo para los mensajes más importantes. Se llama Otros correos.

Otros correos examina su comportamiento pasado para determinar los mensajes que es más probable que vaya a ignorar y los mueve a una carpeta denominada Otros correos. Siga usando el correo electrónico como de costumbre y la función Otros correos aprenderá cuáles son los mensajes que no son importantes para usted. De vez en cuando, esta función puede equivocarse. Mueva a la bandeja de entrada los mensajes incorrectamente identificados como Otros correos y la función lo tendrá en cuenta en el futuro.

Su privacidad es muy importante para nosotros. Quitamos cualquier información de identificación personal de los datos que usamos para mejorar las funciones.

Y si encuentra que Otros correos no es para usted, puede desactivarlo en cualquier momento.

Si desea que Otros correos deje de sacar mensajes de la bandeja de entrada, puede ir a Opciones y desactivarlo.

Esta notificación del sistema no es un mensaje de correo electrónico y no se puede responder a ella.

*No es alerta de seguridad pero se publicó en la web del SIC en el apartado “Alertas”.

--

*Según nos informa Microsoft, la configuración de Thunderbird con IMAP está dando problemas. Hasta que el problema esté solucionado, os recomendamos que accedáis a vuestro correo a través de la web: https://portal.office.com

21 de enero de 2016

*No es alerta de seguridad pero se publicó en la web del SIC en el apartado “Alertas”.

2015

--

Con fecha 18 de septiembre de 2015 se ha detectado el envío de correos fraudulentos a cuentas de la UBU. El asunto del mensaje es "ACTUALIZACIÓN!".

--

Con fecha 2 de septiembre de 2015 se ha detectado el envío de correos fraudulentos a cuentas de la UBU. El asunto del mensaje es "correoweb".

--

Con fecha 19 de agosto de 2015 se ha detectado el envío de correos fraudulentos a cuentas de la UBU. El asunto del mensaje es "Correo informacion".

--

Con fecha 21 de julio de 2015 se ha detectado el envío de correos fraudulentos a cuentas de la UBU. El asunto del mensaje es "última advertencia".

--

Os informamos de que el próximo miércoles día 8 de julio vamos a proceder a instalar el equipamiento de red averiado el pasado día 4 de junio.

Hemos intentado buscar una fecha adecuada que permita estabilizar las infraestructuras de red, una vez finalizada la selectividad y antes del comienzo del proceso de matrícula.

Las actuaciones previstas, suponen cortes intermitentes de los servicios de red entre las 9 y las 15h, lo se que comunica previamente a efectos de que impacten lo menos posible en vuestro trabajo.

Disculpad las molestias que os pueda ocasionar, pero se trata de tareas importantes que no conviene demorar más.

--

15/06/15

Te informamos de una nueva campaña del virus CryptoLoker que ha afectado a algunos equipos de la Universidad.

Este peligroso virus de tipo ransomware puede atacar, bien por correos que simulan ser un envío de paquete a través de la Sociedad Estatal de Correos y Telégrafos (Correos), o bien por acceder a ciertas páginas comprometidas.

Un ransomware es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Para prevenir infecciones desde páginas dañinas así como ficheros ofimáticos dañinos que puedan llegar al equipo por medio de correo electrónico, redes sociales, etc., se recomienda mantener el software correctamente actualizado. El navegador, versiones antiguas de Java, Flash o Adobe Acrobat suelen ser algunas de las principales vías de infección en ataques de este tipo.

--

Con fecha 6 de junio de 2015 se detectó el envío, a cuentas de correo de la UBU, de correos fraudulentos que intentaban obtener datos personales de forma ilícita. El "Asunto" del correo fue "ADVERTENCIA !!!".

--

Con fecha 9 de marzo de 2015 se detectó el envío, a cuentas de correo de la UBU, de correos fraudulentos que intentaban obtener datos personales de forma ilícita. El "Asunto" del correo fue "Nota: Universidad de Burgos usuario webmail".

--

Con fecha 16 de febrero de 2015 se ha detectado el envío, a cuentas de correo de la UBU, de correos fraudulentos que intentan obtener datos personales de forma ilícita. El "Asunto" del correo es "Estimado titular de la cuenta" o "Revalidar su buzón de correo".

--

Con fecha 29 de enero de 2015 el Centro Criptológico Nacional (CCN) nos ha informado de la existencia de una nueva campaña masiva de ransomware.

El ransomware es un software dañino que, tras haber cifrado los documentos del usuario, muestra un mensaje solicitando el pago de una cantidad específica para, supuestamente, recuperar el acceso a todos los ficheros cifrados.

Los asuntos que se han estado utilizando hasta ahora en estos correos electrónicos son:

Fax from RAMP Industries Ltd

[Fax server]= +07955-168045

[Fax server] : LPY.5705BBC7.1118

New incoming fax, NB-112420319-8448

[Operational Support Ltd] Fax transmission=U2W9MABD921532EC5

2014 y anteriores

Con fecha 9 de diciembre de 2014 se ha detectado un nuevo envío de correos electrónicos fraudulentos solicitando información personal. El asunto del correo es "actualización".

Anteriores correos fraudulentos llevaban este tipo de "Asunto": "actualización" [04/12/14], "Límite de Cuota" [17/11/14], "Advertencia re-validar su buzón" [15/09/14], "re" [06/07/14], "Estimado usuario de correo electrónico," [08/04/14], "gracias" [07/04/14], "::Estimado usuario Webmail Mail::" [29/03/14], "Su buzón está casi lleno" [26/03/14], "Advertencia: Actualice su buzón Ahora" [11/03/14], "notificación" [10/02/14]…

Recordamos a todos los usuarios que este tipo de correos es fraudulento y solo busca recoger datos de cuentas de correo para realizar actividades ilícitas con ellas.

Si ha recibido este correo, no lo responda y muévalo a la bandeja de SPAM. Si ha respondido accidentalmente, cambie su contraseña de inmediato.

Si responde a este tipo de mensajes podrá ser víctima de fraudes realizados con su cuenta de correo, y personas ajenas a usted podrán acceder a sus mensajes y enviar mensajes en su nombre.

Le recordamos una vez más que el Servicio de Informática y Comunicaciones NUNCA solicitará sus datos personales, ni por correo ni por teléfono.

Si detecta algún correo más de este tipo no dude en ponerse en contacto con el SIC mediante la dirección de correo serv.informatica@ubu.es.

Si cree que alguien puede estar accediendo a su correo sin su consentimiento háganoslo saber.

Para más información sobre Phishing:

http://es.wikipedia.org/wiki/Phishing

http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx

http://windows.microsoft.com/es-ES/windows-vista/smartscreen-filter-frequently-asked-questions