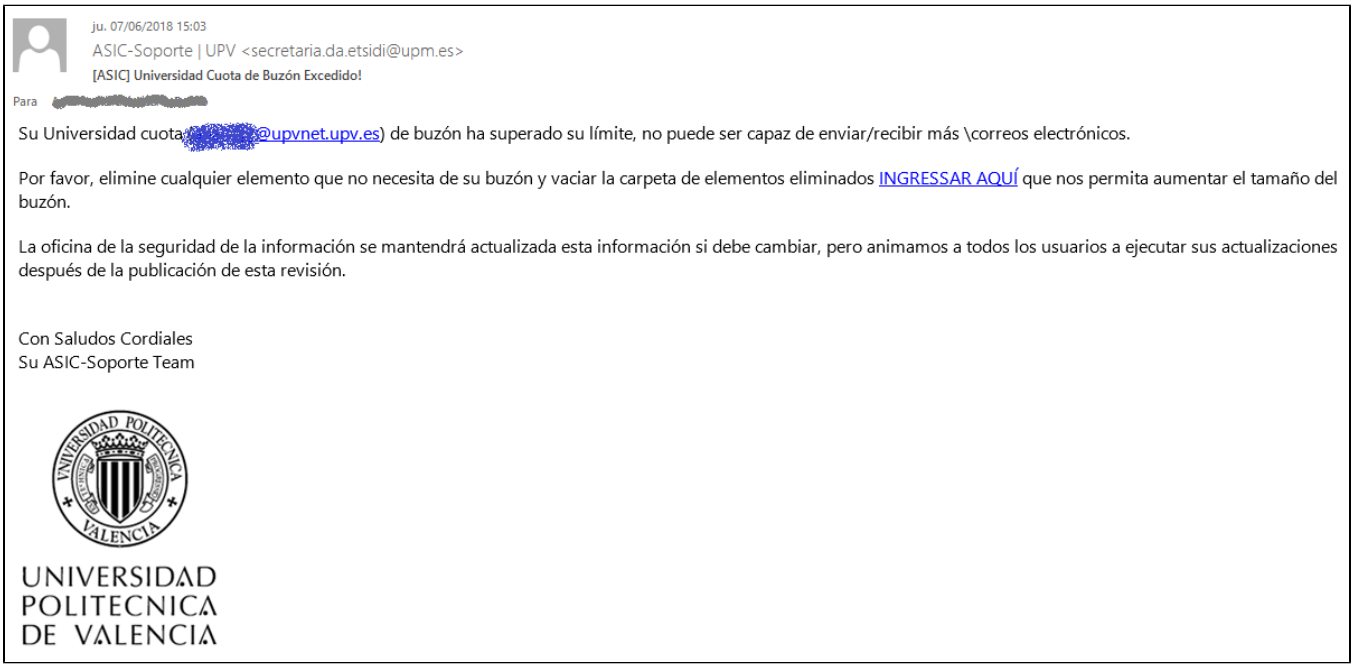
Phishing a la UPV

¿Qué es el phishing?

En la UPV, como en otras instituciones, se reciben ataques de **phishing** con cierta frecuencia.

El phishing es una técnica que persigue robar nuestras credenciales de acceso a los servicios de la UPV.

Suele empezar con un correo fraudulento, que nos informa de un problema (inexistente) y nos urge a realizar una acción. Por ejemplo:



ju. 07/06/2018 15:03

ASIC-Soporte | UPV <secretaria.da.etsidi@upm.es>

[ASIC] Universidad Cuota de Buzón Excedido!

Para [redacted]

Su Universidad cuota([redacted]@upvnet.upv.es) de buzón ha superado su límite, no puede ser capaz de enviar/recibir más \correos electrónicos.

Por favor, elimine cualquier elemento que no necesita de su buzón y vaciar la carpeta de elementos eliminados INGRESSAR AQUÍ que nos permita aumentar el tamaño del buzón.

La oficina de la seguridad de la información se mantendrá actualizada esta información si debe cambiar, pero animamos a todos los usuarios a ejecutar sus actualizaciones después de la publicación de esta revisión.

Con Saludos Cordiales
Su ASIC-Soporte Team

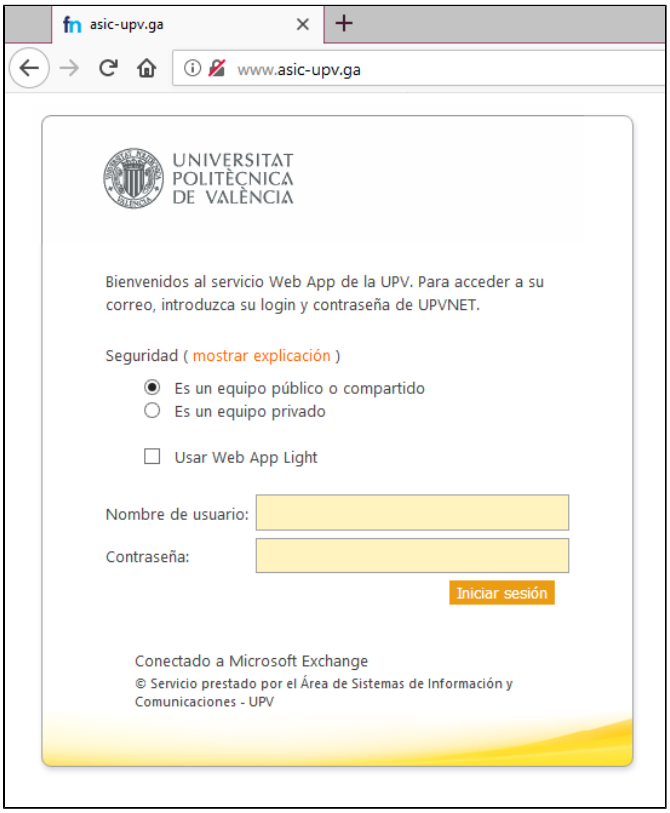
UNIVERSIDAD POLITECNICA DE VALENCIA

En el correo fraudulento anterior intentan suplantar al ASIC (aunque se puede ver que la dirección de correo del remitente no tiene nada que ver con la UPV) y nos amenazan con no poder recibir más correos por haber excedido una cuota (es el problema inexistente). Además, nos conminan a realizar una acción (ir a una página web) para eludir el problema (que no es tal).

Los mensajes de phishing suelen contener muchos elementos que permiten descartarlos rápidamente: las **direcciones** de correo de remitente y destinatarios, la **redacción** del mensaje, el pedirnos que **hagamos** algo para evitar males mayores, **datos** que no corresponden a la UPV, etc. No obstante, si tiene dudas sobre la legitimidad de un correo, recuerde que desde la UPV los **correos oficiales** se envían firmados electrónicamente y puede consultarlos en su Intranet (Consulta de correos oficiales UPV).

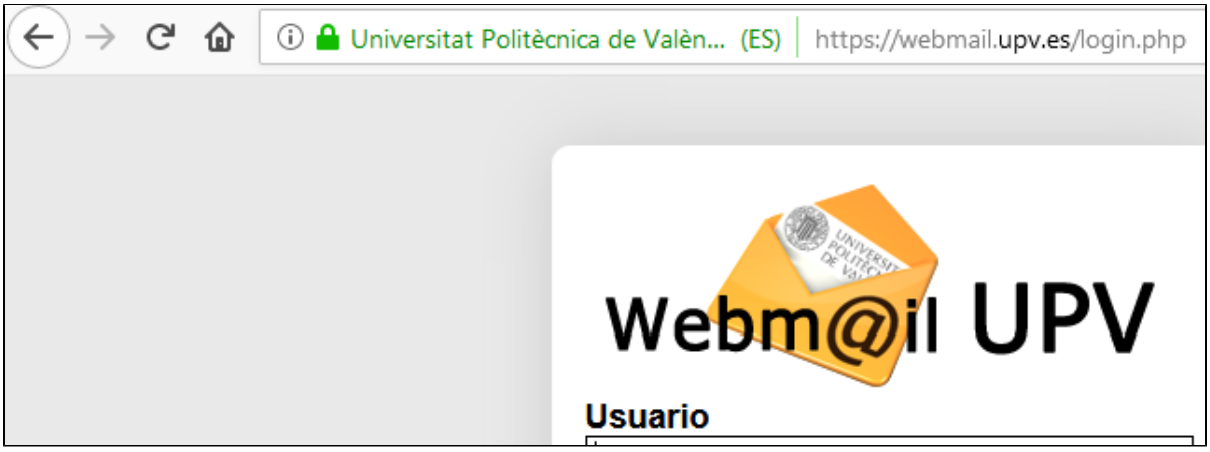
El segundo paso del phishing es una web falsa, que intenta suplantar al servicio.

En el ejemplo anterior, si un usuario picaba el anzuelo se llegaba a esta web:



En toda web, sobre todo si es confidencial y solicita datos personales o credenciales, es imprescindible comprobar la **zona de seguridad** del navegador, para verificar que es una página segura y que estamos contactando con la organización que queremos. En el ejemplo anterior, el navegador ha colocado la advertencia de web no segura, así que ha de descartarse inmediatamente su uso. También podemos fijarnos en que el dominio no corresponde al de la UPV.

Recuerde que, en la UPV, las páginas de acceso a los servicios cuentan con un certificado EV y el navegador le mostrará el nombre de la Universitat en su zona de seguridad:



¿Qué puede hacer si ha recibido un phishing?

Descártelo y no acceda a ninguno de los enlaces que aparezcan en el mensaje. Tampoco conteste al correo.

Para poder realizar el análisis del correo fraudulento, puede usted remitir el correo sospechoso a la dirección fraudeinternet@upv.es. Es importante que utilice la opción *Reenviar como datos adjunto* (en algunos clientes puede aparecer con otros nombres, como *Reenviar como adjunto*); de esta manera el correo a analizar se remite íntegro, sin modificaciones. A continuación, se tomarán las medidas oportunas para anular dicho ataque.

Puede obtener ayuda para el reenvío de un correo como adjunto en la siguiente página: Reenviar correo como adjunto.

¿Qué hace el ASIC para eliminar un phishing?

Una vez detectamos uno de estos ataques (la mayor parte de las veces por la colaboración de los usuarios), intentamos anular la web atacante lo antes posible. En ocasiones podemos cerrarla en minutos y en ocasiones puede haber una demora de horas.

¿Qué ataques se han detectado últimamente?

A continuación tiene un listado de los últimos ataques de *phishing, scam...* recibidos en la UPV y cuyo objetivo era robar credenciales de nuestros servicios:

20200729a RE: IT-Service

20200728a Atención !!

20200708a ¡Atención!

20200706a Atención !!

20200622a Actualización de contraseña

20200615b Tienes {1} nuevo mensaje importante

20200615a Tu buzón está lleno

20200611b Última atualização do Covid-19 <NÃO IGNORAR

20200611a Actualiza tu correo electrónico

20200610a Actualice

20200525b Nueva actualización de seguridad 9.1

20200525a Notificación por correo

20200523a Email Verification usuario@upvnet.upv.es

20200518b Actualización de la aplicación web

20200518a Instrucciones para usted ADVERTENCIA FINAL

20200512a Actualiza tu correo electrónico

20200508a Hola

20200429a Administración de correo electrónico

20200420a Tienes 1 mensaje nuevo del administrador de la facultad.

20200330a Actualice su correo electrónico de la Universidad Politécnica de Valencia UPV,

20200310a Server :: Upgrade your account settings

20200305a FW: Mensaje importante

20200303a UPDATED SECURITY FOR usuario@upv.es

20200302a ATENCION

20200227b Desactivación de cuenta en progreso

20200227a RE: Gracias,

20200214a Última advertencia

20200213a Alerta !

20200205a Actualización importante para *usuario*@upv.es

20200128a Alerta por correo electrónico de la Universidad Politécnica de Valencia

20200116a OLAT learning group OSTA-WS1415

20191126a Notificación 9TXMZY: Comunicación para [...]@upv.es ha detenido

20191115a Presupuesto Orden de compra Urgente

20191108a Documento Importante del Ministerio de Economía y Empresa.

20191103a Confirme Su Casilla de Correo

20191016c IT Sevice.

20191016b Your service has been suspended.

20191016a IT-Service-Desk.

20191001a actualizar cuenta

20190925a Correo electrónico Verificación de acceso

20190920a Confirmation ! Your Email will be shutdown Next 24 hour

20190910a Actualizar

20190905a Incoming email failed

20190830a IT Service Desk. / Service d'assistance informatique.

20190828a IT Service Desk.

20190823a AW: IT Service Desk.

20190822a Re: IT Service.

20190813a Advertencia de actualización del sistema!

20190809a IT Service Desk.

20190807a IT Service Desk.

20190801a Actualización de contraseña

20190725a Suspicious E-mail Login Attempt

20190704a Verifique su cuenta de correo electrónico upv.es ahora!

20190701b Re: IT Help Desk

20190701a Alerta de la biblioteca:

20190619a ACCIÓN REQUERIDA URGENTEMENTE ...

20190612a Alerta web Confirma tu buzón !!!

20190605a Soporte por correo

20190604a Confirma tu buzón !!!

20190521a Actualizar su cuenta

20190515b AVISO DE SERVIDOR DE CORREO WEB

20190515a alerta de correo !!!

20190513a Confirma tu buzón !!!

20190509a Re: Pago

20190508a Soporte UPV

20190507a Confirma tu buzón

20190506a Account Mesage

20190429a Confirma tu buzón !!!

20190425a Correo de la universidad

20190424a Une tentative de connexion à votre compte a été effectuée.

20190419a Por favor verifique su buzón !!!

20190418a Confirma tu buzón !!!

20190416a Actualización de contraseña

20190327a Servicio de asistencia

20190326a Querido usuario

20190325a Estimado usuario de upv.es,

20190320a Su buzón está lleno

20190308a Cuenta Actualizar

20190304a You have 8 pending messages

20190301a Límite de almacenamiento

20190222a Valide su cuenta

20190221a Question - chief of staff / head of school

20190207a Estimado usuario valorado

20190206a Centro de Informacion

20190204a ADVERTENCIA de cuota

20190128c Suspicious E-mail Login Attempt

20190128b Hola

20190128a Hola

20190125a Contact request for faculty application

20190109a Hola

20181231a Help Desk

20181109a Notificación del sistema de emergencia

20181107a Notificaciones urgentes del sistema

20180709a Advertencia de vencimiento del buzón !!

20180707a Atención

20180607a [ASIC] Universidad Cuota de Buzón Excedido!

20180531a NOTIFICACIÓ ACTUALITZADA

20180530a OBLIGATORIO PARA xxxxx@upv.es - CONFIRME SU SOLICITUD PARA DESACTIVAR SU CORREO ELECTRÓNICO EL 30 DE MAYO DE 2018

20180523a Valida tu cuenta

20180517a Límite de cuenta