PHISHING

CONCIENCIACIÓN

Para:
- Revisar siempre quién envía el correo, comprobar qué dirección exacta es **nombre@ucm.es.**
- No conozco a la persona que me envía el correo.
- No reconozco su dirección, no es de la UCM “**Externo**” (no es @ucm.es)
- Aunque el correo sea enviado desde la UCM, no debería haberlo recibido, no le conozco personalmente, no tengo ninguna relación de investigación-docencia-gestión, no me he comunicado con esa persona recientemente.
- Es un correo no esperado con un hipervínculo o archivo adjunto.
- El correo se ha enviado a más gente que no conozco o no tiene sentido que lo reciban.

Asunto:
- Revisa el asunto, tiene sentido que yo reciba un email con ese asunto.
- El asunto está relacionado con el contenido.
- Es un correo electrónico que no he pedido recibir o no debería recibir.

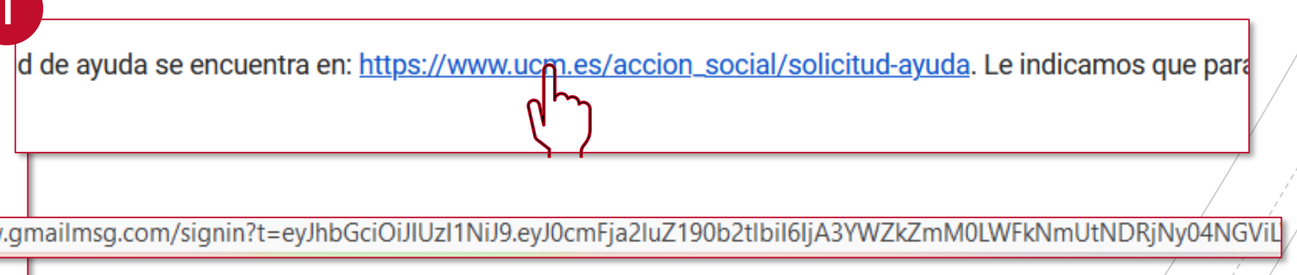
Fichero adjunto:
- Se incluye un fichero que no tiene sentido que reciba en esa forma ya sea por el contenido del mensaje o por la naturaleza de la información que debiera contener.
- Cualquier documento puede ser peligroso, **nunca habilites macros o contenido de terceros** si no conoces al remitente.
- Si al abrir el fichero ves algo raro puede que ya sea tarde.

Contenido:
- El contenido me insta a **descargar o clicar en un enlace, de forma apresurada** o ilógica para la manera de actuar de la UCM.
- El contenido me genera una sensación inconfortable.
- El contenido me ofrece información que yo no debería tener o que no tiene ninguna relación con mi responsabilidad dentro de la UCM.
- En la actualidad el contenido de un correo de *phishing* puede estar escrito en un perfecto castellano.

Hipervínculo (link):
- Son tan peligrosos como los fichero adjuntos.
- No te fíes de la dirección que aparece en el contenido:

1. Coloca el ratón sobre el hipervínculo
2. Observa la dirección a la cuál te va a redireccionar

- Desconfía si no es del UCM
- Desconfía si es “muy Larga”
- Nunca introduzcas tus credenciales (contraseña) desde un enlace de un correo.



PHISHING

CONCIENCIACIÓN

Un ataque de phishing consiste en intentar mediante **correos electrónicos aparentemente fiables** adquirir fraudulentamente información de los usuarios (principalmente contraseñas) o instalar software malicioso en sus ordenadores.

- Instar a los usuarios a clicar en páginas web falsas que intentan engañar al usuario para facilitar datos de carácter personal (contraseñas, cuentas bancarias, número de la seguridad social …).
- Instar a los usuarios a descargase archivos aparentemente fiables para instalar software de carácter malicioso en su ordenador.

1

Envío de correos fraudulentos a varios usuarios

2

Una persona de la UCM abre el correo

3

Esa persona se descarga el fichero o clica sobre un enlace que ejecuta un malware (virus)

4

El ordenador de esa persona se ha visto comprometido y probablemente el virus se extienda a otros ordenadores y servidores de la UCM

CONTRAMEDIDAS

- Comprueba siempre el dominio del remitente
- Comprueba los enlaces que lleguen por correo
- Evita descargar archivos adjuntos si no conoces al remitente
- Evita introducir tu usuario@ucm.es y contraseña desde enlaces del correo
- Mantén actualizado el navegador
- No utilices tu cuenta @ucm.es para darte de alta en aplicaciones no relacionadas directamente con tu desempeño profesional
- Utiliza sólo aplicaciones descargadas desde sitios oficiales
- Habilita el segundo factor de autenticación y cambia la contraseña cada 6 meses

Notifica cualquier correo raro a abuse@ucm.es

PHISHING

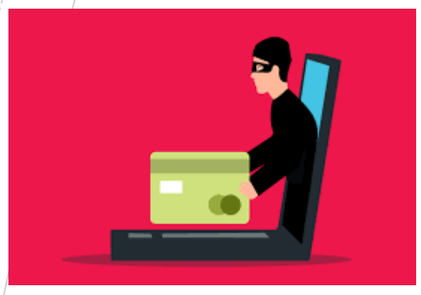
CONCIENCIACIÓN

IMPORTANCIA DEL PERSONAL DE LA UCM

El phishing representa el **vector de ataque más utilizado** contra los actores internos más vulnerables de una organización; hasta en un **38% de los incidentes** involuntarios provocados por actores internos se han originado a través de este vector de ataque*. Todo ello sitúa al personal interno como uno de los agentes de amenaza más presente en los próximos periodos.

https://financesonline.com/insider-threat-statistics

CÓMO TE LEVANTAN 100.000€ SIN PESTAÑEAR



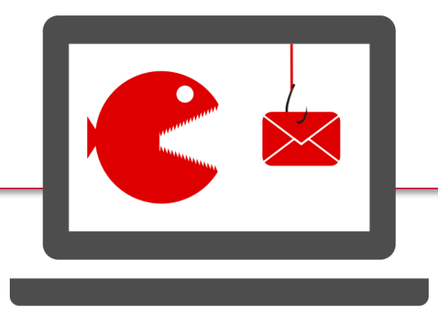
Para socavar las finanzas de las empresas, los atacantes falsifican cuentas y sitios web corporativos (normalmente mediante ligeras modificaciones del nombre), envían **correos de phishing dirigido** (spear phishing) o introducen malware específico para analizar previamente los correos y no levantar sospechas, o bien para acceder a datos confidenciales de las potenciales víctimas

https://www.securityartwork.es/2019/12/10/como-te-levantan-100-000e-sin-pestanear-analisis-forense-de-una-estafa-al-ceo-iv/

CUENTA @UCM COMPARTIDA EN OTRAS PLATAFORMAS

A principios de 2021 se pone de manifiesto la vulnerabilidad que suponen las técnicas de scraping automatizadas a gran escala en las redes sociales, con la filtración masiva de datos personales de plataformas como **TikTok, YouTube, Facebook, Clubhouse y LinkedIn**. Se trata de la mayor colección de información privada conocida hasta la fecha extraída mediante el abuso de funcionalidades y favorecida por la laxa configuración de privacidad por defecto de los perfiles de usuarios. **Esta información será sin duda utilizada en futuras campañas de phishing.**

- A finales de 2020, investigadores de ciberseguridad detectaron otra campaña de phishing llevada a cabo por este grupo, también conocido como Charming Kitten. Sus objetivos fueron empleados técnicos de la OMS, y organizaciones del sector médico y centros de investigación de la salud de los Estados Unidos.
- Intensa actividad de phishing durante todo 2020 contra objetivos militares, gubernamentales y diplomáticos en Ucrania.
- Ataques contra la campaña presidencial de Joe Biden, mediante el envío de spearphishing suplantando a una reconocida empresa de ciberseguridad.
- Campañas de phishing contra organismos gubernamentales del gobierno de Malasia, a quienes enviaron un fichero infectado que suplantaba a un evento político local.
- Phishing de suplantación del Ministerio de Trabajo.
- Phishing de suplantación de la Agencia Tributaria.
- Campaña de phishing suplantando a la Dirección General de Tráfico.
- Ataque de phishing a la Universidad de Barcelona



QUÉ ESPERAR

Los ataques de phishing, en todas sus formas, ya sean correos electrónicos para toda la empresa, ataques al empleado dirigidos a su correo electrónico corporativo (BEC) seguirán muy presentes en 2022.

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html