Phishing

Los mensajes de remitentes suplantados pueden engañar al destinatario para que seleccione un vínculo y ceda sus credenciales, descargue malware o responda a un mensaje con contenido confidencial.
Como en este ejemplo:

De: Microsoft Outlook (Anna Korompay) <korompay.anna@med.semmelweis-univ.hu>
Enviado: jueves, 10 de agosto de 2023 08:22
Asunto: Notificaciones de buzones.

(!) Consejo útil:
Remitente externo. Tenga cuidado cuando un correo electrónico sea externo, contenga un adjunto o vínculo incrustado. Incluso si el remitente le parece familiar, asegúrese siempre antes de hacer clic en el adjunto o enlace.

499MB **499MB**

El buzón de tu cuenta Microsoft está lleno. "haga clic aquí" para actualizar su cuenta de buzón y recibió un nuevo mensaje.

Gracias,
Administrador del sistema.

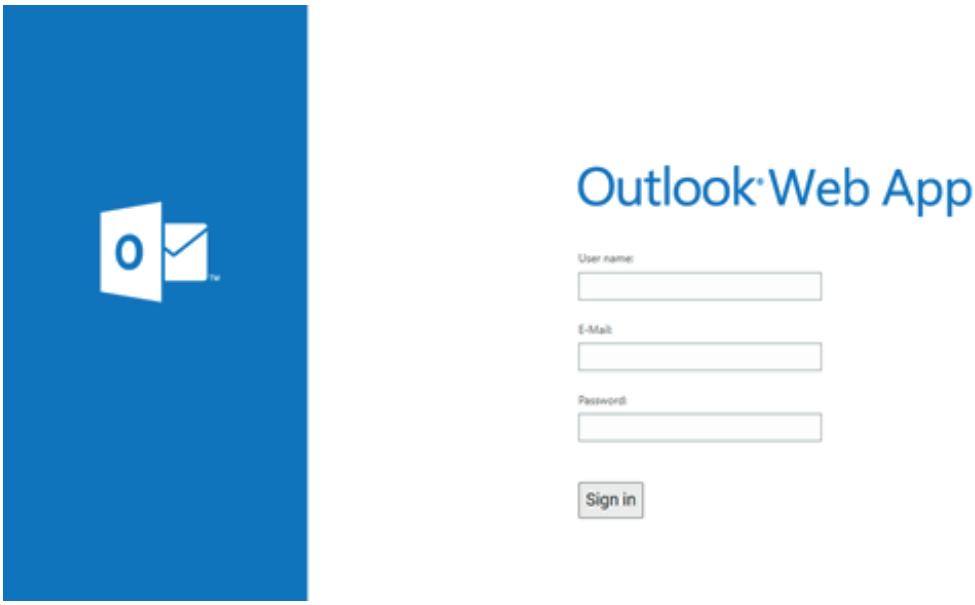
Este mensaje no proviene del Depto. Redes de Honorable Cámara de Diputados, sino que el remitente intentó engañar al destinatario buscando que al confundirlo, ingresara en el vínculo y cambiara su contraseña, proporcionandole de este modo sus datos.
Al poner el puntero del mouse donde dice "haga clic aquí", veremos que el link no es de una página oficial perteneciente a la HCD.

499MB **499MB**

El buzón de tu cuenta Microsoft está lleno. "haga clic aquí" para actualizar su cuenta de buzón y recibió un nuevo mensaje. http://sss3sf.builder.hemsida24.se/

Gracias,
Administrador del sistema.

Se trata de una estafa mediante correo electrónico que han recibido varios usuarios de Outlook.com, dónde se les solicita que verifiquen su cuenta. Esto es una estafa diseñada para obtener acceso a su datos y los spammers puedan utilizarlos para enviar spam.

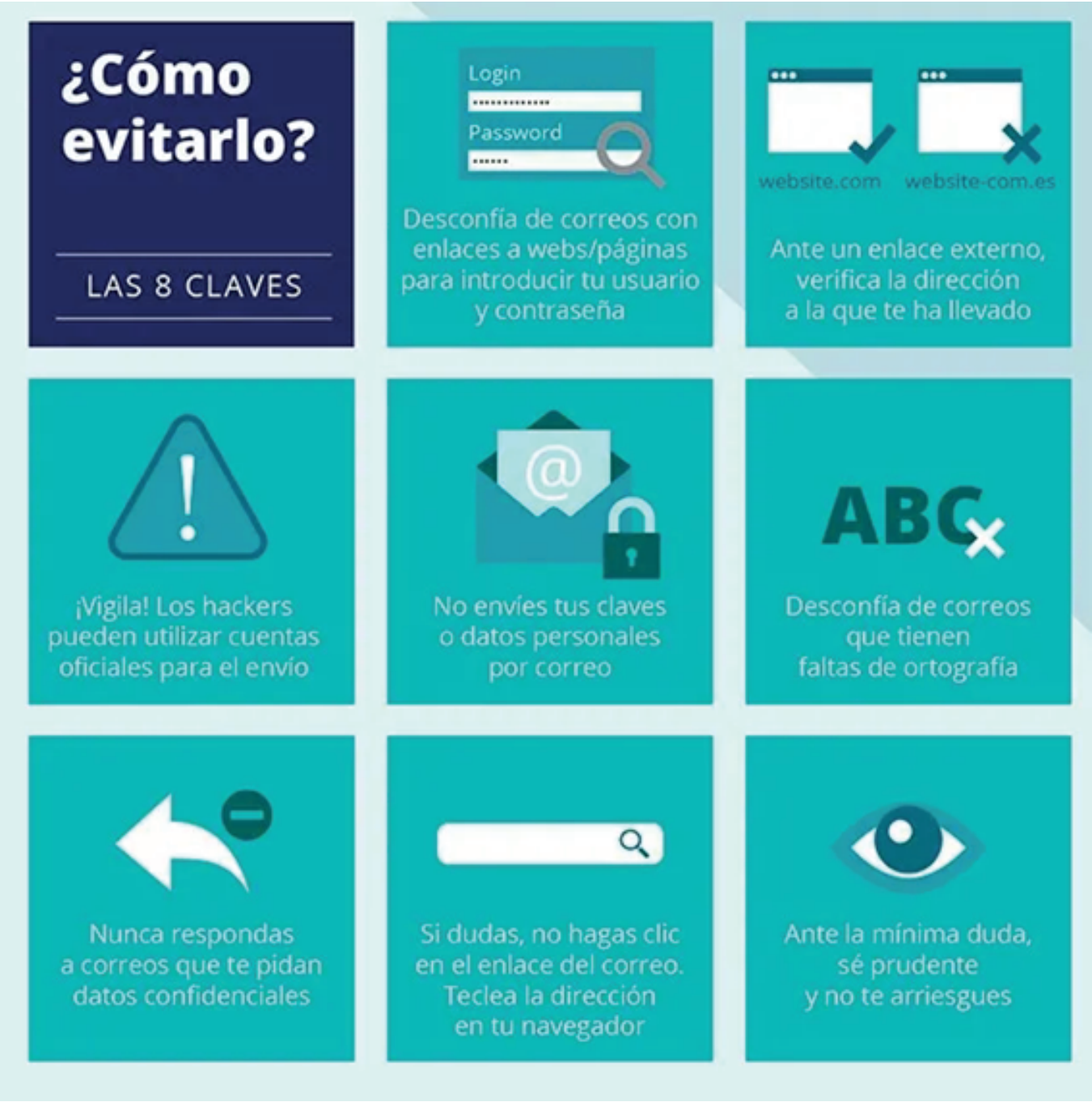


El link de esta página falsa es wewvin.builder.hemsida24.se
No es nuestro dominio **(hcdiputados-ba.gov.ar)** por lo tanto se trata de un caso de Phishing para robar nuestras credenciales y utilizarlas para otros fines.

El Depto. Redes y Conectividades nunca pedirá cambiar la contraseña de esta forma, sino mediante un mail de recuperación.

Tampoco se informa de esta manera la cuota de su buzón.

Nunca introduzca sus datos en este tipo de páginas.


¿Cómo evitarlo?
LAS 8 CLAVES
Login
Password
Desconfía de correos con enlaces a webs/páginas para introducir tu usuario y contraseña
website.com
website-com.es
Ante un enlace externo, verifica la dirección a la que te ha llevado
¡Vigila! Los hackers pueden utilizar cuentas oficiales para el envío
No envíes tus claves o datos personales por correo
ABC
Desconfía de correos que tienen faltas de ortografía
Nunca respondas a correos que te pidan datos confidenciales
Si dudas, no hagas clic en el enlace del correo. Teclea la dirección en tu navegador
Ante la mínima duda, sé prudente y no te arriesgues