



Fuerzas Armadas de Honduras

Estado Mayor Conjunto

Dirección de Comunicaciones e Informática (C-6)

"200 Años al Servicio de la Patria"



Comayagüela, M.D.C.
20 de junio de 2025

REGISTRO : EMC-(C-6) / EMC-(DEPENDENCIAS) / No.0372-06-2025
EXPEDIENTE : EMC-(C-6) / EMC-(C-6)

A S U N T O : **CIRCULAR**

A L : SEÑOR (ES)
DIRECTORES DE ORGANISMOS Y DEPENDENCIAS DEL ESTADO MAYOR CONJUNTO Y COMANDOS ESPECIALES, CFAC, FTC-GPPG, FTC-MAYA CHORTI, FTC-LENCA SUMPUL, FTC-XATRUCH, CALFFAA, XXI BTN. DE PM, UHR, UOMP, HOSPITAL MILITAR, CODOCEM, GHP, INP, CENTROS DE ESTUDIOS (UDH, CDN, ECEM Y CELFFAA)
SU OFICINA

I. Muy atentamente y con instrucciones del señor Jefe del Estado Mayor Conjunto, General de División Don **Roosevelt Leonel Hernández Aguilar**, por este medio me dirijo a usted (es) para informar que se ha detectado la recepción de correos electrónicos fraudulentos, conocidos como intentos de **suplantación de identidad (phishing)**, en **varias cuentas de correo institucional** de las FF.AA. Estos mensajes tienen como objetivo engañar a los usuarios para que revelen sus credenciales (usuario y contraseña), accedan a sitios falsos o realicen acciones que puedan comprometer la seguridad de la institución.

Ante esta situación, **se instruye a todo el personal a adoptar de inmediato medidas de seguridad preventivas**. Al identificar un correo sospechoso o fraudulento, **no debe abrirlo, hacer clic en ningún enlace, ingresar credenciales, ni descargar archivos adjuntos**. En su lugar, debe **reportarlo inmediatamente a la Dirección C-6**, siguiendo las recomendaciones que se detallan a continuación:

- A. Medidas obligatorias para prevenir ataques de suplantación de identidad (phishing):
1. **No abrir correos electrónicos de remitentes desconocidos o sospechosos.** En caso de duda, contactar con la Dirección C-6 antes de interactuar con el mensaje.

2. **No hacer clic en enlaces incluidos en correos sospechosos**, incluso si aparentan ser institucionales.
3. Verificar siempre la dirección del correo institucional antes de ingresar sus credenciales. El único sitio válido es: **<https://mail.ffaa.mil.hn>**
4. No proporcionar nombres de usuario ni contraseñas institucionales a través de correos electrónicos, formularios o enlaces no oficiales.
5. Ignorar y reportar mensajes que soliciten acciones urgentes, como cambiar contraseñas, actualizar datos o verificar cuentas, especialmente si el tono es alarmante.
6. No descargar ni abrir archivos adjuntos inesperados o con extensiones inusuales, como .exe, .rar, .zip, entre otros.
7. Utilizar exclusivamente el correo institucional para el manejo de información oficial.
8. Reportar de inmediato cualquier correo sospechoso a esta Dirección C-6.
9. **Si accidentalmente ingresó a un sitio fraudulento o proporcionó sus credenciales, notifíquelo de inmediato a la Dirección C-6** para recibir la asistencia correspondiente y evitar un compromiso mayor de la red institucional.

B. Evidencias recientes de intentos de phishing

Se adjuntan ejemplos reales de correos electrónicos maliciosos que han sido recibidos en cuentas institucionales de las Fuerzas Armadas, cuyo propósito era obtener credenciales o inducir a ingresar a sitios falsos. Estos mensajes representan una amenaza directa a la seguridad institucional.

Las características comunes de estos correos son:

1. Remitentes falsos o desconocidos
2. Mensajes con tono urgente, alarmista o sospechosos
3. Enlaces engañosos que imitan sitios oficiales
4. Archivos adjuntos no solicitados o con nombres extraños

5. Errores ortográficos o gramaticales evidentes, o redactados en un idioma diferente al español.

Se recuerda al personal no interactuar con este tipo de correos y reportarlos inmediatamente a la Dirección C-6.

Se adjunta, Ejemplos de correos fraudulentos de suplantación de identidad (phishing) recibidos.

- II. Sin otro particular, me suscribo de usted (es) con mis muestras de consideración y estima.

HONOR

LEALTAD

SACRIFICIO



OMNC/fyve
CC/

Ejemplos reales de correos electrónicos de phishing.

Actualización de su cuenta zimbra.

De: "ADMIN ZIMBRA" <barka@inpt.ac.ma> 1 mensaje
2 de Junio de 2025 18:00

Hola usuario,

Esta es la última actualización de ZIMBRA si te perdiste la última, es una notificación de una actualización obligatoria para aumentar el uso del buzón y la actualización.

Tenga en cuenta que es la última notificación. Se desactivará cualquier casilla de correo que no se haya actualizado. Esta es una actualización gratuita.

Haga clic aquí para actualizar su correo electrónico.

Cordialmente,
Gestión de Servicios Tecnológicos

Important Message

Cerrar Responder Responder a todos Reenviar Archivo Eliminar Spam Acciones ▾ 4 de Junio de 2025 07:01

De: "zimbra helpdesk" <lorena@iberlegal.com>
Para: "Direccion de, Cmns. e Informatica" <c-6@ffaa.mil.hn>
Responder a: helpdesk@zimbra.com

(9) nine new incoming pending messages, Kindly use the link below to sign into your zimbra account c-6@ffaa.mil.hn to restore important pending messages.

Restore incoming messages.

Failure to do so, your zimbra account may not receive any incoming messages.

Vuelva a validar su cuenta ahora.

De: "Zimbra Management" <mogarcia@dgeip.edu.uy> 1 mensaje
9 de Junio de 2025 00:13

ADVERTENCIA !!! ADVERTENCIA !!! ADVERTENCIA !!! ADVERTENCIA !!!

Estimado usuario valioso:
Su cuenta será: **SUSPENDIDA**
Si desea continuar usando su dirección de correo electrónico
Haga clic en el enlace e inicie sesión

Haga clic para actualizar su cuenta de correo electrónico ahora

Nota: El propietario de la cuenta que se niega a actualizar su cuenta dentro de los siete días posteriores a la recepción de este aviso termina siendo suspendido permanentemente.

Gracias por su cooperación para ayudar a mejorar nuestro servicio.

© Zimbra, Inc. Departamento 317, PO Box 18025, Palo Alto, 44801 Copyright ©2025

Verifique y valide su cuenta de correo electrónico.

1 mensaje

* De: "Zimbra Management" <agonnet@dgeip.edu.uy>

10 de Junio de 2025 02:41

Atención: esta es una alerta de servicio por correo electrónico del servicio de asistencia técnica. Nuestra última seguridad de IP descubrió un intento de inicio de sesión irregular en su cuenta de correo electrónico hoy desde una ubicación desconocida con dirección IP: 197.269.112.82. Nuestra seguridad de acceso limitado requiere que verifique y valide su cuenta de correo electrónico.

HAGA CLIC AQUÍ y siga las instrucciones para actualizar y verificar su cuenta de correo electrónico. El incumplimiento resultará en la cancelación de su cuenta de correo electrónico.

Saludos,
Soporte técnico de Zimbra
Copyright ©2025 Zimbra Sistema de actualización*

Cerrar Responder Responder a todos Reenviar Archivo Eliminar Spam Acciones ▾

Se necesita una intervención urgente

11 de Junio de 2025 15:09

De: "HelpDesk" <luciana.bonucchi@terredicastelli.mo.it>

Estimado usuario:

Nuestros registros indican que su cuenta no se ha actualizado como parte de nuestro mantenimiento regular. Estamos cerrando algunos correos electrónicos registrados en Zimbra que están causando un mal funcionamiento de nuestro sistema debido a que no se utilizan. Por lo tanto, estamos eliminando todas las cuentas no utilizadas para crear espacio para nuevas cuentas.

Para evitar la suspensión de su cuenta

(Revise su cuenta aquí)

Atentamente
Equipo de Soporte Técnico.
Copyright © 2005-2025 Todos los derechos reservados