

## **Nota de Seguridad UNAM-CERT-2011-001 Aviso: Intentos de engaño recibidos en el correo electrónico UNAM**

Un correo legítimo nunca le solicitará que envíe el nombre de usuario ni contraseña de su cuenta, por lo cual no debe responder a estos mensajes.

- **Fecha de Liberación:** 23-Mar-2011
- **Última Revisión:** 23-Mar-2011
- **Fuente:** UNAM-CERT

### **1. Usuarios afectados**

Cualquier usuario del servicio de correo electrónico de la UNAM.

### **2. Descripción**

Algunos usuarios del servicio de correo electrónico de la UNAM han recibido mensajes por esta vía con el fin de obtener información personal relevante (como nombre de usuario y contraseña). Estos correos son FALSOS, utilizan una técnica conocida como Phishing y de ninguna manera se debe responder a ellos.

Los correos legítimos enviados por administradores de este servicio de la UNAM NUNCA solicitarán este tipo de información.

### **3. Impacto**

Los usuarios que respondieron a estos mensajes pueden haber comprometido el nombre de usuario y contraseña de sus cuentas de correo electrónico, así como las direcciones de sus contactos, a quienes muy probablemente podrán reenviárseles estos correos para reproducir el ciclo de distribución.

### **4. Solución**

Con la finalidad de proteger la integridad de las cuentas de correo electrónico, se ha puesto a disposición de los usuarios, el "[Manual de identificación y notificación de correo fraudulento para usuarios UNAM](#)".

Si respondió a alguno de estos mensajes, solicite el cambio de inmediato. Para mayores informes, contacte a la Coordinación del Centro de Atención a Usuarios, DGTIC, UNAM, a los teléfonos 56651966 y Ext. 46190 a 46194, o bien al sitio [www.ayuda.telecom.unam.mx](http://www.ayuda.telecom.unam.mx).

### **5. Referencias**

- ◆ "Manual de identificación y notificación de correo fraudulento para usuarios UNAM" [http://www.seguridad.unam.mx/manual\\_phishing.dsc](http://www.seguridad.unam.mx/manual_phishing.dsc)
- ◆ Consejos sobre Phishing Scam [http://www.seguridad.unam.mx/consejos\\_phishing.dsc](http://www.seguridad.unam.mx/consejos_phishing.dsc)
- ◆ Buenas prácticas de seguridad informática [http://www.seguridad.unam.mx/buenas\\_practicas.dsc](http://www.seguridad.unam.mx/buenas_practicas.dsc)

6. **Anexo**

----- Ejemplo de este tipo de correos -----

Asunto: URGENTE - Verificación de la cuenta de actualización 2011

De: "UNAM"

Fecha: Vie, 11 de Febrero de 2011, 12:51 pm

Para: undisclosed-recipients;--

Estimado cliente,

Este mensaje es de la UNAM WEBMAIL centro de mensajes a todos los servidor.unam.mx particular cuenta de correo web. En estos momentos estamos actualizando nuestra base de datos y el centro cuenta de correo electrónico.

Para evitar que su cuenta se cierre tendrá que actualizarlo respondiendo a este mail a continuación para que podamos saber que es una cuenta que se utiliza actualmente.

Confirmar su identidad EMAIL UNAM ABAJO:

Su nombre:

Dirección completa:

Nombre de usuario de correo electrónico:

Email Contraseña:

Advertencia! Cualquier propietario de la cuenta que se niega a actualizar su cuenta de correo electrónico después de haber recibido esta advertencia perderá su cuenta permanentemente.

Gracias por usar webmail.servidor.unam.mx

Código Advertencia: VX2G99AAJ

Gracias,

WEB Jefe de equipo

UNAM SERVICIO WEBMAIL

Universidad Nacional Autónoma de México.

-----FIN-----

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

## UNAM-CERT

- Galvy Ilvey Cruz Valencia (gcruz at seguridad dot unam dot mx)
- Jesús Mauricio Andrade Guzmán (mandrade at seguridad dot unam dot mx)

### UNAM-CERT

Equipo de Respuesta a Incidentes UNAM  
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx

phishing at seguridad.unam.mx

<http://www.cert.org.mx>

<http://www.seguridad.unam.mx>

<ftp://ftp.seguridad.unam.mx>

Tel: 56 22 81 69

Fax: 56 22 80 47