

## INTENTOS DE ENGAÑO RECIBIDOS EN EL CORREO ELECTRÓNICO

- 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.
- Un correo legítimo **NUNCA** le solicitará que envíe el nombre de usuario ni contraseña de su cuenta, por lo que **NO DEBE RESPONDER** dichos mensajes.
- Si respondió a alguno de estos mensajes, debe solicitar el cambio inmediatamente, para lo cual deberá ponerse en contacto con la Coordinación del Centro de Atención a Usuarios, DGTIC, UNAM, a los teléfonos 56651966 y extensión 46190 a 46194 o bien al sitio <http://ayuda.telecom.unam.mx>

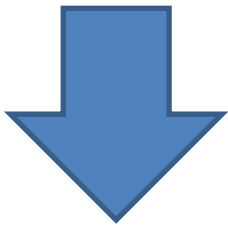
# Reportar incidentes

- La Subdirección de Seguridad de la Información/UNAM-CERT pone a disposición de toda la comunidad usuaria de cómputo, las siguientes cuentas de correo electrónico para reportar incidentes de seguridad informática

# Reportar incidentes

- phishing @seguridad.unam.mx

- Para reportar Phishing Spam. Incluir en el correo la URL (Uniform Resource Locator-localizador uniforme de recursos) del sitio phishing, esta URL se obtiene colocando el puntero del mouse sobre el hipervínculo, por ejemplo si coloco el puntero del mouse sobre la palabra TELMEX aparecerá su URL como sigue:

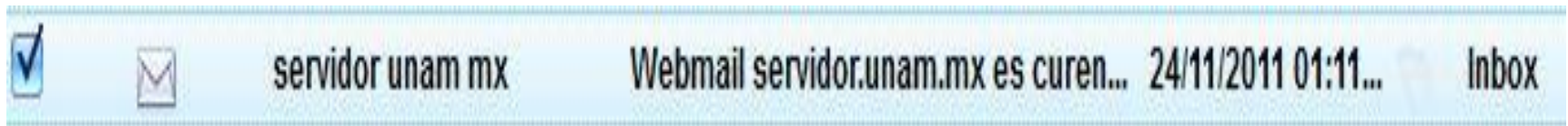


<http://www.telmex.com>

# Reportar incidentes

phishing @ seguridad.unam.mx

Si usted recibió un correo electrónico y sospecha que se trata de un caso de phishing spam, por favor envíe los encabezados del correo



# **Junto con el correo original.**

**Estimado suscriptor Webmail,**

Debido al spam quejas de los usuarios de correo electrónico en nuestro webmail sistema, nuestra investigación muestra que su dirección de correo electrónico está comprometida y se utiliza para enviar spam en nuestro webmail system. As resultado, nuestro ingeniero de red realizar una nuestros servicios de mantenimiento del sistema de correo web, su nombre de usuario será desactivado **si no nos envíe la la información requerida dentro de las 24 horas.**

**La información que se necesita:**

**Sus nombres:**

**Conexión página:**

**Nombre de usuario:**

**Contraseña:**

**Vuelva a escribir la contraseña:**

Por favor, acepte nuestras disculpas por cualquier inconveniente.

Nosotros valoramos su negocio y gracias por usar nuestros

Webmail Service.Maintenance

Webmail del equipo. Actualización de la web el servicio de correo

Cuenta de correo electrónico del Equipo de Apoyo

Código de advertencia: ID67565434

# incidentes @ seguridad.unam.mx

Para reportar cualquier otro incidente de seguridad informática. Incluya su información de contacto, una descripción del problema del incidente, incluyendo direcciones IP(Internet protocol-protocolo de internet) y/o nombres de host o dominio involucrados.

# SUGERENCIAS PARA LA CREACIÓN DE CUENTA Y CONTRASEÑA DE UN USUARIO

- Para crear contraseñas con mayor seguridad es recomendable que sean caracteres alfanuméricos y símbolos
- Evitar utilizar información personal como: números telefónicos y fechas de nacimiento.
- Se recomienda cambiar la contraseña por lo menos cada 60 a 90 días
- Utilizar contraseñas con un número mínimo de 8 caracteres
- Limitar el uso de redes sociales desde el trabajo, como son: correo electrónico personal, mensajería instantánea, Facebook, Twitter, etc., excepto cuando exista un caso de negocio válido y documentado para su uso.
- No compartas tus contraseñas con nadie.
- Evita utilizar la misma contraseña para distintos servicios.

# SUGERENCIAS PARA LA CREACIÓN DE CUENTA Y CONTRASEÑA DE UN USUARIO

Uso de programas Anti Spyware: Spyware es un término utilizado para los programas que pueden alojarse en tu PC a fin de monitorear y registrar las actividades que realizas mientras navegas por Internet. El resultado de este monitoreo puede utilizarse tanto para fines comerciales como con propósitos maliciosos, por ejemplo para extraer información personal que hayas ingresado como contraseñas, números telefónicos, números de tarjetas de crédito así como claves de tus cuentas bancarias.

***\* Si notas que tu equipo se alenta, por favor acude al Departamento de Apoyo Técnico de Cómputo de esta Facultad.***