



**CIRCULAR No. 10532 /16**

NT/nt

Montevideo, 13 de abril de 2016

**DE: DIRECCION GENERAL**

**A: TODOS LOS SERVICIOS DE CAPITAL E INTERIOR**

**Asunto:** Alerta sobre recepción de mensajes tipo **phishing** que llegan a los usuarios del mail institucional y recomendaciones.

Atento a que el Departamento de Tecnologías de la Información informa que la semana pasada y en el día de la fecha se han registrado varios casos de mensajes tipo phishing y se confirma por parte de AGESIC que INAU es el principal afectado en estos casos ya que sus casillas han sido vulneradas con mucha frecuencia, lo que hace que el dominio @inau.gub.uy sea más atacado que el resto por la cantidad de correos que le están llegando.

Al respecto, se hace necesario alertar a los usuarios del mail institucional respecto a lo que está sucediendo y se exhorta a los servicios a cumplir con las recomendaciones establecidas por el Departamento de Tecnologías y los administradores del correo institucional Sra. Araceli Sánchez y Sr. Daniel Pavoni.

**Recomendaciones:**

- Eliminar este tipo de mensajes
- Nunca brindar información de contraseña a nadie
- hacer correr el antivirus en la PC
- En caso de haber ofrecido la información solicitada en el mensaje, cambiar la contraseña de la casilla de mail.
- Reportar al Departamento de Tecnologías de la Información a través de seguridadinformatica@inau.gub.uy la existencia de ese tipo de mensajes.

A fin de ampliar la información, se adjunta texto elevado por el Departamento de Tecnologías de la Información.

RB.

**Psic. ISABEL BATA  
DIRECTORA GENERAL  
I.N.A.U.**

Atento a que durante las últimas semanas se ha registrado un volumen considerable de mensajes de mail tipo phishing, es necesario realizar las siguientes puntualizaciones:

**Que son los phishing:** El “phishing” consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

**Texto del phishing:** En términos generales están redactados en forma tal que intentan adquirir información confidencial del usuario y en general encabezan el asunto del mensaje de correo electrónico haciendo referencia a que la casilla de correo está llena o sin espacio.

**Riesgo del phishing:** Los remitentes de estos mensajes intentan obtener información de las cuentas y el hecho de que el usuario por desconocimiento ofrezca la información allí solicitada hace además que se reenvíen automáticamente grandes cantidades de spam al resto de la base de contactos. Esto **pone en riesgo a todas las cuentas del organismo** ya que el servidor detecta anomalía en el tráfico de mensajes y automáticamente pone las cuentas de dominio @inau.gub.uy en **lista negra**, lo que significa que se bloquean sin posibilidad de enviar o recibir.

**Qué hacer :**

- cuando llegan estos mensajes no hay que abrirlos, hay que **ELIMINARLOS**
- NUNCA** brindar información de **contraseñas a nadie**
- Hacer correr inmediatamente el antivirus y antimalware a ~~la~~ máquina para evitar la pérdida de información contenida en la PC.

Desde el Departamento de Tecnología los funcionarios administradores de la plataforma de mails institucionales son únicamente: Araceli Sánchez ([asanchez@inau.gub.uy](mailto:asanchez@inau.gub.uy)) y Daniel Pavoni ([dpavoni@inau.gub.uy](mailto:dpavoni@inau.gub.uy)) por lo tanto en caso de comunicar por mail algún asunto relacionado a las casillas de correo institucionales, únicamente se hará a través de esos remitentes.

**En ningún caso los administradores solicitarán información de las contraseñas.**