República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Informe

Número: IF-2021-92362684-APN-DICO#PNA

CIUDAD DE BUENOS AIRES
Miércoles 29 de Septiembre de 2021

Referencia: BOLETIN INFORMATIVO DE SEGURIDAD N° 06/21

BOLETIN INFORMATIVO DE SEGURIDAD Nº 06/21

SITUACIÓN:

Se tomó conocimiento que se filtraron datos sensibles, de los afiliados del Instituto de Obra Social de las Fuerzas Armadas y de Seguridad (IOSFA), algunos de los datos expuestos fueron:

APELLIDOS, NOMBRES, DNI / LE, FECHA DE NACIMIENTO, SEXO, ESTADO CIVIL, PARENTESCO, TIPO AFILIADO, GRADO, CODIGO SUC, CALLE, NRO CALLE , PISO DPTO, TIPO REV, CODIGO POSTAL, LOCALIDAD, PROVINCIA, TELEFONO, DELEGACION, MAIL.

RECOMENDACIÓN:

Esta información resulta de gran valor para los ciberdelincuantes, dándoles facilidad en sus ataques dirigidos de phishing o vishing fraudes dado que poseen datos personales.

Es importante concientizar a la totalidad de nuestros Recursos Humanos, que existe la posibilidad de que sean llamados por ciberdelincuentes haciéndose pasar por personal de la obra social IOSFA (Instituto de Obra Social de las Fuerzas Armadas y de Seguridad), ya que poseen todos los datos necesarios para armar una estafa tanto vía telefónica (vishing), redes sociales (facebook, instagram, twitter), como por email (phishing).

Tenga en cuenta que el ciberdelincuente puede poseer, tanto sus datos personales, como el de su entorno familiar afiliado (esposa, esposo, hijo, hija, conyuge, etc).

Importante: Ante el caso de que ocurra esta situación, no brinde ningún tipo de datos y comuníquese inmediatamente a los teléfonos oficiales de la obra social para ser asesorado.

NO OLVIDE:

- No abra correos de usuarios desconocidos o que no haya solicitado, elimínelos directamente.

- No haga clic en los enlaces que aparezcan en los correos electrónicos no solicitados o que cuyo remitente desconoce, esto le ayudara a no ser víctima de fraudes y malware.
- No conteste en ningún caso a estos correos, ni envíe información personal.
- Tenga siempre actualizado el sistema operativo y el antivirus.
- No utilice la misma contraseña en todos los servicios online que use, no es una práctica segura.
- Para una mayor seguridad en sus procesos de acceso a sistemas bancarios, correo electrónico o redes sociales es conveniente establecer un doble factor de autenticación. Para solicitar el instructivo de configuración del doble factor de autenticación en las cuentas de correo oficial comunicarse al Interno 2977.
- Prestar atención al dejar de utilizar un sistema, correo electrónico, cuenta bancaria, etc. y cierre siempre sesión.
- Realice copias de seguridad de la información que almacena en sus dispositivos. De esta manera, en caso de intrusión (hackeo), pérdida o robo del dispositivo siempre podrá recuperar sus datos.
- Realice periódicamente análisis con antivirus de los equipos de trabajo y de todos los archivos que descargue de internet o transfiera desde otras computadoras, ya sea por red, correo electrónico o pendrives. Recordar que el mismo puede descargarse desde la Intranet.
- Tenga activado el Firewall de su PC.
- De manera preventiva cambie su actual contraseña por una más fuerte con combinaciones de letras en mayúsculas y minúsculas, caracteres especiales y números.
- Se recuerda el uso responsable de las PC institucionales y su acceso a la red de Internet e Intranet (Publicación R.I. PNA 3-004 "Políticas de Seguridad de la Información de la Prefectura Naval Argentina" disponible en la Intranet), como también el correcto uso y conservación del material informático.
- Fuera de la institución, aquellos usuarios autorizados a ingresar a la Red Privada Virtual vía conexión VPN, deben mantener sus dispositivos protegidos (PC/Notebook, u otro utilizado para conectarse vía VPN) con programas al efecto: antivirus, firewall, etc., en caso de dudas contactarse con la División Seguridad Informática de la DICO para consultar por estos programas y cuáles son los recomendados sin costo.
- Lea con frecuencia las actualizaciones del sitio de la División Seguridad Informática de la DICO en la Intranet.
- Ante la recepción de este tipo de correos electrónicos dar aviso a la Sección Mensajería Institucional (interno 2977) o a la División Seguridad Informática (internos 2942/44) enviar copia del email a segu-info@prefecturanaval.gov.ar. Para mejor proveer se adjunta copia de correo recibido.

“RECUERDE QUE EL USO RESPONSABLE Y CONSCIENTE DE LAS TECNOLOGÍAS REDUCE SIGNIFICATIVAMENTE LOS RIESGOS, AUMENTANDO TANTO SU SEGURIDAD COMO LA DE LA INSTITUCIÓN”

Digitally signed by Gestion Documental Electronica
Date: 2021.09.29 13:10:17 -03:00

Jorge Osvaldo Soto
Prefecto Principal
Dirección de Informática y Comunicaciones
Prefectura Naval Argentina

Digitally signed by Gestion Documental Electronica
Date: 2021.09.29 13:10:17 -03:00