Recomendaciones para el buen uso del correo institucional

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA UTN (01 Julio 2020)

El Correo Electrónico Institucional es un servicio brindado por la Universidad Tecnológica Nacional para contribuir con el desarrollo de las actividades laborales y académicas. Las siguientes recomendaciones son para instruir a los usuarios que posean una cuenta institucional de la UTN sobre el adecuado uso de dicho servicio de correo electrónico con el fin de garantizar seguridad y eficiencia, evitando en lo posible la recepción y envío de correo no deseado (SPAM) y/o fraudulento.

Buenas prácticas en general

- Elija contraseñas seguras (robustas). A la hora de elegir la contraseña de acceso a su correo electrónico, tenga en cuenta las siguientes consideraciones:
  - Debe tener al menos 10 caracteres de longitud.
  - Debe ser una combinación de letras (en mayúsculas y minúsculas), números y caracteres especiales.
  - No elija palabras que se relacionen fácilmente con Ud. como por ejemplo el nombre de algún familiar, mascota, equipo de fútbol, fecha de cumpleaños, número de teléfono, etc.
- No comparta la contraseña. La contraseña debe ser secreta. No la comparta con nadie, ni siquiera con personas de confianza, colegas de trabajo ni administradores de red. Si alguien le exige su contraseña diciendo que es necesaria para dichas tareas, Ud. debe negarse y notificarlo al responsable de TIC.
- Cambie la contraseña de forma periódica. La contraseña debe ser modificada frecuentemente.
- Para evitar los mensajes de correo no deseado, no proporcione su cuenta de correo electrónico para asuntos ajenos a la Universidad como por ejemplo: tiendas comerciales, redes sociales o páginas de entretenimiento.

Buenas prácticas en la recepción de correo

- ***La Universidad Tecnológica Nacional por ningún motivo ni medio pedirá sus datos de acceso de su cuenta de correo.***
- Se recomienda a los usuarios no abrir archivos adjuntos que no hayan solicitado o que se reciban de direcciones de correo desconocidas, debido a que es la principal fuente de difusión de fraudes y virus informáticos.
- En caso de recibir un mensaje de correo sospechoso, verificar con el remitente si es un correo que él realmente envió.
- No visite los sitios web mencionados en mensajes de correo electrónico cuyo remitente sea desconocido. Tenga especial cuidado si el sitio web mencionado en el mensaje recibido le pide que ingrese sus datos personales, sus claves de acceso, sus datos financieros, etc. El sitio podría estar siendo usado por un atacante para robar su identidad, técnica conocida como "phishing".

Buenas prácticas en el envío de correo

- Se sugiere evitar el envío de mensajes de correo no solicitado (cadenas de mensajes), esta actividad puede comprometer su dirección de correo electrónico así como al servicio de e-mail de la Universidad provocando rechazo de los mensajes o que sean catalogados como spam.

"2020 – AÑO DEL GENERAL MANUEL BELGRANO"
"60° Aniversario de la Primera Colación de Grado de la Universidad Tecnológica Nacional"