Departamento de Seguridad Informática
Dirección General de Sistemas

Recomendaciones para el uso apropiado del correo electrónico de la Universidad Nacional de Luján

El correo electrónico institucional es un servicio brindado por la Universidad para contribuir con el desarrollo de las actividades laborales.

Este documento contiene recomendaciones para el uso apropiado del correo electrónico de la Universidad Nacional de Luján, de acuerdo con lo sugerido por normas y estándares nacionales e internacionales para llevar adelante buenas prácticas en el uso de recursos de tecnologías de la información y las comunicaciones.

RECOMENDACIONES SOBRE LA CLAVE DE ACCESO AL CORREO ELECTRÓNICO

1. 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 12 caracteres de longitud.
» Debe ser una combinación de letras (en mayúsculas y minúsculas), números y símbolos de puntuación.
» No elija palabras que se relacionen fácilmente con Ud. como por ejemplo su nombre o número de documento, el nombre de algún familiar, mascota, equipo de fútbol, fecha de cumpleaños, número de teléfono, etc.
» Tampoco deben utilizarse palabras que figuren en el diccionario.

2. No comparta la contraseña

La contraseña debe ser secreta. No la comparta con nadie, ni siquiera con personas de confianza, colegas de trabajo, secretarias ni administradores de red. Los administradores de red no necesitan conocer las contraseñas para realizar tareas administrativas o de mantenimiento. Si alguien le exige su contraseña diciendo que es necesaria para dichas tareas, Ud. debe negarse y notificarlo al responsable del Departamento de Seguridad Informática.

3. Cambie la contraseña de forma periódica

La contraseña debe ser modificada periódicamente.
A tal efecto, puede acceder mediante su navegador web a la interfaz de correo web de la UNLu: https://webmail.unlu.edu.ar/, ingresando su nombre de usuario y clave de acceso de correo electrónico. Una vez dentro del correo, haga clic en el enlace "*Opciones*" del menú superior, y seleccione "*Cambiar contraseña*".
Es conveniente que no utilice la misma contraseña para todos los accesos digitales (por ejemplo, correo electrónico personal, home-banking, correo electrónico institucional, etc).

Si sospecha que su cuenta de correo electrónico está siendo utilizada por un tercero, cambie inmediatamente su clave de acceso y notifique al Departamento de Seguridad Informática de la UNLu al teléfono 02323 42-3171 / 42-3979, interno 1611.

RECOMENDACIONES SOBRE EL ENVÍO DE MENSAJES

1. No envíe información crítica por correo electrónico sin utilizar un sistema de cifrado

El contenido del mensaje puede ser capturado en cualquiera de los equipos informáticos por los que circula el mensaje desde que es enviado hasta que se entrega en el buzón del destinatario. Si debe enviar información crítica por correo electrónico, contacte al Departamento de Seguridad Informática.

2. Siempre revise los mensajes

Antes de enviar un mensaje, cerciórese de que el contenido es adecuado y de que la dirección de destino es la correcta. Si envía archivos adjuntos, asegúrese de que son los correctos y están en su totalidad.

3. No envíe archivos de gran tamaño por correo electrónico

El sistema de correo electrónico está diseñado para el envío y recepción de mensajes y archivos digitales de tamaño no mayor a 5 MB. Si el tamaño del archivo es mayor, divídalo en varios archivos y envíe cada archivo en un mensaje separado. Los mensajes cuyo tamaño exceda del espacio disponible en el buzón de mensajes del destinatario no podrán ser entregados al mismo.

4. Si debe reenviar o "hacer forward" de un correo electrónico:

- » Borre las direcciones de correo de los remitentes, de no hacerlo, estará divulgando las direcciones a todos los destinatarios del mensaje, quienes podrán utilizar dichas direcciones para enviar correo masivo o spam.
- » Copie el contenido del correo original y redacte uno nuevo.
- » Si reenvía a más de una persona, ingrese las direcciones de los destinatarios en el campo Copia Oculta (CCO o BCC) del programa; de no ser así, cada receptor podrá conocer los demás destinatarios que recibieron el mismo mensaje de correo electrónico.

5. No utilice el correo electrónico como medio para difundir ideas políticas, religiosas, propagandas, etc.

RECOMENDACIONES SOBRE LA RECEPCIÓN DE MENSAJES

1. Verifique la autenticidad del remitente del mensaje

Los mensajes de correo electrónico pueden ser falsificados fácilmente. Tenga en cuenta que un atacante podría generar mensajes que parezcan ser originados por algún tercero en el cual Ud. confía. Si se trata de información crítica y el contenido del mensaje despierta alguna sospecha, trate de validar los datos del remitente por otro medio alternativo.

2. Elimine mensajes no esperados o de un remitente desconocido

No conteste ni reenvíe mensajes de correo electrónico que no espera recibir. Si no reconoce el remitente o no esperaba el mensaje, no lo responda, ya que podría estar confirmando a un posible atacante que su cuenta de correo electrónico es válida y se encuentra activa.

3. No abra archivos adjuntos que no está esperando

Muchos virus informáticos utilizan el correo electrónico como medio para propagarse, enviando copias de sí mismos como archivos adjuntos a los contactos que figuran en su libreta de direcciones. Los archivos adjuntos y el software de fuentes no confiables muchas veces contienen código malicioso (virus, troyanos, etc.) que podrían permitir a un atacante robar información de su equipo o afectar el funcionamiento de su computadora.

- » No abra archivos anexados a los mensajes por más que sean de un remitente conocido si no los está esperando. Ante la duda, consulte al remitente si él efectivamente lo envió antes de abrir el adjunto.
- » No abra archivos adjuntos que tengan extensiones ejecutables (.exe, .bat, .pif)

- » No abra archivos adjuntos que tengan más de una extensión (.jpg.exe, .doc.exe), ya que en estos casos, intentan engañar al destinatario a fin de que ejecute el programa adjunto utilizando mensajes sugestivos y pretendiendo ser una archivo de imagen o un documento.
- » Siempre analice los archivos recibidos con un antivirus.

4. No visite los sitios web que figuran en los mensajes

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". Encontrará más información sobre phishing en el documento *Cómo protegerse del phishing*.

5. El software antivirus de su computadora debe mantenerse actualizado

- » Utilice un antivirus reconocido, con la configuración establecida por el Servicio Técnico de la Dirección General de Sistemas.
- » Verifique que el software antivirus instalado en el equipo se encuentra activo y actualizado, ya que periódicamente se descubren nuevas vulnerabilidades y aparecen nuevos virus.
- » Analice siempre los medios removibles (discos, pen-drives, mp3, celulares, cámaras digitales) que se conecten a la computadora.
- » Ejecute un análisis completo del equipo al menos una vez por semana.
- » Respalde periódicamente sus mensajes de correo.
- » Proteja las copias de respaldo con contraseña y no las deje al alcance de terceros.