CIBERSEGURIDAD
Universidad Nacional del Comahue

Seguridad en el Uso del Correo Institucional

Proteger la seguridad del correo institucional de la Universidad Nacional del Comahue es esencial para salvaguardar la información confidencial e institucional. A continuación, te ofrecemos recomendaciones clave para un uso seguro:

- **Contraseña segura:**
  - Usa una contraseña robusta que combine letras mayúsculas, minúsculas, números y caracteres especiales.
  - Cambia tu contraseña de forma regular y no la compartas con nadie.
- **Cuidado con correos electrónicos sospechosos**
  - Evita enlaces y descargas:
    - No hagas clic en enlaces ni descargues archivos adjuntos de remitentes desconocidos o correos no solicitados.
    - Verifica siempre la dirección del remitente antes de responder.
  - Precaución con intentos de phishing:
    - Sé escéptico ante correos que solicitan información confidencial como contraseñas o números de tarjeta de crédito.
    - Nunca proporciones datos personales o sensibles sin verificar la autenticidad del correo.
- **Uso de redes Wi-Fi seguras**
  - Evita acceder al correo institucional a través de redes Wi-Fi públicas no seguras. Si es inevitable, utiliza una conexión VPN para proteger la información.
- **Archivos adjuntos y mensajes sospechosos**
  - Abre archivos adjuntos solo si fueron solicitados. Si provienen de un remitente conocido pero no esperados, confirma su legitimidad mediante otro medio, como una llamada telefónica.
  - Verifica que el nombre del remitente coincida con la dirección de correo electrónico real.
- **Buenas prácticas al enviar correos**
  - Usa copia oculta (CCO): Cuando envíes correos a múltiples destinatarios no relacionados, utiliza el campo de copia oculta para proteger sus direcciones.

    - Cifrado de información sensible: No envíes datos como contraseñas, cuentas bancarias o información confidencial en texto plano. Asegúrate de cifrar los mensajes antes de enviarlos.
    - Destinatarios confiables: Antes de enviar documentos o imágenes sensibles, verifica la legitimidad del destinatario.
- **Gestión de correos no deseados y solicitudes inusuales**
    - Descarta correos no deseados (SPAM) sin abrirlos.
    - Ante solicitudes atípicas o poco comunes, verifica su autenticidad mediante otro canal de comunicación.
    - Si recibes mensajes que soliciten cambiar contraseñas o acceder a sitios web, confirma su veracidad antes de proceder.
- **Denuncia de incidentes de seguridad**
    - Si detectas actividad sospechosa en tu cuenta o sospechas de un incidente de seguridad, informa de inmediato a la unidad de TI correspondiente y a ciberseguridad@central.uncoma.edu.ar.
    - Mensajes extorsivos o intimidatorios deben ser reportados al responsable de sistemas de manera urgente.
- **Prevención ante fraudes y estafas**
    - Desconfía de mensajes que anuncian premios, herencias, donaciones u ofertas sospechosas. Estas suelen ser intentos de estafa.

La ciberseguridad es responsabilidad de todos. Aplicando estas recomendaciones, puedes proteger la información sensible de la Universidad Nacional del Comahue y contribuir a un entorno digital más seguro.