ANÁHUAC CANCÚN

Protocolo de Actuación para Víctimas de Estafas.

En caso de ser víctima de una estafa, actúe rápidamente para minimizar el impacto del incidente y aumentar las posibilidades de recuperar bienes o información comprometida, se recomienda:

1. **Detener toda interacción con el estafador:**

- Suspenda inmediatamente la comunicación con la persona o entidad sospechosa.
- No realice pagos adicionales ni proporcione más información personal o financiera.

2. **Reunir evidencia:**

- **Correos electrónicos**: Conserve el correo original, incluyendo los encabezados.
- **WhatsApp y mensajería**: Capture pantallas de mensajes, números telefónicos y cualquier archivo compartido.
- **Llamadas telefónicas**: Tome nota del número, la fecha, la hora y detalles de la conversación.
- **Pagos realizados**: Si transfirió dinero, reúna comprobantes de pago, números de referencia y detalles bancarios involucrados.

3. **Reportar a las autoridades universitarias.**

- **Jurídico:** Realice una denuncia formal y aporte toda la evidencia recopilada al correo juridico.uac@anahuac.mx
- **Dirección de Tecnología y Transformación Digital**: En caso de haber sido hackeado, contacte al equipo de tecnologías al correo: sistemasuac@anahuac.mx

4. **Proteger su información personal**

- **Cambie contraseñas**: Actualice los datos de acceso de las cuentas comprometidas, usando combinaciones seguras.
- **Monitoree su cuenta bancaria**: Si se ha comprometido información financiera, comuníquese con su banco para vigilar posibles fraudes.
- **Active alertas de seguridad**: Configure notificaciones en sus cuentas bancarias y plataformas de pago para detectar movimientos no autorizados.

5. **Alertar a su red personal o laboral**

- Informe a amigos, familiares y compañeros de trabajo sobre el incidente, especialmente si su información pudo haber sido utilizada para intentar estafar a otros.
- Manténgase informado sobre los métodos de estafa más comunes.
- Solo comparta información personal en plataformas y con personas confiables.
- Instale programas de seguridad en sus dispositivos para proteger sus datos.
- Informe cualquier actividad sospechosa a las autoridades competentes o a la institución involucrada.

Para cualquier consulta o aclaración, puede contactarnos directamente a través de nuestros canales oficiales. Su seguridad es nuestra prioridad.