Comunicado Oficial en caso de Fraude o suplantación de identidad.

Asunto: Recomendaciones para prevenir estafas y proteger su información personal

Con el objetivo de salvaguardar la integridad de nuestras operaciones y la seguridad de toda comunicación oficial, hacemos un llamado a nuestra comunidad para estar alerta frente a posibles intentos de estafa. A continuación, compartimos medidas preventivas específicas según la plataforma utilizada:

1**. Correos electrónicos**

Verifique la dirección del remitente: Asegúrese de que los correos provengan de un dominio oficial (por ejemplo, @anahuac.mx). Desconfíe de direcciones similares pero sospechosas (e.j., @anahuac.co, @annahuac.com)

No comparta información confidencial: Nunca proporcione datos personales, contraseñas o información financiera en respuesta a un correo electrónico.

Confirme con la institución: Antes de realizar cualquier acción solicitada en el correo, confirme su validez directamente con la institución mediante los canales oficiales publicados en su sitio web.

Evite abrir enlaces o archivos adjuntos no solicitados: Los archivos o enlaces maliciosos pueden comprometer su dispositivo o información personal.

2. WhatsApp y otras aplicaciones de mensajería

Verifique la identidad del remitente: Desconfíe de mensajes enviados por números desconocidos, especialmente si incluyen solicitudes de transferencias, datos personales o información confidencial.

Revise la ortografía y redacción: Los mensajes fraudulentos suelen tener errores gramaticales o un tono inusual que no coincide con la comunicación oficial de la institución.

Exija documentación oficial: Ante cualquier solicitud, solicite documentación respaldatoria con sellos y firmas de las autoridades correspondientes.

Desconfíe de ofertas o premios inesperados: Es común que los estafadores utilicen promociones irreales o premios falsos para obtener su información.

3. Llamadas telefónicas

No proporcione datos personales: Si recibe una llamada solicitando información sensible, absténgase de compartirla hasta confirmar la legitimidad de la misma.

Solicite un número oficial para verificar: Pida al interlocutor un número telefónico o extensión para devolver la llamada y confírmelo en la página oficial de la institución.

Desconfíe de llamadas urgentes o amenazas: Los estafadores suelen generar un sentido de urgencia para presionarlo a actuar rápidamente. Mantenga la calma y verifique los hechos antes de responder.

Reporte números sospechosos: Si identifica una llamada sospechosa, repórtela a las autoridades correspondientes o a la institución implicada.

Protocolo de Actuación para Víctimas de Estafas

En caso de haber sido víctima de algún tipo de estafa, es fundamental actuar con rapidez y seguir los pasos que se detallan a continuación. Estas acciones pueden minimizar el impacto del incidente y aumentar las posibilidades de recuperación de bienes o información comprometida.

1. Detener toda interacción con el estafador

Suspenda inmediatamente toda 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 encabezados (puede solicitarlos en su proveedor de correo).

WhatsApp y mensajería: Capture pantallas de los mensajes, números telefónicos, y cualquier archivo compartido.

Llamadas telefónicas: Tome nota del número, la fecha, hora, y detalles relevantes de la conversación.

Pagos realizados: Si transfirió dinero, reúna comprobantes de pago, números de referencia y detalles bancarios involucrados.

3. Reportar a las autoridades

Jurídico: Realice una denuncia formal. Aporte toda la evidencia recopilada al correo jurídico.uac@anahuac.mx.

Sistemas UAC: En caso de haber sido víctima de hackeo, contacte al equipo de sistemas al correo sistemasuac@anahuac.mx

4. Proteger su información personal

Cambie contraseñas: Actualice las contraseñas de las cuentas comprometidas, usando combinaciones seguras.

Monitoree su crédito: En el caso de información financiera comprometida, comuníquese con las agencias de crédito 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.

6. Prevenir futuros incidentes

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.

Recomendaciones generales

1. Mantenga actualizados sus datos de contacto únicamente en los canales oficiales.

2. Active medidas de seguridad en sus cuentas, como la autenticación en dos pasos.

3. Informe inmediatamente 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.