PERIÓDICO	PÁGINA	FECHA	SECCIÓN
LA CRÓNICA DE HOY	12	11/07/2023	NACIONAL

Alertan sobre correos que suplantan la identidad de dependencias de seguridad

Debido a la presencia de correos maliciosos que buscan robar información personal al hacerse pasar por dependencias de seguridad nacional o internacional, la Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México emitió una alerta a la ciudadanía.

Recientemente, se han recibido reportes de personas afectadas por mensajes spam que advierten sobre la presentación de cargos por actividades ilícitas. Estos correos solicitan a los destinatarios que accedan a un enlace o respondan al correo para seguir las supuestas instrucciones de las autoridades.

Unidad de Policía Cibernética.

Con el fin de prevenir este tipo de estafas, la Policía Cibernética brindó las siguientes recomendaciones para evitar abusos por parte de ciberdelincuentes que suplantan la identidad de instituciones legítimas:

- Cambiar regularmente las contraseñas de las cuentas de correo electrónico.
- Evitar compartir la dirección de correo electrónico en sitios web, foros públicos u otros espacios en línea donde los spammers puedan recopilarla fácilmente.
- Utilizar una dirección de correo electrónico secundaria o desechable al registrarse en servicios en línea, suscripciones o formularios que puedan generar spam.
- Mantener actualizado el antivirus o utilizar herramientas antispam proporcionadas por el proveedor de correo electrónico.
- No abrir correos electrónicos de remitentes desconocidos o sospechosos, ni hacer clic en enlaces o descargar archivos adjuntos de dichos correos.
- Marcar como spam o mover a la carpeta de correo no deseado aquellos mensajes que se consideren no deseados, lo que ayudará a entrenar el filtro de correo para que sea más efectivo en el futuro.
- Recordar que la prevención es fundamental para evitar vulnerabilidades a través de correos no deseados.

Es importante tener en cuenta que los correos spam son mensajes no deseados que se envían en grandes cantidades con el objetivo de engañar a las personas. Estos correos pueden incluir supuestas notificaciones de premios en concursos no participados, solicitudes de datos o pagos para liberar supuestos paquetes, entre otros casos.

La prevención y la vigilancia activa son herramientas esenciales para protegerse de las amenazas cibernéticas. • *(Gerardo Mayoral)*