¿Cómo saber si alguien ha entrado en nuestro correo electrónico?

¿Alguna vez has pensado que alguien lee constantemente tu correo personal? ¿Los correos electrónicos no leídos se marcan como leídos y sus amigos reciben correos electrónicos que no has enviado? Soy José Luis Martir Millán **perito informático colegiado** y en este artículo te explicaré qué puede estar sucediendo.

Puede ser que alguien haya entrado en tu buzón de correo y tus datos confidenciales pueden caer rápidamente en las manos equivocadas: los delincuentes de Internet pueden obtener acceso a tus servicios de pago en línea como PayPal; realizar compras a tu nombre, espiar secretos de la empresa o incluso participar en actividades fraudulentas.

Como experto en investigación forense digital sé que los correos electrónicos son admisibles en los tribunales; pero se deben presentar de acuerdo a los requisitos de la ley para que puedan ser admitidos como evidencia en un juicio.

Perito informático: ¿Alguien ha entrado en tu correo electrónico?

Dado que muchos usuarios de Internet solo usan una contraseña para diferentes servicios, un ataque a un sitio web es suficiente para que los ciberdelincuentes obtengan acceso a innumerables cuentas de correo electrónico y cuentas de sitios web. Esto se puede evitar fácilmente utilizando una **contraseña única** y segura **para cada inicio de sesión**.

¿Cómo saber si han vulnerado mi buzón de correo?

Si tus correos electrónicos aparecen en tu bandeja de entrada marcados como leídos, antes de iniciar sesión, es una clara señal de que tu buzón ha sido vulnerado.

Otra señal que te puede indicar que tu correo electrónico ha sido vulnerado es si ves un correo electrónico en tu bandeja de salida que no has enviado.

Cuenta Gmail

Si tu cuenta es Gmail, puedes ver los eventos recientes desde el panel de control. Una vez que inicies sesión en Google selecciona "Mi cuenta". Selecciona las actividades del dispositivo y los eventos de seguridad para revisar y verificar todos tus dispositivos.

Dado que Google rastrea cada inicio de sesión y registra el tipo de dispositivo utilizado, así como la hora y la ubicación de conexión, podrás chequear si todo está normal y en orden.

Cuenta Outlook Web Access

En caso de tener cuenta Outlook web Access, puedes proceder de manera similar a lo que he indicado para la cuenta Gmail. Para ello, inicia sesión en la página de tu cuenta de Microsoft. Ve a la opción correspondiente a la pestaña de seguridad y selecciona ver actividad reciente. Nuevamente verifica tu clave y comprueba si todo está en orden

Microsoft también rastrea cada inicio de sesión y registra todos los dispositivos utilizados, además, muestra la ubicación y la hora de cada registro.

Qué puedo hacer cuando alguien irrumpe en mi buzón

Si alguien irrumpe en tu buzón, debes actuar de inmediato, ya que cualquier retraso puede afectar seriamente tu vida online. Dependiendo de los correos electrónicos involucrados y de cómo se utilicen, tu reputación puede sufrir daños importantes.

Debes cambiar tu clave, activar la autenticación de dos factores, asegurarte de disponer de software de seguridad actualizado, y luego notificar a tu lista de contactos lo que ha pasado.

Cambia tu clave

Cambia la clave de la cuenta de correo electrónico afectada y usa una contraseña única e independiente para cada cuenta. La nueva clave debe ser notablemente diferente de la anterior y no tener cadenas de caracteres o números repetidos.

Si la contraseña ya ha sido cambiada por personas no autorizadas, puedes obtener acceso a tu cuenta con la mayoría de los proveedores de correo respondiendo una o más preguntas de seguridad.

También, cambia las contraseñas de todos los servicios en línea que están vinculados a la dirección de correo electrónico pirateada.

Activa la autenticación de dos factores

Utilizar la autenticación de dos factores para tus cuentas más importantes te permite protegerte de este tipo de ataques. Este es un sistema de seguridad doble que requiere un código numérico separado además de una contraseña para iniciar sesión.

Esto generalmente se envía al destinatario autorizado a través de SMS. Un dispositivo solo se puede autenticar para usar la cuenta con una contraseña y un código.

Los piratas informáticos, por otro lado, solo pueden robar la contraseña, pero no el código asociado. Cada vez más proveedores de correo y portales web ofrecen opciones similares para la autenticación de dos factores en la configuración de la cuenta.

Contratar un perito informático WhatsApp en España

Utiliza software de seguridad confiable y actualizado

Escanea y elimina cualquier software sospechoso y reinicia tu ordenador. Si la contraseña ha sido descubierta y la cuenta de correo electrónico pirateada, el malware también podría leer la

contraseña cambiada. Si el escaneo muestra un resultado, asegúrate de cambiar la contraseña nuevamente después de eliminar el malware.

Informa a tus contactos

Envía un correo electrónico rápido que permita saber a tus amigos que podrían haber recibido un enlace malicioso o una súplica falsa de ayuda para evitar que envíen dinero que no recuperarán o que instalen malware en sus ordenadores.

Perito informático en España: Correo electrónico como prueba digital

En España se acepta el correo electrónico como prueba digital y es admisible como evidencia en un tribunal si al igual que cualquier otra evidencia se comprueba la confiabilidad, integridad y/o autenticidad de la prueba electrónica.

Por lo tanto, durante el **peritaje informático** de correo electrónico se debe cumplir con la cadena de custodia y demostrar que la prueba se obtuvo y almacenó de acuerdo con las buenas prácticas de la **investigación forense**.

Además, para asegurarse de que la evidencia no haya sido alterada entre el momento de la extracción y almacenamiento y el momento de su presentación ante el tribunal, se pueden utilizar herramientas de encriptación que brindan una característica llamada HASH, de modo que; a través de caracteres relativamente cortos, se pueda mostrar que el expediente depositado es idéntico al expediente presentado como prueba en el juicio.

¿Cómo se autentican los correos electrónicos?

Hay muchas rutas para autenticar correos electrónicos. Puede ser tan fácil como hacer que el testigo que recibió el correo electrónico testifique que recibió el correo electrónico impreso. Los correos electrónicos también suelen mostrar la fuente, por lo que la autenticación se puede realizar con el código fuente.

Cuando no se dispone de pruebas directas para establecer la autenticidad de un correo electrónico, se pueden utilizar pruebas circunstanciales.

Ejemplos de evidencia circunstancial que puede ser utilizada por el tribunal para autenticar correos electrónicos incluyen la dirección IP del remitente, el contenido del correo electrónico; es decir, ¿contienen información que solo el presunto remitente poseería?

También se puede hacer uso de nombres o apodos, y cualquier otro factor de identificación que pueda vincular una dirección de correo electrónico a una determinada persona como su remitente o autor.

Finalmente, si ha sido víctima de un ataque pirata informático o desea realizar un **peritaje informático** de correo electrónico, puede comunicarse conmigo a través de: lluis@peritinformatic.com y www.peritinformatic.com. **Soy perito informático titulado, con amplia experiencia en el campo de la investigación forense digital.**