¿Qué hacer para que no te hackeen?

Guía de Prevención

LEX SUITE CONSULTING
PRIVACIDAD

Saber si has sido hackeado puede no ser inmediato, pero hay ciertos indicadores y señales que pueden sugerir una compromiso de tus dispositivos o cuentas.

Signos y síntomas a tener en cuenta

Comportamiento inusual de la computadora o dispositivo: Si tu ordenador comienza a funcionar lentamente, muestra mensajes de error inesperados, se reinicia sin motivo aparente o ejecuta programas que tú no iniciaste, podría ser una señal.

Cuentas de correo o redes sociales comprometidas: Si recibes notificaciones de cambios que no has realizado (como cambios de contraseña), o si amigos y contactos reciben mensajes extraños provenientes de tu cuenta, es posible que hayas sido hackeado.

Transacciones no autorizadas: Si observas cargos no reconocidos en tus tarjetas de crédito o débito, o cambios inexplicables en tus cuentas bancarias, es crucial actuar rápidamente.

Contraseñas que ya no funcionan: Si de repente no puedes acceder a alguna de tus cuentas y estás seguro de que la contraseña es correcta, puede que alguien haya cambiado tu contraseña.

Software o aplicaciones no autorizadas: Si notas programas o aplicaciones en tu dispositivo que no recuerdas haber instalado, puede ser una señal de un malware o de un acceso no autorizado.

Desaparición o alteración de archivos. Si archivos desaparecen, se mueven sin razón o se modifican sin tu intervención, podría ser una señal.

Aumento del uso de datos. Un aumento inesperado en el uso de datos podría indicar actividades maliciosas en segundo plano.

Navegadores web que actúan de forma extraña: Si tu página de inicio cambia sin tu consentimiento, o aparecen barras de herramientas que no instalaste, podrías estar ante un caso de software malicioso.

Redireccionamientos no deseados: Algunos tipos de malware redirigen el tráfico de tu navegador web a sitios web no deseados o muestran anuncios no solicitados.

Notificaciones de servicios de protección de identidad: Si cuentas con un servicio de monitoreo de crédito o protección de identidad y recibes una alerta sobre actividad sospechosa, es posible que hayas sido comprometido.

Notificaciones de acceso desde ubicaciones inusuales: Muchos servicios en línea notifican o bloquean intentos de inicio de sesión desde ubicaciones geográficas inusuales.

Uso inusual de la CPU: Un aumento inesperado en el uso del procesador puede indicar que tu dispositivo ha sido comprometido y está siendo utilizado para actividades malintencionadas, como la minería de criptomonedas.

Más signos de haber sido hackeado

Micrófono o cámara activados sin permiso: Si notas que la cámara o el micrófono de tu dispositivo se activan sin que tú lo hayas permitido, podría ser un signo de que alguien ha ganado acceso a tu dispositivo.

Mensajes SMS o correos enviados sin tu conocimiento: Si aparecen mensajes en tus registros que tú no enviaste, es posible que alguien haya comprometido tu dispositivo.

Configuraciones alteradas: Cambios en la configuración de tu dispositivo o aplicaciones que no recuerdas haber hecho pueden ser una señal de actividad maliciosa.

Actividad en la red sospechosa: Un monitoreo inusual de la actividad de red o conexiones a direcciones IP desconocidas puede ser indicativo de un compromiso.

Alertas de seguridad de diferentes plataformas: Algunas plataformas te notificarán si se ha iniciado sesión en tu cuenta desde un nuevo dispositivo o ubicación.

¿Qué debemos hacer si sospechamos que hemos sido hackeados?

CIBERCOMPLIANCE

www.lexsuite.es

Cambia tus contraseñas inmediatamente, empezando por las cuentas más críticas (correo electrónico, banca en línea, etc.).

Realiza un análisis completo con software antivirus y antimalware actualizado.

Considera restaurar tu sistema a un punto anterior, especialmente si es evidente que hay malware.

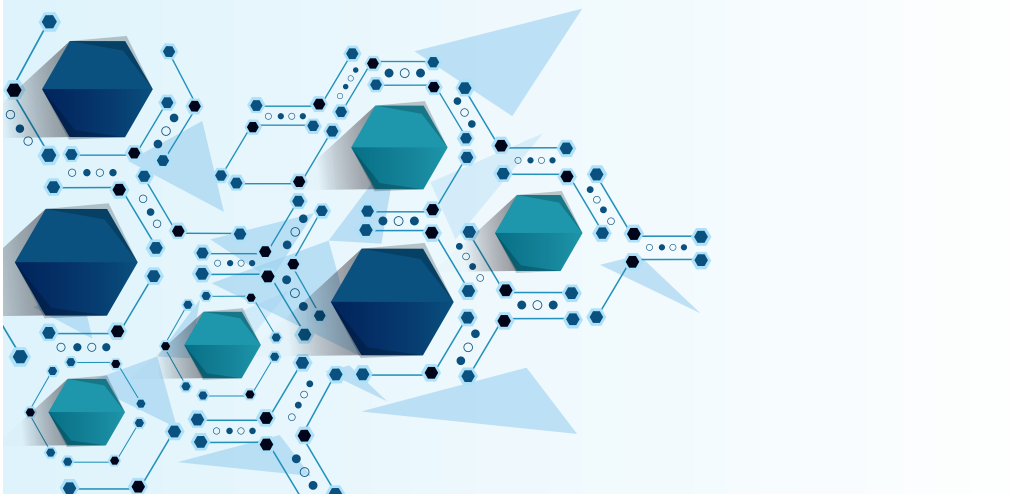
Desconectar de la red: Si sospechas que tu dispositivo ha sido comprometido, desconéctalo de la red (Wi-Fi, datos móviles). Esto puede prevenir la transferencia de datos adicionales al atacante o evitar más daños.

Verifica tus aplicaciones: Si notas aplicaciones que no reconoces, es posible que se hayan instalado sin tu consentimiento. Desinstala cualquier aplicación sospechosa.

Revisa registros y logs: Si tienes habilidades técnicas o conoces a alguien que las tenga, revisar los registros del sistema puede revelar actividad sospechosa.

Asegura otros dispositivos: Si uno de tus dispositivos ha sido comprometido, otros podrían estar en riesgo. Cambia contraseñas y verifica la integridad de otros dispositivos en tu red.

Activa alertas: Activa notificaciones para actividad inusual en tus cuentas. Muchos servicios ofrecen notificaciones por SMS o correo electrónico para cambios de contraseña, inicios de sesión desde dispositivos desconocidos, etc.



Verifica la seguridad de tus respuestas de seguridad: A menudo, las respuestas a preguntas de seguridad pueden ser encontradas o adivinadas a través de la información en redes sociales. Considera usar respuestas ficticias que solo tú conozcas.

Notifica a las instituciones pertinentes, como bancos, si crees que tus cuentas financieras pueden estar comprometidas.

Mantente alerta a correos o llamadas fraudulentas que se aprovechen de la situación.

La prevención es la mejor defensa.

Mantén tus sistemas actualizados, utiliza software de seguridad confiable y mantente informado sobre las últimas amenazas y tácticas de phishing.

La premisa "la prevención es la mejor defensa" es fundamental en el ámbito de la ciberseguridad.

Veamos algunas razones por las cuales la prevención es crucial:

Costos y daños reducidos: Prevenir un ataque cibernético es generalmente más económico y menos perjudicial que recuperarse de uno. Las brechas de seguridad pueden tener consecuencias financieras significativas, que van desde pérdida de datos hasta daño a la reputación.

Tiempo y recursos ahorrados: La recuperación de un ataque cibernético puede llevar mucho tiempo y esfuerzo. La prevención eficaz puede evitar la interrupción del negocio y permitir que los recursos se centren en actividades críticas en lugar de en la respuesta a incidentes.

Protección de la reputación: Una violación de seguridad puede dañar la reputación de una empresa, lo que a su vez puede afectar la confianza de los clientes y socios comerciales. La prevención ayuda a mantener la confianza y la credibilidad de la organización.

Cumplimiento normativo: Muchas industrias tienen regulaciones estrictas sobre la seguridad de la información. La prevención proactiva ayuda a cumplir con estos requisitos y evita posibles sanciones y multas.

Concientización y cultura de seguridad: La prevención implica la creación de una cultura de seguridad en la que todos los empleados entiendan los riesgos cibernéticos y jueguen un papel activo en la protección de la información.

Adaptabilidad a nuevas amenazas: La ciberseguridad es una carrera armamentista constante entre defensores y atacantes. Adoptar una mentalidad preventiva significa estar al tanto de las últimas amenazas y tomar medidas proactivas para mitigarlas antes de que se conviertan en problemas.

Enfoque integral: La prevención no se trata solo de tecnología. También implica aspectos como la capacitación de empleados, la implementación de políticas de seguridad, la actualización constante de sistemas y la realización de auditorías de seguridad.

INFORMACIÓN OFRECIDA POR

LEX SUITE CONSULTING
PRIVACIDAD Y PROTECCIÓN DE DATOS