www.mexis.net

AL FINAL LO HARÁS: CINCO TRUCOS DE SEGURIDAD GRATUITOS Y A PRUEBA DE TONTOS QUE ME SALVAN LA ESPALDA

mexis aggity

“¿Por qué haría clic en ese enlace, idiota?” He escuchado frases similares e incluso me las he dicho a mí mismo demasiadas veces. Sin embargo, he tenido la suerte de tener un colchón de seguridad. Tú también puedes tenerlo.

Seamos realistas. Los sofisticados piratas informáticos estatales rusos o chinos con malware avanzado y meses de vigilancia no están detrás de ti. No desperdiciarían costosas vulnerabilidades de día cero para secuestrar tu cuenta de Instagram o comprar una tarjeta de regalo de Amazon con tu dinero.

¿Qué es más probable? Que aparezca algo inesperado en Internet. Encontrarás un anuncio con una oferta increíble. Un código QR con una oferta tentadora. Un enlace en un correo electrónico o mensaje SMS que ofrece un nuevo trabajo o una oportunidad de inversión. O será aterrador y te avisará de que tu computadora está infectada. Y de vez en cuando, harás clic.

Yo también lo hice. **Una vez recibí un correo electrónico relacionado con el trabajo de estafadores que se hacían pasar por consultores de relaciones públicas y que les presentaban una historia.** Los periodistas reciben cientos de correos electrónicos similares, todos parecen similares. A veces, cuando el correo electrónico de phishing está muy bien elaborado, puede pasar desapercibido para uno mismo. ¿Qué pasó después?

“No se puede acceder a este sitio”, se encogió de hombros el navegador. **“ERR_CONEXIÓN_RECHAZADA”** Como en el modelo del queso suizo , cada capa de defensa tiene agujeros. Incluso mi conciencia. Pero si se añaden capas adicionales, las posibilidades de que el ataque tenga éxito disminuyen exponencialmente. Yo estaba a salvo porque tenía algunas lonchas de queso preparadas con antelación.

Supongo que tienes algunas capas de protección, como contraseñas seguras y únicas y autenticación multifactor (MFA) o claves de acceso. Si no las tienes, empieza por aquí. Este artículo se centra en lo que ocurre antes de que la MFA tenga que protegerte.

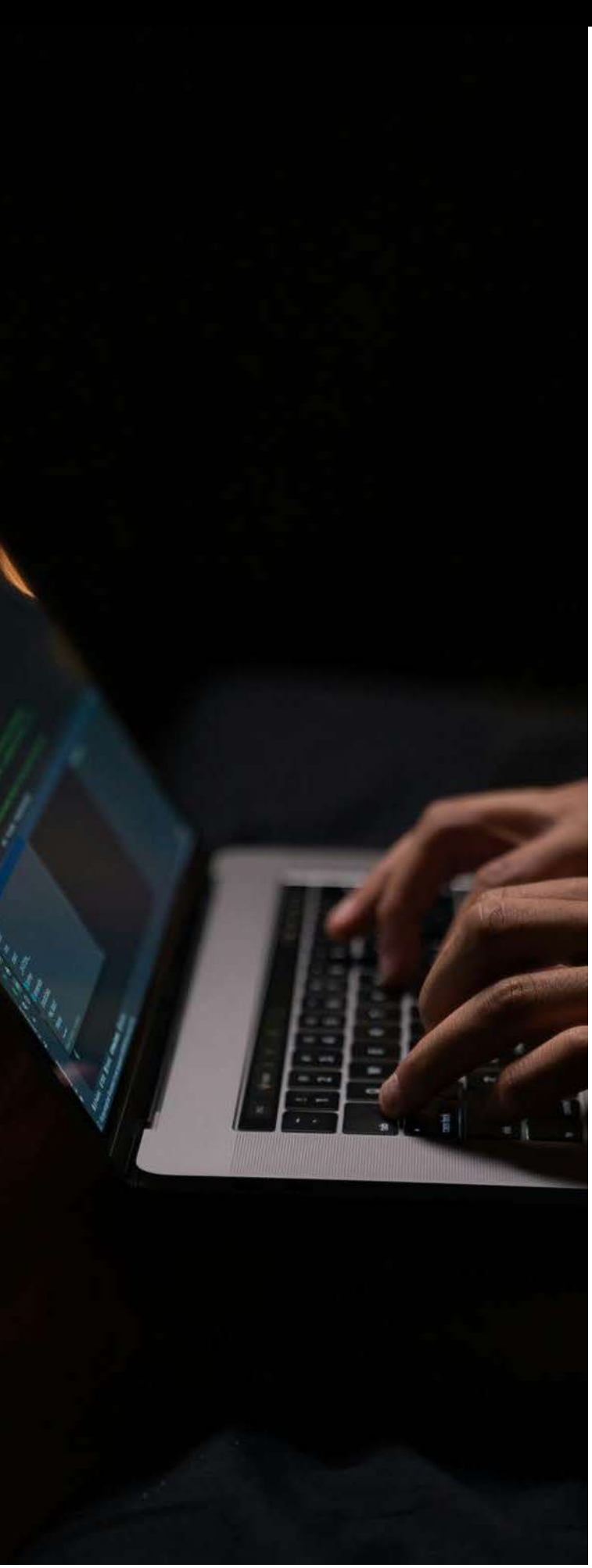
Es posible que MFA sea una de las últimas rebanadas de queso suizo que intentan proteger sus cuentas de los piratas informáticos, pero no querrá acercarse a esa situación.

1. No puedes hacer clic en un enlace malicioso si no lo recibes: utiliza un bloqueador de anuncios

Los bloqueadores de anuncios no solo sirven para mejorar la experiencia de navegación, sino que también son una herramienta de seguridad fundamental. Los piratas informáticos suelen comprar anuncios en Google, Meta y otras plataformas para distribuir malware. Suplantan marcas y disfrazan enlaces maliciosos para que no se distingan de los auténticos. **Hasta que el mercado publicitario pueda garantizar la seguridad de forma adecuada, es mejor no exponerse a riesgos.** Los sitios maliciosos pueden contener scripts que los bloqueadores de anuncios pueden bloquear de forma eficaz.

Las estafas son un juego de números, y la defensa contra ellas también funciona de manera similar. **Cuantos menos enlaces maliciosos obtengas y veas, menos probabilidades habrá de que suceda algo malo.**

Por eso, para mí el bloqueador de publicidad uBlock Origin es esencial. Incluso cambié de Chrome a Firefox solo para seguir usándolo . Si por alguna razón no te gusta este bloqueador de publicidad, usa una alternativa que funcione para ti. Prueba AdGuard, AdBlock Plus u otros.



¿No confías en mí? Confía en el FBI.

“Utilice una extensión bloqueadora de anuncios cuando realice búsquedas en Internet. La mayoría de los navegadores de Internet permiten al usuario agregar extensiones, incluidas extensiones que bloquean anuncios. Estos bloqueadores de anuncios se pueden activar y desactivar dentro de un navegador para permitir anuncios en ciertos sitios web mientras bloquean anuncios en otros”, dijo el FBI en 2022.

¿Aún no estás convencido? La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos también **recomienda el uso de bloqueadores de anuncios debido a los siguientes beneficios:**

- **Reduce el riesgo de publicidad maliciosa** o redireccionamientos a sitios maliciosos o de phishing.
- **Mejora el rendimiento del lado del cliente** y una carga de páginas más rápida.
- **Reduce el riesgo de recopilación de datos** por parte de terceros

Sin embargo, el trozo de queso del bloqueador de publicidad no está exento de agujeros y también es bastante pequeño: no cubre toda su vida digital, que ahora se ha ampliado a las aplicaciones de teléfonos inteligentes, el correo electrónico, las llamadas, etc.

Aunque la mayoría de los proveedores de correo electrónico filtran los mensajes de correo no deseado, los estafadores suelen encontrar la manera de evitarlos. Si eres usuario de Windows, considera el cliente de correo electrónico Thunderbird y configura los ajustes para que todos los mensajes de correo electrónico se muestren en texto sin formato en lugar de HTML. Si bien esto mejora significativamente la seguridad, reducirá un poco el atractivo visual de la mayoría de los boletines informativos.

En iOS, no encontré un cliente de correo que permita desactivar los enlaces activos. Por lo tanto, me quedo con la aplicación de correo predeterminada. Sin embargo, bloqueo todo el contenido remoto. **Esto no te protegerá de dejar enlaces activos, pero será más difícil para los remitentes de spam y los anunciantes rastrearte** y engañarte para que hagas clic en algo no deseado.

Para habilitar esta función en tu iPhone, ve a Ajustes, luego Aplicaciones, selecciona Correo y luego Protección de privacidad. **Desactiva la opción Proteger actividad de correo y elige las opciones Ocultar dirección IP y Bloquear todo el contenido remoto.**

Gmail también tiene una opción en la configuración general para preguntar antes de mostrar imágenes externas: selecciónela para deshabilitar el correo electrónico dinámico.

Ahora bien, **para reducir las posibilidades de recibir llamadas de estafadores, utilizo principalmente la aplicación Signal para comunicarme.** Aquí nunca recibo spam ni "invitaciones" extrañas, pero eso puede cambiar.

He desactivado la funcionalidad MMS.

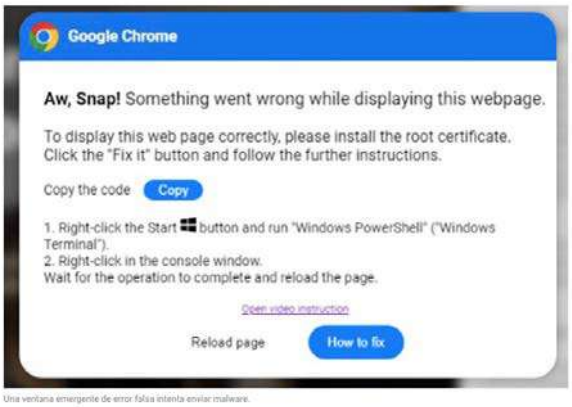
En los teléfonos Samsung, los usuarios tienen un filtro o bloqueo de llamadas fraudulentas o spam de forma predeterminada, proporcionado por Hiya. Quería mantener esta funcionalidad en iOS, por lo que utilizo la funcionalidad básica de la aplicación Hiya de forma gratuita. Como alternativa, existen otras aplicaciones, como Truecaller; es posible que quieras probarlas.

2. Si haces clic en él, estarás seguro siempre y cuando no se cargue.

Tal vez hayas escaneado un código QR o hayas hecho clic en una URL acortada que no se ha filtrado a tu bloqueador de publicidad o a tu sistema de seguridad de correo electrónico. ¿Cuál es tu próxima línea de defensa?
Filtra el tráfico de Internet. No quieres que llegue "cualquier agua" a casa, sino que te llegue limpia. Lo mismo ocurre con la navegación web.

¿Sitios web maliciosos conocidos? No, gracias. ¿URL mal escritas? No debería cargarse. ¿Páginas web recién registradas sin historial? Es probable que sean maliciosas. ¿Por qué las necesitaría? ¿Sitios web gratuitos y dudosos en plataformas populares o dominios estacionados que nadie usa? Bloquéelos también. Y también, bloquee millones de dominios en listas de bloqueo seleccionadas que ofrecen anuncios, rastreadores, contenido malicioso o no deseado.

El DNS privado es un servicio increíble que me ha salvado de cargar sitios web maliciosos muchas veces. Es mucho más conveniente que configurar tu propio sumidero de DNS (Pi-Hole).



Una ventana emergente de error falsa intenta enviar malware.

Hay pocos para elegir, pero soy fan de NextDNS, porque es sencillo y gratuito para hasta 300.000 consultas al mes, lo cual es más que suficiente para mí.
Creé un perfil, habilité la mayoría de los filtros y configuraciones, seguí las guías de configuración para todos mis dispositivos y listo. **Cubre todos los dispositivos, aplicaciones y tráfico de Internet,** por lo que esta porción de queso es mucho más amplia. Esta herramienta filtrará la mayor parte del tráfico malicioso. Si hace clic en un enlace malicioso, no se cargará en la mayoría de los casos. Incluso usé la herramienta para rastrear lo que hacen mis aplicaciones mientras duermo .

Puede que necesites algo de tiempo para adaptarte. Si eliges una configuración demasiado estricta, **es posible que algunas páginas no se carguen o no funcionen correctamente.** Algunos filtros bloquearán sitios para adultos, sitios de apuestas y servidores de juegos, y si necesitas acceder a uno en particular, es posible que tengas que agregarlo a la lista de permitidos o revisar qué listas de bloqueados son relevantes para ti.

3. Si hace clic y se carga la URL, ¿qué pasa?

La mayoría de las recomendaciones de higiene en materia de ciberseguridad cubren esta etapa de un ataque. **Mantener el software actualizado lo protegerá de la explotación de vulnerabilidades conocidas.** Puede considerar reducir los privilegios de su cuenta solo para asegurarse de que necesita ingresar una contraseña de administrador cada vez que se deba instalar una aplicación.

Los antivirus y otros programas de protección de terminales (el gratuito Windows Defender también es una buena opción) son otra opción que puede evitar la ejecución de malware. Si te quedas con las aplicaciones oficiales y eliminas las que ya no usas, **también reducirás la superficie de ataque potencial.**

Este es un truco que uso todos los días: en lugar de una aplicación, elijo un servicio web. **Siempre que necesito consultar X (Twitter), Facebook, YouTube o cualquier servicio, accedo a él desde el navegador web.** De esta manera, no solo se necesitan menos aplicaciones, sino que el navegador agrega una capa adicional conocida como **"aislamiento del navegador", que limita el acceso de los servicios web a su equipo.**

Recibes menos notificaciones, que también se han utilizado de forma abusiva para enviar contenido malicioso. La excepción son las aplicaciones bancarias legítimas, que podrían ofrecer funciones de seguridad aún mejores.

4. Si se ejecuta el malware, es mejor tener esa MFA activada

Si un malware se infiltra en su dispositivo, la situación cambia. Debe asumir que los atacantes han extraído información de su sistema y que **ya no se trata de prevenir, sino de controlar los daños.**

El cifrado, las copias de seguridad y la MFA son sus mejores amigos en estos casos, pero todos ellos deben prepararse con antelación. **Es posible que los piratas informáticos hayan obtenido su dirección de correo electrónico e información del sistema,** pero aún no podrán acceder a sus cuentas si las credenciales están encriptadas y la autenticación multifactor (MFA) está habilitada.

Las claves de acceso son el nuevo tipo de autenticación multifactor (MFA) poco utilizada y resistente al phishing que resulta muy difícil de eludir para los atacantes, ya que dependen del cifrado de hardware. Siempre que me ofrecen la opción de configurarlas, **elijo las claves de acceso en lugar de otros métodos de autenticación.** Para las cuentas en las que no hay claves de acceso disponibles, me quedo con las aplicaciones de autenticación como una alternativa sólida.

5. La última línea de defensa es tu banco

Nunca estuve cerca de esto, pero incluso en caso de que los atacantes encontraran una forma de acceder a la información de mi tarjeta de pago y a mi cuenta bancaria, tengo una última estrategia de seguridad.

Nunca guardo mucho dinero en cuentas vinculadas a ningún tipo de tarjeta de crédito o de pago. Los certificados de depósito y las cuentas de ahorro sin vínculo a una tarjeta ofrecen una barrera adicional que los atacantes deben superar: no pueden simplemente transferir o gastar el dinero. Tendrían que cancelar el depósito antes de transferir el dinero a otra cuenta, lo que es un paso adicional. **Los límites diarios y mensuales estrictos evitarán que se robe todo el dinero de una sola vez.**

Para la seguridad de los pagos, **recurro a tarjetas virtuales de un solo uso siempre que sea posible.** Muchas empresas de tecnología financiera ofrecen servicios similares. Por lo tanto, cualquier tarjeta que pueda verse comprometida tiene un valor limitado.

Por supuesto, el error humano sigue siendo la mayor vulnerabilidad. Ningún banco ni herramienta puede proteger por completo a alguien que compra voluntariamente tarjetas de regalo para estafadores o envía dinero a estafadores románticos o de inversión. **También es importante tener a alguien con quien hablar antes de tomar decisiones importantes.**

Las capas adicionales de defensa nunca son 100 % efectivas, pero crean barreras y pueden detener muchos ataques antes de que causen daño. Es posible que la llamada maliciosa se bloquee, la URL no se cargue, el malware no pueda explotar una aplicación vulnerable o acceder al centro de comando y control, o el atacante no pueda eludir su autenticación multifactor.

Estas son solo mis preferencias personales. ¿Has desarrollado una mejor estrategia para protegerte? Compártela con otros.

Fuente de información: cybernews.com