

OUCH!

El Boletín Mensual de Concientización en Seguridad para TI

Detrás de las sombras: cómo los cibercriminales roban tus contraseñas

Una pesadilla digital: La exposición no deseada de Lisa

Lisa, una diseñadora gráfica con un don para la creatividad, vivió gran parte de su vida en línea. Ella gestionaba su banco, compras e interacciones sociales a través de varias aplicaciones y sitios web. Un día, notó algunos retiros extraños de su cuenta bancaria: artículos que nunca había comprado en tiendas que nunca había visitado. Sus cuentas de redes sociales comenzaron a publicar mensajes de spam que promocionaban productos y servicios extraños, y sus amigos reportaron haber recibido correos electrónicos inusuales de ella.

El pánico se apoderó de Lisa cuando se dio cuenta de que había perdido el control de su identidad digital. Sus fotos personales se filtraron y sus conversaciones privadas quedaron expuestas. Sus clientes comenzaron a cuestionar su confiabilidad y su reputación se vio afectada. Después de consultar con expertos en ciberseguridad, Lisa descubrió que sus contraseñas habían sido comprometidas. Cibercriminales habían obtenido acceso a sus cuentas más importantes, deshaciendo su mundo digital pieza por pieza. La pregunta seguía: ¿Cómo pasó esto?

Las tácticas encubiertas de los cibercriminales: cinco métodos comunes

Los actores de amenazas utilizan una variedad de técnicas para obtener contraseñas. Te compartimos cinco formas habituales en las que podrían obtener las tuyas, como lo hicieron con las de Lisa:

1. Ataques de ingeniería social

La ingeniería social es cuando los atacantes se hacen pasar por alguien o algo que conoces o en quien confías, con el fin de engañarte para que realices acciones que no deberías. Envían correos electrónicos o mensajes que parecen legítimos, lo que suele generar una fuerte sensación de urgencia, miedo o curiosidad.

Cómo pasó: Lisa recibió un correo electrónico que parecía ser de su banco, con logotipos y la marca oficial. El correo afirmaba que había actividad sospechosa en su cuenta y la instaba a hacer clic en un enlace para verificar su identidad. El enlace la llevó a un sitio web falso que capturó sus credenciales de inicio de sesión cuando las ingresó.

2. Malware

Son programas maliciosos diseñados para infectar computadoras. Una vez infectadas, los cibercriminales pueden hacer lo que quieran. Los keyloggers (a veces llamados *ladrones de información*) son un tipo de malware que registran cada pulsación de tecla realizada en un dispositivo, incluidos los usuarios, las contraseñas e información sensible.

Cómo pasó: Lisa descargó lo que pensó que era una tipografía legítima para su trabajo de diseño. En su interior se ocultaba un keylogger que se instalaba automáticamente en su computadora. Con el tiempo, registró sus datos de inicio de sesión para varias cuentas y se los envió al atacante.

3. Ataques de fuerza bruta

En los ataques de fuerza bruta los cibercriminales usan herramientas automatizadas para intentar varias combinaciones de contraseñas hasta que obtengan la correcta. Las contraseñas débiles son especialmente vulnerables a este método.

Cómo pasó: Lisa usó contraseñas simples como “lisa2020” para muchas de sus cuentas. Los atacantes usaron programas que probaban sistemáticamente contraseñas comunes y fácilmente vulneraron sus cuentas.

4. Fuga de datos

Cuando una página de Internet o servicio se ve comprometido puede afectar a todas las cuentas que se encuentren almacenadas en el servidor. Si alguien utiliza la misma contraseña para varias cuentas, cuando esa contraseña se ve comprometida para alguna entonces esa misma contraseña puede ser usada para acceder a las demás cuentas de la víctima también.

Cómo pasó: Una red social popular que Lisa usaba sufrió una fuga de datos. Como ella utilizaba la misma contraseña en otros sitios, los atacantes accedieron a sus demás cuentas usando las credenciales filtradas.

5. Credenciales compradas

Los cibercriminales pueden simplemente comprar tus contraseñas en Internet, frecuentemente en la Dark Web. Algunos actores de amenaza se especializan en robar contraseñas de sus víctimas, utilizando cualquiera de los métodos mencionados al momento. Ellos guardan y venden las contraseñas robadas a otros cibercriminales.

Cómo pasó: Un cibercriminal decidió que quería hacer tanto dinero como fuera posible el fin de semana, entonces entró a la Dark Web y compró alrededor de 100,000 cuentas comprometidas con sus contraseñas completas. Una de las cuentas de Lisa estaba en esa lista.

Tres pasos clave que puedes tomar

Afortunadamente, al tomar estos simples tres pasos puedes hacer mucho para proteger tus cuentas y tu vida digital en línea.

1. Utiliza una contraseña larga y única para cada una de tus cuentas. Te recomendamos utilizar frases de contraseña, que son contraseñas largas compuestas de varias palabras.
2. Utiliza un gestor de contraseñas para almacenar y administrar de forma segura todas esas contraseñas por ti.
3. Habilita la autenticación multifactor (MFA) siempre que sea posible para tus cuentas en línea más importantes.

Editora invitada

Lekshmi Nair es líder senior en ciberseguridad, con 22 años de amplia experiencia en consultoría de seguridad de la información y estrategia de ciberseguridad. Actualmente es directora senior de consultoría de seguridad de aplicaciones en BlackDuck Software. Es la fundadora y presidenta de WiCyS India.



Recursos

Voces fantasma: Defiéndete de los ataques de clonación de voz: <https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/>

Ataques de mensajes de texto: una saga de smishing: <https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/>

Las 3 principales formas en que los ciberatacantes te convierten en su objetivo: <https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/>

El poder de las frases de contraseña: <https://www.sans.org/newsletters/ouch/power-passphrase/>

El poder de los gestores de contraseñas: <https://www.sans.org/newsletters/ouch/power-password-managers/>

Traducido a la comunidad por: Cécica Martínez Aponte (SSAP) e Ivan Galindo.

OUCH! Es publicado por SANS Security Awareness y distribuido bajo la [licencia Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Eres libre de compartir o distribuir este boletín, siempre y cuando no lo vendas o modifiques. Comité editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.