
Boletín mensual de concientización en seguridad para ti

# Dark Web

## Resumen

Seguramente alguna vez has escuchado a otras personas o en los medios usar el término “Dark Web”, y te has preguntado “*¿qué es eso de Dark Web?*” o “*¿Acaso debería estar haciendo algo al respecto?*”. En este artículo explicaremos que es la Dark Web y qué significa.

## ¿Qué es?

La Dark Web consiste en sistemas en Internet diseñados para comunicarse o compartir información de forma segura y anónima. No existe algo como una Dark Web única, por lo que no es como Facebook que pertenece a una sola organización. En realidad, la Dark Web son colecciones de diferentes sistemas y redes administradas por muchas personas, los cuales son usados para diferentes propósitos. Estos sistemas forman parte de Internet y se encuentran conectados a la misma, aunque generalmente no los encontrarás usando motores de búsqueda normales, por lo regular se necesita un software especial para poder encontrarlos. Un ejemplo de este tipo de software es el proyecto TOR (The Onion Ring) en el cual para poder acceder a esta Dark Web se necesita descargar el navegador TOR (Tor Browser). Cuando te conectas a los servidores web utilizando este navegador, el tráfico viaja cifrado a través de otros equipos que también usan TOR y al ir saltando entre diferentes computadoras la dirección IP de origen va cambiando, lo que significa que en el momento en el que el navegador alcanza el sitio web la actividad en línea es anónima. Otros ejemplos de Dark Web pueden ser Zeronet, Freenet y I2P.

## ¿Quién usa la Dark Web?

Los criminales cibernéticos son un grupo grande de usuarios de la Dark Web. Ellos mantienen sitios web y foros para llevar a cabo sus actividades criminales como la venta de estupefacientes o de gigabytes de datos robados haciéndolo de forma anónima y segura. Por ejemplo, cuando un criminal cibernético hackea un banco o un sitio de venta en línea roba tanta información como le es posible para después vender esa información a otros criminales en sitios de la Dark Web.

Sin embargo, también existen usuarios válidos en esta red. Por ejemplo, en países donde se presenta la censura de forma extensa se puede usar la Dark Web para compartir información y ver qué sucede fuera de dichos países mientras se protege la privacidad y se mantiene el anonimato. Periodistas, informantes y personas preocupadas por su privacidad pueden usar la Dark Web para incrementar el anonimato y evitar la censura. Adicionalmente, las personas que usan tecnologías similares al navegador TOR, pueden usarlas no solo para acceder a la Dark Web, sino también navegar anónimamente en el Internet común.

## ¿Qué debería de hacer?

A menos que no tengas una razón específica para acceder a la Dark Web, te recomendamos no hacerlo. Algunos sitios dentro de la Dark Web son usados para propósitos ilegales, muchos de estos sitios usarán tu equipo en una red de pares (peer) para lograr sus objetivos y en algunos casos tu computadora puede ser atacada. Algunas compañías ofrecen servicios de monitoreo para ayudarte a saber si tu nombre u otra información ha sido robada por criminales cibernéticos y puede encontrarse en la Dark Web, aunque el valor real de estos servicios es cuestionable. La mejor manera de protegerse es asumir que alguna información se encuentra ya dentro de la Dark Web, y está siendo usada por criminales cibernéticos. Por ello, te recomendamos:

- **Sospecha de cualquier llamada telefónica o correo electrónico que pretenda presentarse como una organización oficial y te presione a realizar algo como pagar una multa. Los criminales pueden usar información personal que encuentran de ti para atacar con más seguridad.**
- **Monitorea tus tarjetas de crédito y estados de cuenta. Siempre es una buena idea configurar alertas que envíen un mensaje sobre cualquier transacción. Esto puede llevar a que detectes si está sucediendo un fraude financiero, y en caso de detectarlo repórtalo con tu banco inmediatamente.**
- **Congela tu capacidad de crédito. Esto no impacta en como puedes usar tu tarjeta de crédito y es uno de los pasos más efectivos para protegerte del robo de identidad.**

## Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

## Editor Invitado

***Micah Hoffman*** *(@WebBreacher) es el investigador principal en Spotlight Infosec LLC, instructor certificado del SANS Institute y autor para cursos de SANS OSINT. La pasión de Micah por la inteligencia cibernética y de código abierto se pueden apreciar en sus proyectos, cursos y estilo de enseñanza.*

## Recursos

| | |
|---|---|
| Ataques personalizados: | https://www.sans.org/u/RfW |
| Ingeniería social: | https://www.sans.org/u/Rg1 |
| Robo de identidad: | https://www.identitytheft.gov |
| Congela capacidad de crédito: | https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/ |
| Navegador TOR: | https://www.torproject.org/ |
| Curso SANS OSINT: | https://sans.org/sec487 |
| Mitos y realidades de la Internet profunda: | https://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-internet-profunda |