Video 1

00:10
Bienvenido de nuevo. Es genial tenerte aquí. Este es el curso sobre anonimato en la dark web y ciberseguridad. Te doy la bienvenida de nuevo

00:36
a otro contenido encantador, hermoso y extremadamente útil. El curso trata de usar la dark web y mantener el anonimato

00:46
al mismo tiempo. Y al final, aprenderemos cuáles son los pasos para usar la ciberseguridad. Las mejores prácticas para

00:58
estar en modo privado mientras se accede a contenido público. Muy bien, así que primero comenzaremos con cuáles son los riesgos que existen cuando accedes

01:04
al curso. Es decir, perdón, no exactamente el curso que estás tomando en este momento, sino al acceder a algunos contenidos que consideres muy privados, o tal vez si estás en un negocio donde la libertad de expresión, la libre...

[1:13]
Realmente importante, donde tu discurso corresponde a la prensa. Muy bien. Entonces, aquí es donde tener el poder de ser anónimo es muy, muy importante. Y ahí es donde aprenderemos más sobre cómo usar la dark web para acceder a algunos de los distintos contenidos.

[1:25]
Está bien. Así que este es el lugar donde tener el poder de ser anónimo es muy, muy importante. Y ahí es donde aprenderemos más sobre cómo usar la dark web para acceder a algunos de los distintos contenidos.

[1:34]
No necesariamente para acceder de lleno, sino para ver cuáles son los diferentes contenidos disponibles. ¿Es bueno? ¿Es malo? Y con seguridad será malo el 90% o el 95% de las veces, pero...

[1:45]
Así es como lo vemos. Qué es todo al mismo tiempo. También veremos si incluso

puedes usar libremente tu web pública mientras navegas en modo privado o de forma anónima. Entonces...

[1:58]
"Uso de tu web pública, la web disponible de forma libre. ¿Cuáles son los diferentes pasos para estar en modo privado o ser anónimo? Entonces..."

[2:07]
"...para que cualquier actividad que realices, sigas estando seguro. Muy bien. Así que comencemos. Lo primero que aprenderemos es la introducción de este curso. Y luego..."

[2:16]
"...aquí aprenderemos sobre los diferentes riesgos involucrados. Entonces, si eres un usuario nuevo, como te dije, en el ámbito de la libertad de expresión o temas relacionados con la prensa, o tal vez tienes algún contenido que puedas enviar..."

[2:26]
el cual puede ser muy sensible para alguna parte interesada. ¿Verdad? Así que, en ese caso, es muy importante para ti. Pero antes de llegar a eso,

[2:35]
necesitamos entender dónde reside realmente el riesgo. Muy bien, lo primero es tu hardware: tu sistema, tu laptop, tu computadora de escritorio, tu teléfono móvil,

[2:44]
cualquier dispositivo. De acuerdo. Cualquier cosa relacionada con tu sistema de hardware desde el que accedes al resto del mundo. Ahí es donde entran estos “cruzados”. Tú

[2:53]
podrías tener tus datos, pero eso no evita que otra persona... ¿y si...

[2:58]
eso se convierte en un riesgo para ti, porque es valioso? La persona o la parte de los datos...

[3:04]
si estás usando tecnología de cifrado, existen programas que funcionan en segundo plano y pueden

[3:09]
obtener esa información si ellos...

[3:12]
así lo desean. Muy bien. Lo siguiente es el sistema operativo. Ahora, entiende que este sistema operativo te ayuda

[3:20]
a manejar tu hardware y todas las aplicaciones que se ejecutan en él. Entonces, básicamente, hablamos de

[3:26]
Windows, tal vez hablemos de

[3:28]
Mac OS, tal vez hablemos de Linux, cualquier cosa, incluso Kali. Todos son sistemas operativos. Y ellos..."**[3:31]**
"Hacer o usar todas tus aplicaciones que se ejecutan en tu hardware, ¿verdad? Tal vez hables de Windows. Tal vez hables de Mac OS, menciona tu marca, o Linux, cualquier cosa, incluso Kali. Todos estos son sistemas operativos. Y ahora, si estos pueden almacenar la información (porque nunca sabemos si esta es información de código abierto), si eso es lo suficientemente bueno... pero, al mismo tiempo, Windows o Mac OS son desarrollados por organizaciones privadas y no tenemos ningún control al respecto, ¿verdad?

[3:50]
Entonces, lo siguiente es el navegador. Entiende esto: todo lo que hagamos en la red pública, lo hacemos ya sea a través de conversaciones por correo electrónico o directamente en el navegador. Y el navegador es algo que hace que toda la actividad esté disponible en la situación en la que nos encontramos. Estamos en una era en la que todo se ha trasladado a las aplicaciones, desde cualquier conversación de texto hasta cualquier chat; todo puede ejecutarse dentro del navegador.

[4:05]
Tal vez navegues de otra forma, pero todo puede ser rastreado porque todo está conectado a la red pública, ¿verdad? Así que nunca sabes quién está pasando por la "puerta de enlace" (Gateway), y esta puerta de enlace transmite o envía una copia del tráfico a agencias gubernamentales u otras autoridades para todos sus ciudadanos, con cualquier propósito: ya sea para influir o, como sabes, para ejercer una vigilancia adecuada sobre su actividad, ¿verdad?"

[4:58]
"Y ahí es donde realmente está el riesgo. Así es, y luego llegamos al tema del correo electrónico que tal vez uses, como Gmail o Outlook.com.

[5:07]
Todos estos se crearon con el propósito de ser productivos, brindándote una plataforma útil para enviar correos. Pero si proporcionas cualquier tipo de correo privado o anónimo, o digamos que envías un correo que pasa por sus servidores, desde ahí podría ser 'pescado' (phished) y enviado a múltiples clientes o quizá al destinatario. Así que no existe un tipo de anonimato real ni una forma efectiva de hacerlo anónimo.

Lo siguiente es tu Wi-Fi. Eso es algo normal, suena sencillo, pero adivina qué. No estoy seguro de si has revisado mi otro contenido anterior sobre hacking ético. Deberías saber que, si alguien obtiene acceso a tu red inalámbrica, podría ver... No puede obtener toda la información real, pero tal vez pueda ver tu nombre. Porque, si hay un ataque típico de 'hombre en el medio', ¿verdad?

Entonces, el aspecto más importante es tu web en tu navegador, tu sistema, tus datos o cualquier conexión que salga de tu computadora o dispositivo habitual, ¿de acuerdo? O tal vez lo viste en sesiones anteriores. Bueno, parece sencillo, pero te das cuenta de que hay mucho más.

Muy bien, ahora, al final, sé que suena un poco... pero sí, en general es algo muy distinto. Pero sí, por supuesto, 'gran auto'."

[6:48]
"O cualquier otra información tuya, como el número de Seguro Social de Susan o cualquier otro dato, cualquiera podría localizarlo, ¿verdad? Porque si estás comprando algo y haces un pedido, digamos, con tu tarjeta de crédito, pueden rastrear, 'de acuerdo, ¿quién fue la persona que compró esta información?' Porque ahí es donde tu nombre y dirección, y todo eso, deben ser llenados y podrían filtrarse, ¿verdad?

Ahora, es importante entender cómo se pueden cubrir todos esos riesgos al final. ¿Cierto? Y de eso estamos hablando: ser anónimo no es más que lograr también la privacidad. Así que de eso se trata todo. Ahora, hablemos de cómo reducir el riesgo en cada capa. Hablamos de riesgos en el hardware, en el sistema operativo, en el navegador. Primero, hablemos del sistema operativo.

Muy bien, entonces hablaremos de cada uno de ellos uno por uno. Porque todo se trata de... cuéntame, sí. ¿Qué tiene de especial? A diferencia de cualquier sistema operativo que tiene que vincularse con tu hardware, ya sabes, por supuesto, la MacBook, tu Mac OS solo puede ejecutarse en Apple, claro, pero aun así, la mayoría de las otras, como HP, Dell, Windows, pueden ejecutar todo o cualquier sistema

operativo que instales. Pero recuerda esto: los datos de ese sistema operativo aún permanecen en él. Una vez que instalas un sistema operativo, este se comunica con tu computadora y con el hardware

[8:24]
"almacena esa información y, cuando usas 'televised' (está diseñado para que no sea persistente), puedes usar una memoria USB. Te mostraré

[8:31]
en los cursos posteriores cómo puedes tener una memoria USB de arranque, con Tails Linux y este 'cuento' de métodos (Tails). Una vez que la instalas y la insertas en cualquier laptop,

[8:37]
está lista para funcionar. Puedes hacer tu trabajo y, cuando la retiras, borra o limpia todos los datos que

[8:43]
hayas generado en ella. Así que eso es útil. Muy bien, lo siguiente es el navegador Tor. Lo usaremos cuando queramos acceder o tratar de ver todo lo que

[8:55]
existe en la dark web, ¿verdad? Entonces, en este curso, aprenderemos y lo veremos con fines educativos. ¿Por qué?

[9:02]
Lo digo porque es el mismo entorno, y es muy, muy importante. La dark web es algo que, en su mayoría, se utiliza con fines maliciosos. Pero, con fines educativos, queremos ver qué hay en la dark web para poder educar a otros.

[9:15]
Así podremos asegurarnos de que tú mismo estés seguro y no entres a ningún sitio extraño, esa web o darknet, ya sabes. Solo encuentra la manera de usarla y cómo estar lo suficientemente protegido antes de realizar cualquier actividad allí. Muy bien. Entonces, ahora lo siguiente: usar un hotspot Wi-Fi..."

[8:57]
"De tu hotspot Wi-Fi, adondequiera que vayas, adondequiera que viajes. No uses de forma activa ninguna red Wi-Fi pública. Y estoy hablando de cosas más grandes, como ese mismo asunto, por supuesto, al abrirlo. Y esto es algo muy importante. Es una tecnología muy antigua, pero aún funciona porque aquí es donde, ya sabes,

realmente entra en juego. Envías un correo electrónico, lo encriptas, cifras ese contenido; la otra parte, si tiene la clave, puede descifrarlo y ver qué contiene.

Muy bien. Ahora, todo esto trata de la seguridad de tu correo electrónico. Es decir, que sea lo suficientemente seguro y privado. Pero, en cuanto a lo que llamamos “acuñado”, sé que no lo hago todo, ya sabes, Bitcoin, ¿verdad? Sin embargo, estamos hablando de ello no por dinero. No es para tener una precisión o valoración, nada de eso. De lo que hablo aquí es: si realmente quieres volverte anónimo en cualquier lugar de la red, incluso usando tu información de tarjeta de crédito, asegúrate de no proporcionarla, porque ahí es donde está tu información personal. Así que evítalo.

Muy bien, ahora, “Vernon” o algo así. Recuerdo que hablé del riesgo de tu hardware. Y, si quieres evitarlo usando cualquier computadora portátil popular conocida, muy bien, nunca hagas eso. Nunca, jamás, compartas tu recomendación."

[11:24]
"con cualquiera, ¿verdad? Porque aquí es donde, incluso si lo intentaste todo, tratas de reducir el riesgo en todas partes. Luego compartes tu información personal. No hay forma de saberlo, ¿verdad? Porque nunca sabes exactamente dónde está circulando ni cómo puede usarse.

Ahora, de lo que realmente hablo al final es de lo que sea que vayamos a aprender. Esto es algo personal para fines educativos. Así que asegúrate, asegúrate de no hacer nada ilegal en la dark web. Este es mi consejo muy, muy, muy personal. Porque, si haces algo ilegal y te involucras, podrían rastrearte. Así que debes evitar hacer eso también.

Y esta es toda la introducción sobre los cursos web, el anonimato en la dark web y el curso de ciberseguridad. Ahora hemos aprendido sobre los diferentes riesgos que existen y cómo mitigarlos. A medida que avancemos en el curso, profundizaremos en cada uno de estos puntos, y también veremos algunos temas más avanzados a lo largo de este curso.

Muy bien, espero que te haya gustado esta lección. Nos vemos en la próxima."