



วิธีใช้อินเทอร์เน็ตอย่าง ปลอดภัย

- 
- 1. เก็บรักษาข้อมูลส่วนบุคคล ให้ปลอดภัยอยู่เสมอ
 - 2. เปิดการตั้งค่าความเป็นส่วนตัวของคุณไว้
 - 3. เลือกเว็บเบราว์เซอร์ที่ปลอดภัย
 - 4. ตรวจสอบว่าการเชื่อมต่ออินเทอร์เน็ตของคุณมีความปลอดภัย
 - 5. ระวังสิ่งที่คุณดาวน์โหลด
 - 6. ระวังเว็บไซต์ปลอม

1. เก็บรักษาข้อมูลส่วนบุคคล ให้ปลอดภัยอยู่เสมอ

- นายจ้างหรือลูกค้าที่มีความเคารพมากพอ พวกเขาจะไม่ก้าวล่วงความเป็นส่วนตัวของคุณ ฉะนั้นพวกเขาไม่จำเป็นต้องรู้สถานะความสัมพันธ์ส่วนตัว หรือที่อยู่บ้านของคุณ สิ่งที่เขาจำเป็นต้องรู้คือความสามารถของคุณเกี่ยวกับอาชีพ และวิธีการติดต่อกับคุณเท่านั้น ดังนั้นคุณจึงไม่จำเป็นต้องส่งข้อมูลส่วนบุคคลทั้งหมดให้กับคนแปลกหน้า และอย่าให้ข้อมูลเหล่านี้แก่ผู้คนนับล้านบนโลกออนไลน์

2. เปิดการตั้งค่าความเป็นส่วนตัวของคุณไว้

- นักการตลาดจะอยากทราบข้อมูลทั้งหมดเกี่ยวกับตัวคุณ และแฮกเกอร์ทำเช่นกัน ทั้งสองคนสามารถเรียนรู้ได้จากการเรียกดูและการใช้งานโซเชียลมีเดียของคุณ แต่คุณสามารถดูแลข้อมูลของคุณได้ ตามที่ระบุไว้ใน **Lifehacker** เว็บเบราว์เซอร์และระบบปฏิบัติการบนมือถือจะมีการตั้งค่าเพื่อปกป้องความเป็นส่วนตัวของคุณทางออนไลน์ เว็บไซต์ที่สำคัญเช่น **Facebook** มีการตั้งค่าการเพิ่มความเป็นส่วนตัวที่พร้อมใช้งาน การตั้งค่าเหล่านี้จะทำให้ข้อมูลของคุณไม่ปรากฏบนโลกออนไลน์ และค้นหาได้ยากขึ้น เนื่องจาก บริษัทต้องการให้ข้อมูลส่วนบุคคลของคุณสำหรับมูลค่าทางการตลาด อย่าลืม! ตรวจสอบว่าคุณได้เปิดใช้งานการป้องกันความเป็นส่วนตัวเหล่านี้แล้ว

3. เลือกเว็บเบราว์เซอร์ที่ปลอดภัย

- คุณจะเลือกที่จะเดินผ่านย่านที่อันตราย — อย่าไปที่ย่านที่เป็นอันตรายในโลกออนไลน์ อาชญากรไซเบอร์ใช้เนื้อหาที่น่ากลัวเป็นเหยื่อ พวกเขารู้ว่าบางครั้งคนถูกล่อลวง โดยเนื้อหาที่น่าสงสัยและอาจทำให้การระวังตัวของพวกเขาต่ำลงเมื่อได้ค้นหาได้ทางอินเทอร์เน็ต ซึ่งเต็มไปด้วยข้อผิดพลาดที่ไม่สามารถมองเห็นได้ การคลิกอย่างประมาทอาจทำให้ข้อมูลส่วนตัวหรือทำให้อุปกรณ์ของคุณเกิดการติดเชื้อมัลแวร์ได้ และเป็นการกระตุ้นให้แฮกเกอร์ใช้ช่องโหว่เหล่านั้นในการโจมตีคุณ

4. ตรวจสอบว่าการเชื่อมต่ออินเทอร์เน็ตของคุณมีความปลอดภัย

- เมื่อคุณออนไลน์ในที่สาธารณะ ตัวอย่างเช่น โดยใช้การเชื่อมต่อ **Wi-Fi** สาธารณะ **PCMag** จะแจ้งว่าคุณไม่สามารถควบคุมความปลอดภัยได้โดยตรง ผู้เชี่ยวชาญระบบความปลอดภัยในโลกไซเบอร์กังวลเกี่ยวกับ “จุดปลายทาง” ซึ่งเป็นที่ที่เครือข่ายส่วนตัวเชื่อมต่อกับโลกภายนอก ปลายทางที่ไม่ปลอดภัยคือการเชื่อมต่ออินเทอร์เน็ตในสถานที่ที่คุณอาศัยอยู่ การตรวจสอบจะช่วยคุณสังเกตว่าอุปกรณ์ของคุณปลอดภัย ดังนั้นโปรดรู้สึกว่าคุณจะตรวจสอบเสร็จเรียบร้อยแล้ว ก่อนที่จะให้ข้อมูลเช่น หมายเลขบัญชีธนาคาร

5. ระวังสิ่งที่คุณดาวน์โหลด

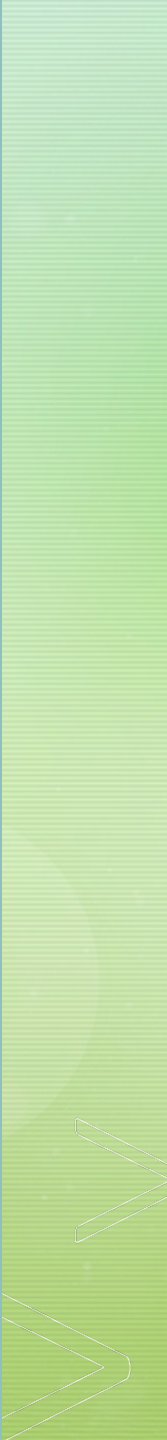
- เป้าหมายสูงสุดของอาชญากรไซเบอร์ คือการหลอกลวงให้คุณดาวน์โหลดโปรแกรมหรือแอปพลิเคชันมัลแวร์ที่มีมัลแวร์ หรือพยายามขโมยข้อมูล มัลแวร์เหล่านี้สามารถปลอมตัวเป็นแอปพลิเคชันใดก็ได้ ตามคำแนะนำของ **PCWorld** อย่าดาวน์โหลดแอปพลิเคชันที่ดูน่าสงสัย หรือมาจากเว็บไซต์ที่ไม่น่าเชื่อถือ

6. ระวางเว็บไซต์ปลอม

- เว็บไซต์เหล่านี้มักมีชื่อเว็บไซต์หรือ **URL** ใกล้เคียงกับเว็บไซต์ของจริง แต่อาจมีการสะกดผิดไปจากเดิมเล็กน้อย ซึ่งถ้าเจอเว็บไซต์ที่มีการสอบถามข้อมูลส่วนตัวเมื่อไหร่ ให้ลองกลับไปดูที่ **URL** อีกทีเพื่อให้แน่ใจว่าคุณเข้าถูกต้องเว็บไซต์



หรือจะหันมาใช้งาน VPN



VPN คืออะไร ?

- สำหรับ **VPN** เป็นตัวย่อที่มาจากชื่อเต็มว่า **Virtual Private Network** หรือแปลความหมายง่ายๆ ว่าเป็นการจำลองเครือข่ายอินเทอร์เน็ตแบบส่วนตัว โดย **VPN** ทำหน้าที่ปกป้องความเป็นส่วนตัวในการทำงานอินเทอร์เน็ต ไม่ว่าจะเป็นการรับ-ส่งข้อมูลที่มีการเข้ารหัส เข้าถึงเนื้อหารูปแบบต่างๆ ได้จากทั่วโลก โดยไม่มีใครสามารถติดตามการใช้งานนั้นๆ ได้ เพราะสาเหตุบางประการในต่างประเทศที่จำเป็นต้องใช้ **VPN** ร่วมด้วย

VPN มีความจำเป็นต้องใช้ไหม ?

- ความจำเป็นในการใช้งาน **VPN** นั้น ขึ้นอยู่กับพฤติกรรมการใช้งานอินเทอร์เน็ตของแต่ละบุคคล โดยเนื้อหาที่ต้องผ่านช่องทาง **VPN** ไม่จำเป็นต้องเป็นเนื้อหาสุ่มเสี่ยงหรือขัดต่อกฎหมายเสมอไป แต่อาจจะเป็นสื่อบันเทิง สื่อให้ความรู้ในต่างประเทศที่ไม่สามารถเข้าถึงได้ด้วยช่องทางปกติ เช่น เกมต่างประเทศที่ต้องเข้าผ่าน **VPN Server** จากประเทศต้นทาง, การฟังเพลง **Podcast** หรือ **Playlist** บนแอปพลิเคชันที่ถูก **Block** ในบางประเทศ หรือแม้แต่การสืบค้นตำราวิชาการต่างประเทศ ฉะนั้น หากต้องการรับทราบข้อมูลข่าวสารหรือเสพความบันเทิงที่น่าสนใจ แต่ไม่สามารถใช้งานได้เพราะอาจถูก **Block** หรือจำกัดการใช้งาน **VPN** ก็เป็นสิ่งที่จำเป็นทีเดียว

- ถ้าใครกังวลเรื่องความปลอดภัยในการใช้งานอินเทอร์เน็ต **VPN** เป็นอีกหนึ่งคำตอบที่ช่วยคุณได้ เพราะ **VPN** เป็นการเปิดช่องทางส่วนตัวให้เข้าถึงข้อมูลผ่านผู้ให้บริการ **VPN** บนเครือข่ายอินเทอร์เน็ต มี **Username** และ **Password** สำหรับใช้งานโดยเฉพาะ สามารถซ่อนเลข **IP** เพื่อไม่ให้ทิ้งพิกัดหรือร่องรอย และด้วยการเข้ารหัสข้อมูล จึงทำให้ไม่สามารถแกะรอยได้ว่ามีการใช้งานผ่าน **VPN** อย่างไรบ้าง แต่ขอให้เลือกผู้ให้บริการ **VPN** อย่างรอบคอบถี่ถ้วน เพราะบริการ **VPN** บางแห่งอาจเกิดจากอาชญากรที่สร้างขึ้นมาเพื่อดักจับข้อมูลส่วนตัวและประวัติการใช้งานอินเทอร์เน็ตเพื่อนำไปก่อเหตุในอนาคตได้

VPN ใช้ได้ในกรณีใดบ้าง ?

- แม้ว่า **VPN** จะถูกหยิบยกขึ้นมาเมื่อเกิดเหตุการณ์ที่เว็บไซต์หรือเนื้อหาใดๆ ถูกปิดกั้นในบางพื้นที่ แต่แท้จริงแล้ว **VPN** สามารถนำมาใช้ในชีวิตประจำวันก็ได้ เพราะการใช้ชีวิตของแต่ละคนอาจต้องพึ่งพาข้อมูลจากต่างประเทศเป็นส่วนใหญ่ และใน **Search Engine** ปกติอาจไม่เพียงพอ รวมถึงบางคนอาจต้องการความปลอดภัยขั้นสูง ฉะนั้น **VPN** จึงเป็นอีกตัวเลือกหนึ่งสำหรับการใช้งานอินเทอร์เน็ตอย่างปลอดภัย เข้าถึงข้อมูลได้มากกว่า

แนะนำบริการ 5 (+1) VPN ที่น่าสนใจ

- 1. บริการ ExpressVPN
- 2. บริการ SurfShark
- 3. บริการ CyberGhost
- 4. บริการ NordVPN
- 5. บริการ VPNhub
- 6. WARP [1.1.1.1 DNS]



1. บริการ ExpressVPN

- หนึ่งในบริการ VPN เก่าแก่จากเกาะอังกฤษที่มีมาตั้งแต่ราวช่วงปี ค.ศ. 2009 (พ.ศ. 2552) นี้ นอกจากจะมีบริการครอบคลุมการใช้งานบนอุปกรณ์ที่หลากหลายแล้วยังสามารถใช้เข้าถึงบริการสตรีมมิ่งได้อย่างครอบคลุมและใช้งาน **Torrent** ได้อย่างไม่จำกัดอีกด้วย
- สำหรับเซิร์ฟเวอร์ของ **ExpressVPN** ก็มีมากกว่า 3,000 เครื่องใน 94 ประเทศทั่วโลก (รวมทั้งในประเทศไทยและจีนด้วย) จึงทำให้ผู้ใช้สามารถเข้าถึงเว็บไซต์ได้เกือบทั่วทุกมุมโลก ซึ่งผู้ใช้สามารถสมัครใช้งาน **ExpressVPN** แบบการันตีคืนเงินได้เป็นจำนวน 30 วันในราคา 12.95 เหรียญสหรัฐต่อเดือน หรือเดือนละ 8.32 เหรียญสหรัฐในแพลงรายปี



2. บริการ SurfShark

- เป็นบริการ **VPN** อีกแบรนด์ที่น่าหยิบมาเพราะราคาต่ำสุด (ตุลาคม ค.ศ. 2020 (พ.ศ. 2563)) ถูกมากๆ เริ่มต้นเพียง 2.49 เหรียญสหรัฐสำหรับแพลง 2 ปี มีให้บริการแทบทุกแพลตฟอร์มหลักไปจนถึง **Linux** และ **Fire TV Stick** ด้วย รวมทั้งไม่จำกัดจำนวนอุปกรณ์ในการใช้งาน
- **Surfshark** โดดเด่นด้าน **Torrent** และการสตรีมมิ่งที่ไม่ถูกจำกัดความเร็ว สามารถดูหนังความละเอียดสูงๆ ได้สบาย แต่ถ้าเทียบกับแบรนด์อื่นๆ แล้ว **Surfshark** ถึงแม้จะครอบคลุมกว่า 63 ประเทศ แต่ก็มีเซิร์ฟเวอร์เพียง 1,700 เครื่องเท่านั้น สำหรับผู้ที่สนใจก็สามารถทดลองใช้งาน **Surfshark** (บน **Android** และ **iOS**) ได้เป็นจำนวน 7 วัน หรือ 30 วัน (บนอุปกรณ์ใดก็ได้) แบบการันตีคืนเงินก่อนตัดสินใจใช้งานต่อได้



3. บริการ CyberGhost

- สำหรับ **CyberGhost** ก็มีความน่าสนใจอยู่ที่เป็นบริการ **VPN** ที่มีเครื่องเซิร์ฟเวอร์สูงเป็นอันดับต้นๆ เลยก็ว่าได้ เพราะนอกจากจะมีเซิร์ฟเวอร์กว่า 6,600 เครื่องแล้ว ยังครอบคลุมไปถึง 90 ประเทศทั่วโลกอีกด้วย (แต่ไม่สามารถใช้งานในประเทศจีนได้)
- นอกจากเซิร์ฟเวอร์ที่ครอบคลุมแล้ว **CyberGhost** ก็ยังมี **UI** ที่เป็นมิตรกับผู้ใช้ที่ไม่ชำนาญการใช้งานอีกด้วย อีกทั้งยังรองรับการใช้งานแทบจะทุกแพลตฟอร์มอุปกรณ์ (แต่สำหรับบน **iOS** จะมีฟีเจอร์ที่น้อยกว่า **Android** อยู่พอสมควร) และรองรับการใช้งานกับจำนวนอุปกรณ์สูงสุดถึง 7 อุปกรณ์ หรืออาจเลือกใช้ **CyberGhost** กับเราเตอร์ เพื่อให้อุปกรณ์ต่างๆ ที่เชื่อมต่ออินเทอร์เน็ตบนเราเตอร์ใช้งานอย่างปลอดภัยได้อีกทางหนึ่ง
- ในด้านของราคาก็น่าคบหาอยู่ที่เพียงเดือนละ 2.25 เหรียญสหรัฐต่อเดือนเท่านั้น (สำหรับการสมัครใช้งาน 3 ปี + 3 เดือน) และมีบริการทดลองใช้งานก่อน 1 วันสำหรับผู้ที่ต้องการทดสอบใช้งานอีกด้วย ส่วนการสมัครใช้แบบการันตีคืนเงินก็มีทั้งแบบ 14 วัน (สำหรับการสมัครใช้รายเดือน) และ 45 วัน (สำหรับการสมัครใช้รายปี)



4. บริการ NordVPN

- เป็นอีกแบรนด์ผู้ให้บริการ **VPN** ที่ได้รับความนิยมเป็นอย่างสูงด้วยความเร็วในการใช้งานจากเครื่องเซิร์ฟเวอร์กว่า 5,000 เครื่องที่กระจายอยู่ในประเทศต่างๆ มากกว่า 60 ประเทศ ซึ่งในบางเซิร์ฟเวอร์รองรับการแชร์แบบ **P2P (Peer to Peer)** รวมทั้งสร้างความปลอดภัยด้วย **Onion VPN** ที่ไม่ระบุ IP ว่าโฮสต์ของเว็บไซต์หรือผู้ที่เข้าถึงเว็บไซต์เป็นใครบ้าง และในอีกหลายๆ เซิร์ฟเวอร์ที่มีความจุสูงเป็นเท่าตัวรองรับการใช้งานได้เกือบทุกอุปกรณ์
- แพ็กเกจของ **NordVPN** เริ่มต้น 11.95 เหรียญสหรัฐต่อเดือน และมีแพ็กเกจ 2 ปี ที่ลดเหลือ 3.71 เหรียญสหรัฐต่อเดือน (ก่อนหน้านี้มีแพ็กเกจ 3 ปีที่มีค่าบริการเหลือเพียง 2.99 เหรียญสหรัฐอีกด้วย) มีให้ทดลองใช้งานแบบรับประกันคืนเงินภายใน 30 วัน



5. บริการ VPNhub

- **VPNhub** เป็นบริการ **VPN** ที่มีโลโก้ค่อนข้างคุ้นเคยสำหรับหลายๆ คน (และแน่นอนว่าทีมผู้พัฒนาเดียวกันกับ **Pornhub** ด้วยเช่นกัน) เปิดตัวขึ้นมาในปี พ.ศ. 2561 (ค.ศ. 2018) ถือว่าเป็นบริการ **VPN** ที่ค่อนข้างใหม่พอสมควร แต่มันก็ครอบคลุมการใช้งานกว่า 60 ประเทศทั่วโลกแม้จะมีเครื่องเซิร์ฟเวอร์ราว 1,000 เครื่องเท่านั้น และสามารถใช้งานบนอุปกรณ์ที่ค่อนข้างหลากหลาย
- ซึ่งบริการนี้มีให้ใช้งานทั้งบน **Windows, Mac, iOS และ Android** อย่างครบถ้วน มีเครื่องข่ายที่ครอบคลุมมากกว่า 60 ประเทศทั่วโลก อย่างไรก็ตามว่ากันว่าประสิทธิภาพของ **VPNhub** ไม่ค่อยเสถียรเท่าที่ควร แต่ก็ไม่ต้องเป็นห่วงเรื่อง **DNS** จะรั่วไหลแต่อย่างใด
- สำหรับค่าบริการของ **VPNhub** ค่อนข้างจะสูงพอสมควร โดยมีค่าบริการเริ่มต้นอยู่ที่เดือนละ 13.99 เหรียญสหรัฐ แต่ถ้าสมัครแพคเกจ 3 ปี จะเหลือเพียงเดือนละ 3.49 เหรียญสหรัฐต่อเดือน และมีให้ทดลองใช้งาน 7 วัน หรือการันตีคืนเงินภายใน 96 ชั่วโมง (ค่าบริการของ **VPNhub** อาจเปลี่ยนแปลงไปตามประเทศของผู้ใช้งาน)



6. WARP [1.1.1.1 DNS]

- สำหรับผู้ที่ต้องการเข้าถึงบางเว็บไซต์ที่ถูกจำกัดการเข้าถึงโดยรัฐบาลแต่ไม่ต้องการสมัครสมาชิกบริการ VPN ต่างๆ ก็สามารถใช้บริการ **Server DNS** เพื่อเข้าถึงเว็บไซต์ที่ถูกบล็อกได้เช่นกัน แต่การใช้งาน **Server DNS** นั้นไม่สามารถซ่อนเลข **IP Address** และเข้ารหัสข้อมูลได้เหมือนกับการใช้งาน **VPN** รวมทั้งยังมีการเก็บข้อมูลการใช้งานบางส่วนของผู้ใช้เอาไว้อีกด้วย
- ซึ่งบริการ **Server DNS** ที่น่าสนใจและปลอดภัยในการใช้งานในขณะนี้ก็น่าจะเป็น **WARP [1.1.1.1] DNS** ของ **Cloudflare** ที่ขึ้นชื่อในเรื่องความปลอดภัยในการใช้งาน เพราะถึงแม้ว่าจะมีการเก็บข้อมูลการใช้งานของผู้ใช้เล็กน้อย (ไม่เก็บข้อมูลส่วนตัวของผู้ใช้) แต่มันก็มีการเคลียร์ข้อมูลทุกๆ 24 ชั่วโมง ด้วยเช่นกัน จึงทำให้ผู้ใช้สามารถมั่นใจได้ว่าข้อมูลการใช้งานเว็บไซต์ต่างๆ ของเรานั้นยังคงถูกเก็บเป็นความลับอยู่นั่นเอง นอกจากนี้ทาง **Cloudflare** ยังเปิดให้สามารถใช้งานกันได้แบบไม่เสียค่าใช้จ่ายและไม่จำกัดการใช้งานอีกด้วย

VPN	ExpressVPN	Surfshark	Cyberghost	NordVPN	VPNHub
Server	3,000+	1,700+	6,600+	5,500+	1,000+
บริการที่สามารถเข้าถึงได้	- Netflix - Disney+ - Amazon Prime - HBO GO - Hulu	- Netflix - Disney+ - Amazon Prime - HBO GO - Hulu	- Netflix - Disney+ - Amazon Prime - Hulu	- Netflix - Disney+ - Amazon Prime - HBO GO - Hulu	- Netflix (US) - Disney+
การใช้งานในประเทศจีน	/	/	-	ใช้งานได้แต่ไม่เสถียร	-
การเชื่อมต่อ	5 เครื่อง	ไม่จำกัด	7 เครื่อง	6 เครื่อง	5 เครื่อง
การเข้ารหัส	AES-256-bit	AES-256-bit	AES-256-bit	AES-256-bit (Double Encryption)	AES-256-bit
โพรโทคอล	- PPTP - L2TP - IKEv2/IPSec - SSTP - OpenVPN	- OpenVPN - IKEv2 - L2TP - Shadowsocks - WireGuard	- OpenVPN - PPTP - IKEv2 - WireGuard - L2TP/IPSec	- OpenVPN - PPTP - L2TP - IKEv2/IPSec	- OpenVPN - IKEv2 - L2TP/IPSec - PPTP - SSTP
Logs	-	เก็บ Log บางส่วน	-	-	เก็บ Log บางส่วน
การใช้งาน	- Windows - macOS - Linux - Browser Extension - Android - iOS - Xbox - Router	- Windows - macOS - Browser Extension - Android - iOS - Router	- Windows - macOS - Linux - Browser Extension - Android - iOS - Xbox - Router	- Windows - macOS - Linux - Browser Extension - Android - iOS - Router	- Windows - macOS - Android - iOS
ระยะเวลาการทดลองใช้	-	7 วัน (เฉพาะบน Android และ iOS)	1 วัน	-	7 วัน
การคืนเงิน	30 วัน	30 วัน	14 วัน (รายเดือน) 45 วัน (รายปี)	30 วัน	96 ชั่วโมง
ค่าบริการ (เหรียญสหรัฐ)	8.32 / เดือน (1 ปี) หรือ 12.95 / เดือน	2.49 / เดือน (2 ปี) หรือ 11.95 / เดือน	2.25 / เดือน (3 ปี) + 3 เดือน) หรือ 12.99 / เดือน	3.71 / เดือน (2 ปี) หรือ 11.95 / เดือน	3.49 / เดือน (3 ปี) หรือ 13.99 / เดือน

ตารางเปรียบเทียบบริการ VPN ยอดนิยม