

# Cyber Security at your fingertips

**Nilay R Mistry**

# Cyber Security

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

# Tips for Cyber Security

Online security is becoming more important than ever. While there's no bulletproof way to prevent a cyber attack, here are some easy tips to help you keep your personal information safe and secure.

## Back up your data



Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

## Keep your operating system up to date



Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

## Install antivirus software



Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

## Choose unique passwords



Create unique passwords for each account - that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.

## Set up two-factor authentication (2FA)



Choose to get a code sent to another device like your phone when logging in online - it helps stop hackers getting into your accounts.

## Use creative recovery answers



Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.

## Be cautious of free WiFi networks



Be careful using free WiFi and hot spots - they are untrusted networks so others could see what you are doing.

## Be smart with social media



What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

## Don't give out personal info



Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.

## Check bank statements regularly



Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

## Get a regular credit check



An annual credit check will alert you if someone else is using your details to get loans or credit.

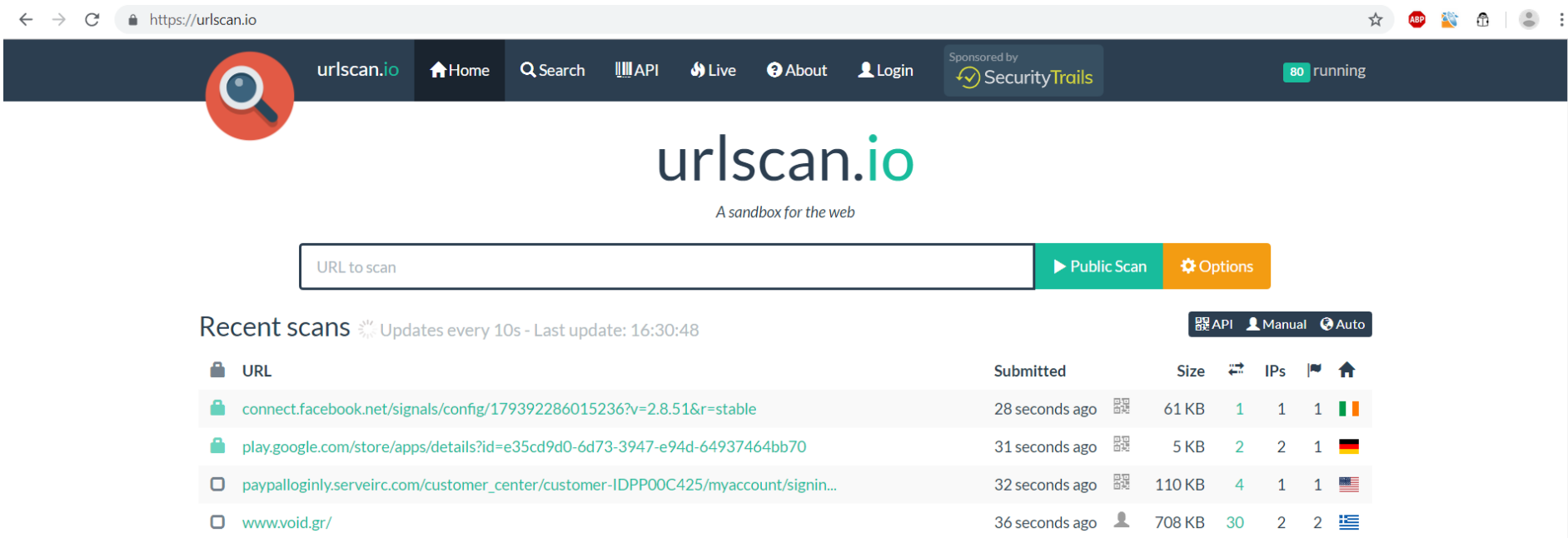
To report a cyber security problem, visit [www.cert.govt.nz](http://www.cert.govt.nz)

# Important tools for Cyber Security

- Tools for URL / Link Analysis
- Tools for File based malware analysis
- Tools for Security & Privacy
- Cyber Threat Intel Map Related Information
- Tools for Security Audit of your personal devices (Smart Devices & PCs)

# Tools for URL / Link Analysis

- For analysis of any suspicious URL or Link please insert your link in URLSCAN.io

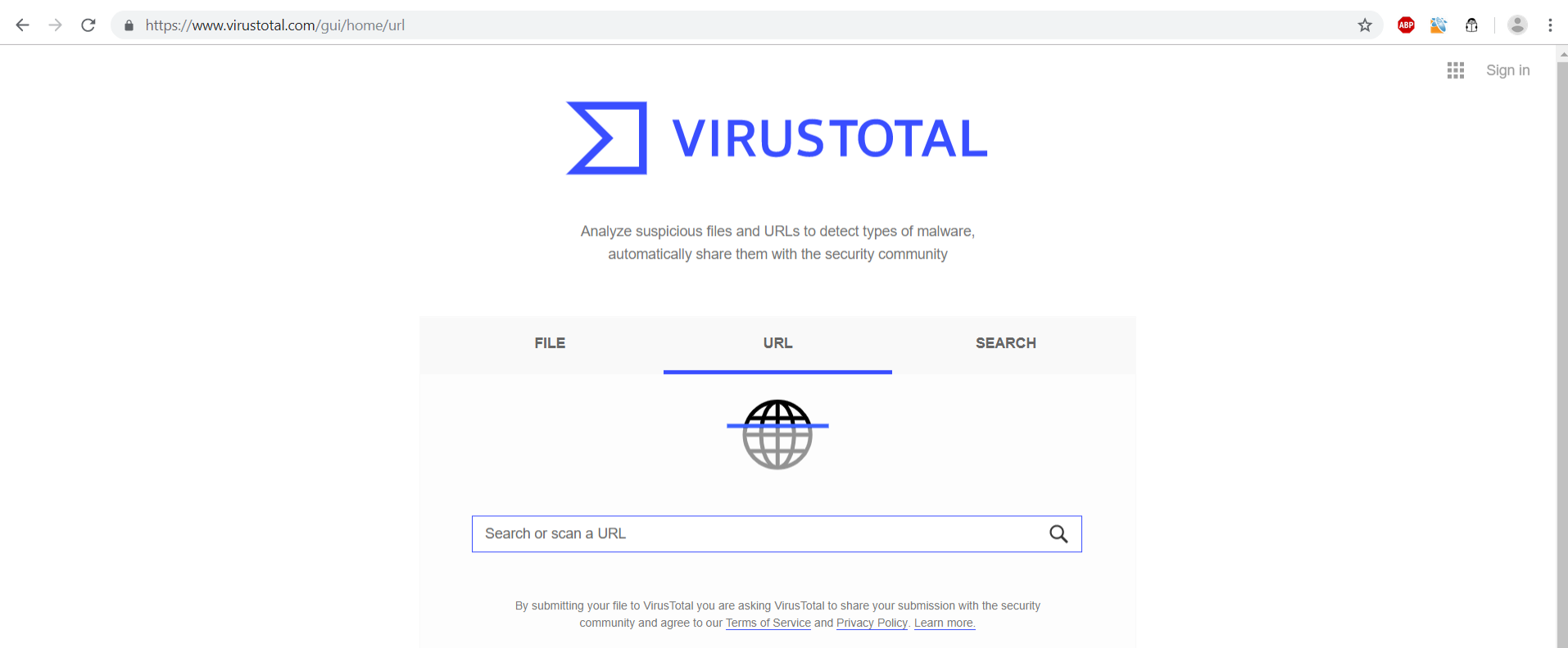


The screenshot shows the URLSCAN.io website interface. At the top, there is a navigation bar with a search icon, 'Home', 'Search', 'API', 'Live', 'About', and 'Login' links. A 'Sponsored by SecurityTrails' badge is visible on the right. The main content area features the URLSCAN.io logo and the tagline 'A sandbox for the web'. Below this is a search bar with the placeholder text 'URL to scan' and two buttons: 'Public Scan' and 'Options'. The 'Recent scans' section is active, showing a table of scan results. The table has columns for 'URL', 'Submitted', 'Size', 'IPs', and a home icon. The scans listed are:

URL	Submitted	Size	IPs	Home
<a href="https://connect.facebook.net/signals/config/179392286015236?v=2.8.51&amp;r=stable">connect.facebook.net/signals/config/179392286015236?v=2.8.51&amp;r=stable</a>	28 seconds ago	61 KB	1 1 1	🇮🇹
<a href="https://play.google.com/store/apps/details?id=e35cd9d0-6d73-3947-e94d-64937464bb70">play.google.com/store/apps/details?id=e35cd9d0-6d73-3947-e94d-64937464bb70</a>	31 seconds ago	5 KB	2 2 1	🇩🇪
<a href="https://paypalloginly.serveirc.com/customer_center/customer-IDPP00C425/myaccount/signin...">paypalloginly.serveirc.com/customer_center/customer-IDPP00C425/myaccount/signin...</a>	32 seconds ago	110 KB	4 1 1	🇺🇸
<a href="http://www.void.gr/">www.void.gr/</a>	36 seconds ago	708 KB	30 2 2	🇬🇷

# Tools for URL / Link Analysis

- Check URL or Link malicious or not please insert your link in [virustotal.com](https://www.virustotal.com)



The screenshot shows the VirusTotal website interface for URL analysis. The browser address bar displays the URL <https://www.virustotal.com/gui/home/url>. The page features the VirusTotal logo, a navigation menu with 'FILE', 'URL', and 'SEARCH' options, and a search input field labeled 'Search or scan a URL'. Below the search field, there is a disclaimer: 'By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more.](#)'

← → ↻ <https://www.virustotal.com/gui/home/url> ☆ ABP 🌐 🔒 👤 ⋮

Sign in

## VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware,  
automatically share them with the security community

FILE URL SEARCH

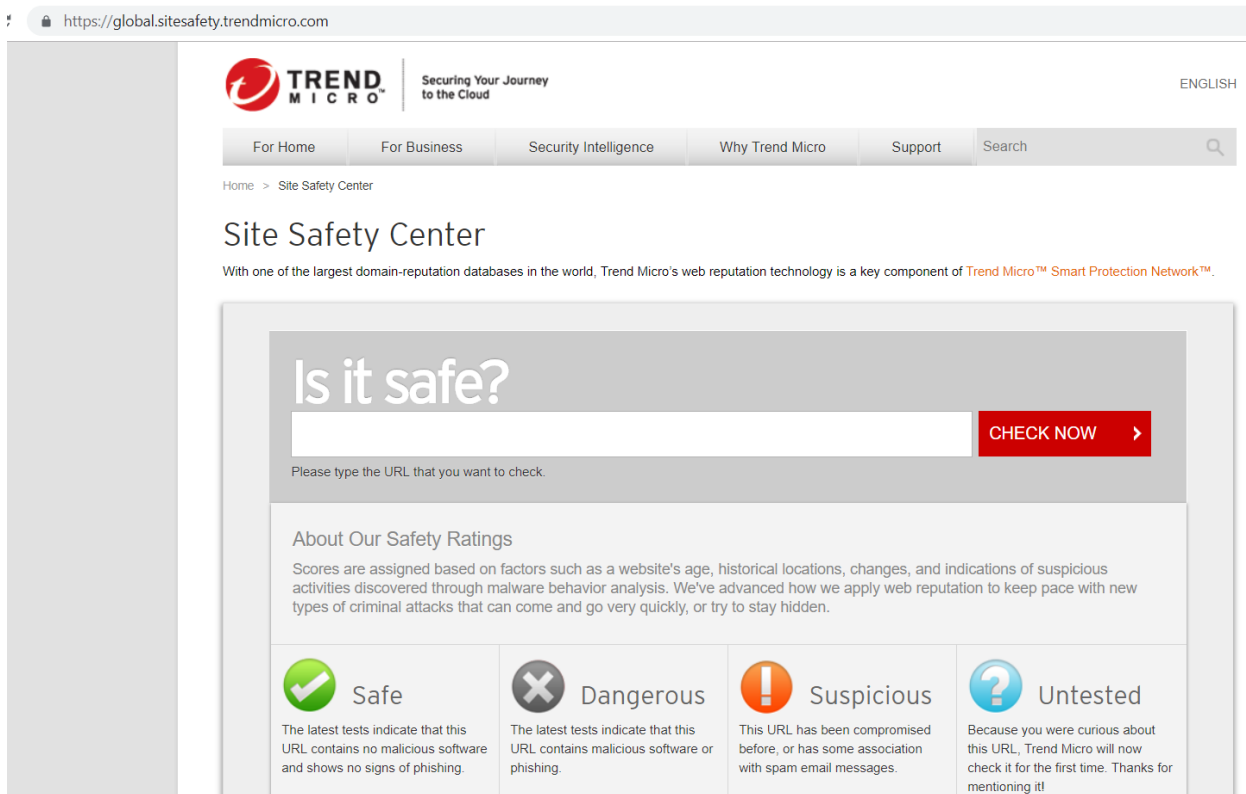
🌐

Search or scan a URL 🔍

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more.](#)

# Tools for URL / Link Analysis

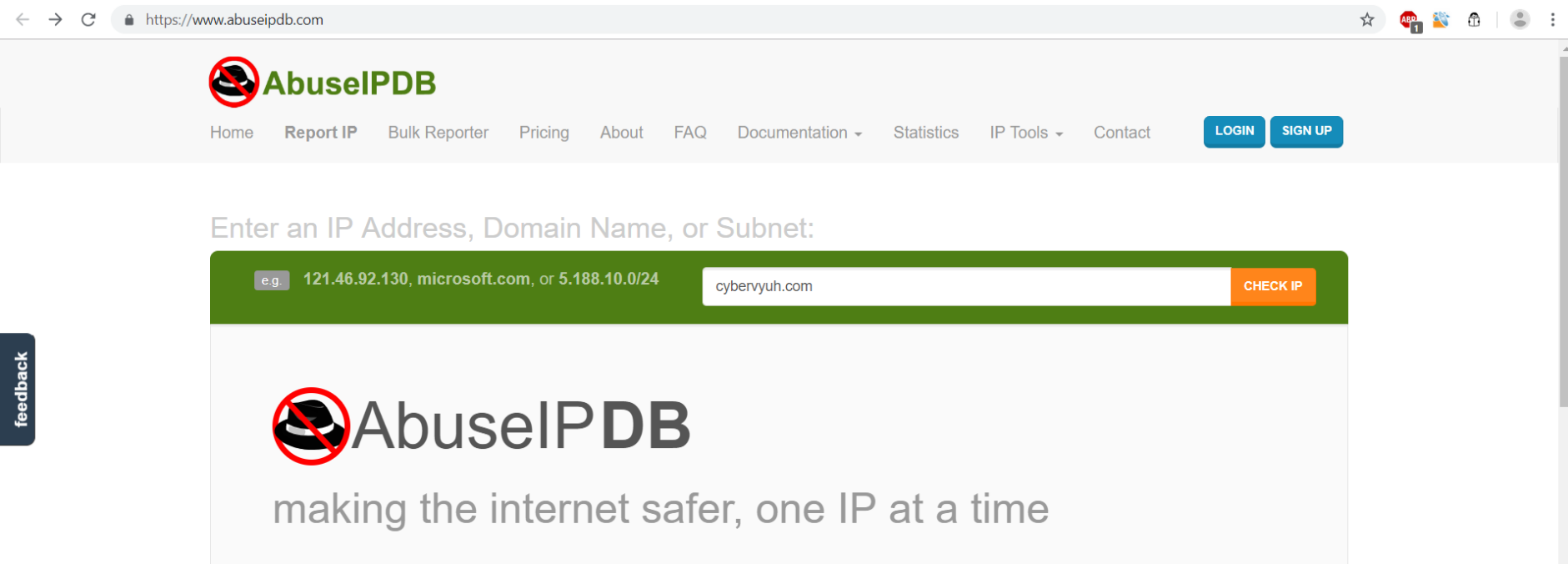
- Check URL or Link safety please insert your link in <https://global.sitesafety.trendmicro.com/>



The screenshot shows the Trend Micro Site Safety Center website. The browser address bar displays <https://global.sitesafety.trendmicro.com>. The page features the Trend Micro logo and tagline "Securing Your Journey to the Cloud" in the top left, and a language selector for "ENGLISH" in the top right. A navigation menu includes links for "For Home", "For Business", "Security Intelligence", "Why Trend Micro", "Support", and "Search". Below the navigation, the breadcrumb "Home > Site Safety Center" is visible. The main heading is "Site Safety Center", followed by a sub-heading: "With one of the largest domain-reputation databases in the world, Trend Micro's web reputation technology is a key component of Trend Micro™ Smart Protection Network™." The central focus is a large grey box titled "Is it safe?" containing a search input field and a red "CHECK NOW" button. Below this, a section titled "About Our Safety Ratings" explains that scores are based on website age, historical locations, and suspicious activities. At the bottom, four safety rating categories are listed: "Safe" (green checkmark), "Dangerous" (grey X), "Suspicious" (orange exclamation mark), and "Untested" (blue question mark), each with a brief description of what the rating indicates.

# Tools for URL / Link Analysis

- Check URL or Link reputation and other details please insert your link in <https://www.abuseipdb.com/>



The screenshot displays the AbuseIPDB website. At the top, the browser address bar shows the URL <https://www.abuseipdb.com>. The website header features the AbuseIPDB logo (a red circle with a black slash over a black silhouette of a person) and the text "AbuseIPDB" in green. Below the logo is a navigation menu with links: Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. To the right of the menu are two blue buttons: "LOGIN" and "SIGN UP".

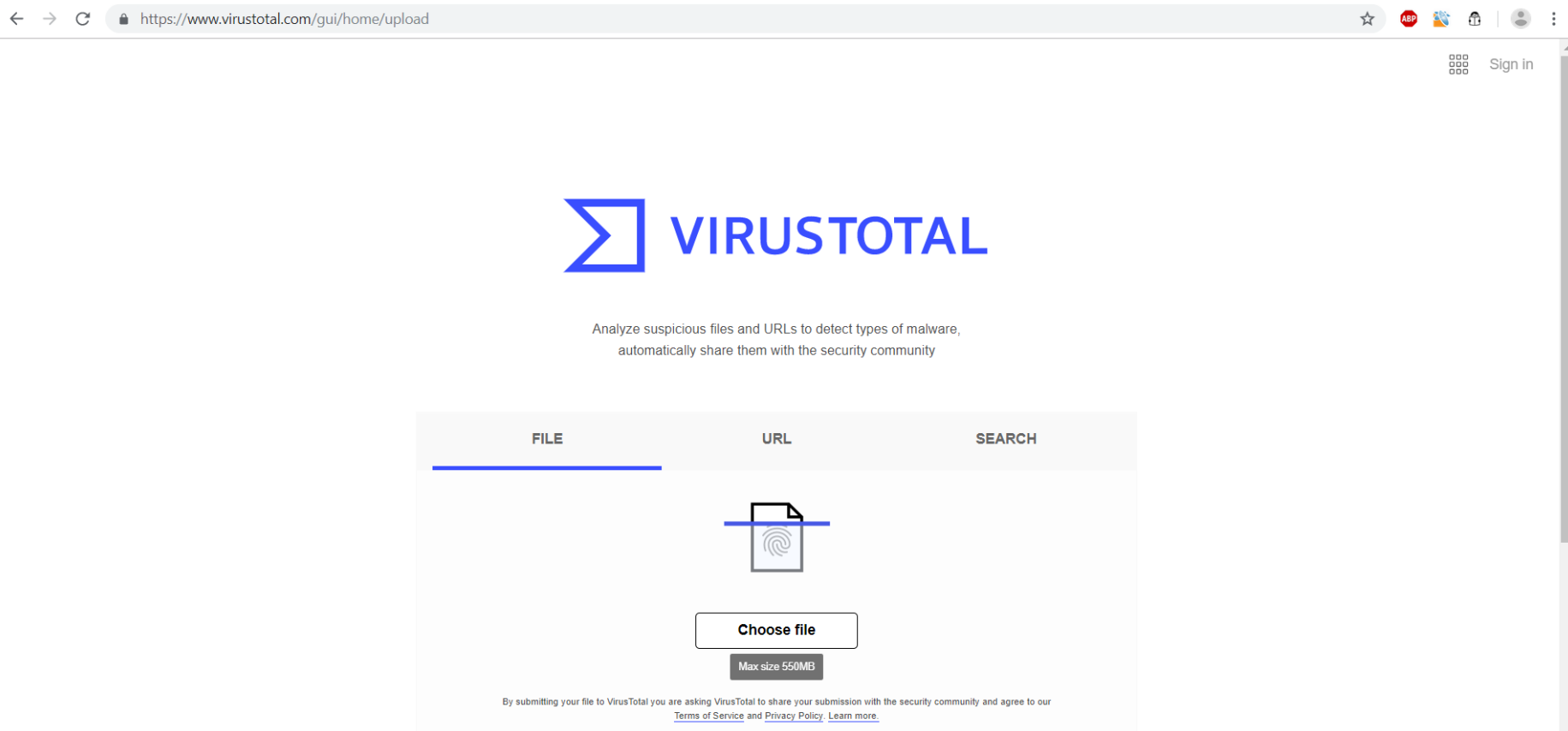
The main content area has a heading "Enter an IP Address, Domain Name, or Subnet:" followed by a search input field. The input field contains the text "cybervyuh.com" and is preceded by a placeholder example: "e.g. 121.46.92.130, microsoft.com, or 5.188.10.0/24". To the right of the input field is an orange button labeled "CHECK IP".

Below the search bar, the AbuseIPDB logo and name are repeated in a larger font, with the tagline "making the internet safer, one IP at a time" underneath. A vertical "feedback" button is visible on the left side of the page.



# Tools for Malicious File Analysis

- Check exe file is suspicious or not please upload your file at [virustotal.com](https://www.virustotal.com)



The screenshot shows the VirusTotal website's upload interface. At the top, the browser address bar displays the URL <https://www.virustotal.com/gui/home/upload>. The page features the VirusTotal logo, a blue square icon with a white 'V' shape, and the text "VIRUSTOTAL". Below the logo, a tagline reads: "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community". The main content area has three tabs: "FILE", "URL", and "SEARCH". The "FILE" tab is selected, indicated by a blue underline. Under the "FILE" tab, there is a large icon of a document with a fingerprint, representing a file upload. Below this icon is a button labeled "Choose file" and a smaller button labeled "Max size 550MB". At the bottom of the page, a small disclaimer states: "By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#)."

# Tools for Malicious File Analysis

- Check exe file is suspicious or not please upload your file at <https://sandbox.pikker.ee/>

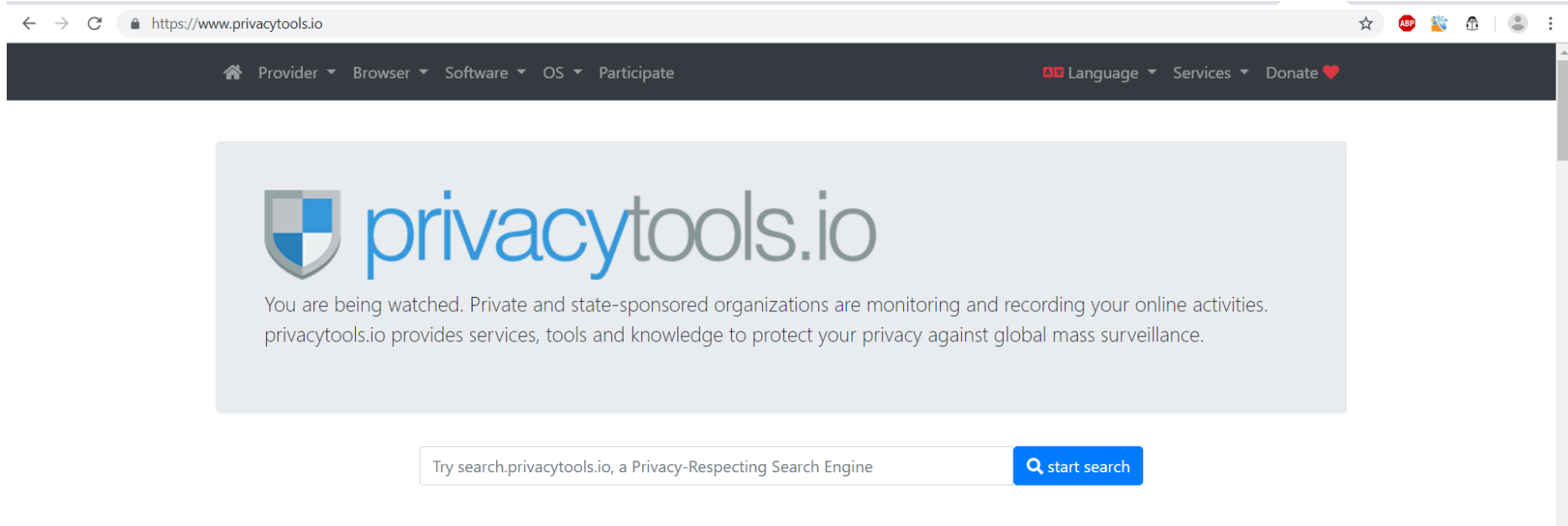
The screenshot displays the Cuckoo Sandbox web interface. The top navigation bar includes 'Dashboard', 'Recent', 'Pending', and 'Search' options, along with 'Submit' and 'Import' buttons. The main content area is divided into several sections:

- Insights:** A sidebar on the left containing:
  - Cuckoo Installation:** A table showing 'Version: 2.0.6' and the status 'You are up to date.'
  - Usage statistics:** A table with the following data:

Category	Count
reported	1125303
completed	11
total	1138962
running	33
pending	0
  - From the press:** A link to 'Click here for more'.
- Cuckoo:** The central area for file submission, featuring a large 'SUBMIT A FILE FOR ANALYSIS' button with an upload icon and a text input field for 'SUBMIT URLS/HASHES'. A 'Submit' button is located below the input field. A note at the bottom of this section reads: 'Drag your file into the left field or click the icon to select a file.'
- System info:** A section at the bottom right showing system metrics with progress indicators:
  - FREE DISK SPACE:** 55.8 TB
  - CPU LOAD:** 30%
  - MEMORY USAGE:** 195.7 GB

# Tools for Security & Privacy


- Ensure your security & privacy via [privacytools.io](https://www.privacytools.io)



The screenshot shows the homepage of [privacytools.io](https://www.privacytools.io). The browser's address bar displays the URL. The navigation menu includes links for Provider, Browser, Software, OS, and Participate, along with Language, Services, and a Donate button. The main content area features the site's logo, a warning message about surveillance, and a search bar.

https://www.privacytools.io

Provider Browser Software OS Participate Language Services Donate

 **privacytools.io**

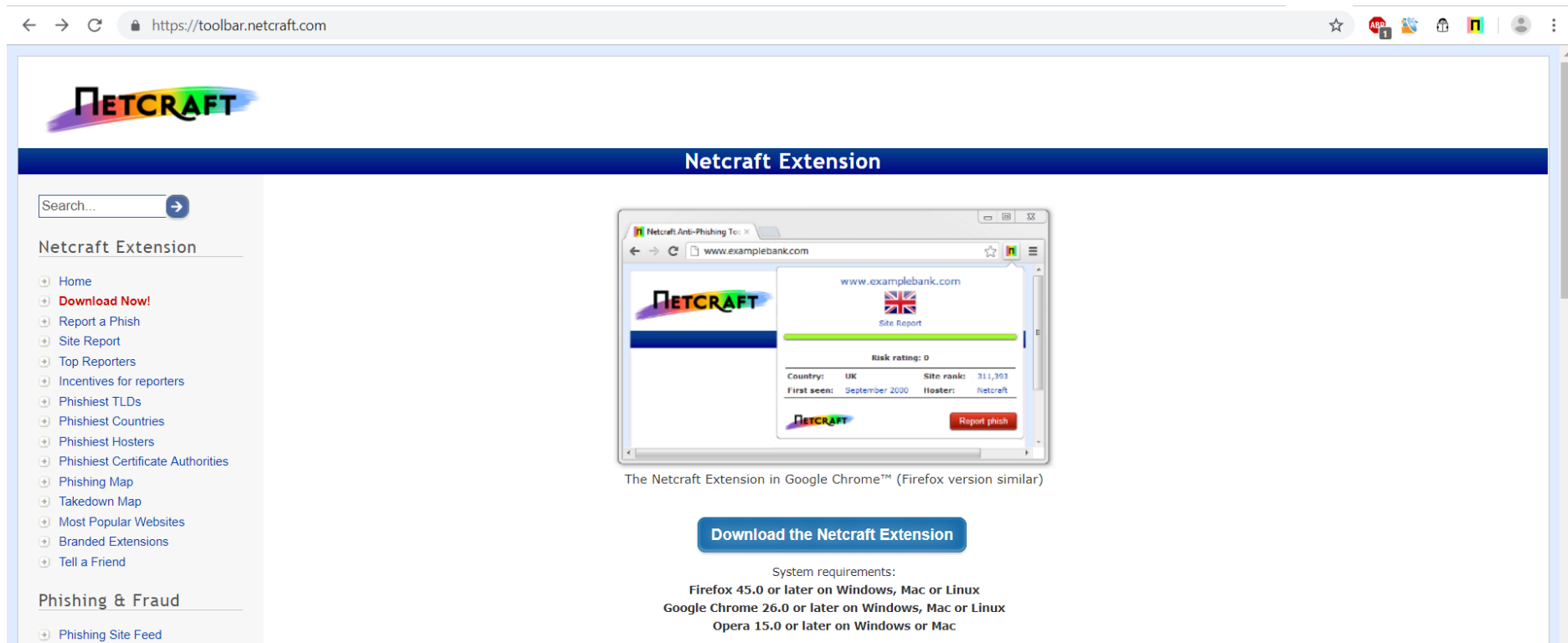
You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. [privacytools.io](https://www.privacytools.io) provides services, tools and knowledge to protect your privacy against global mass surveillance.

Try [search.privacytools.io](https://search.privacytools.io), a Privacy-Respecting Search Engine [start search](#)

# Tools for Security & Privacy

- Secure yourself against phishing attack

<https://toolbar.netcraft.com/>



The screenshot shows the Netcraft website interface. At the top, the Netcraft logo is displayed. Below it, a dark blue banner reads "Netcraft Extension". On the left side, there is a search bar and a navigation menu with the following items: Home, Download Now!, Report a Phish, Site Report, Top Reporters, Incentives for reporters, Phishiest TLDs, Phishiest Countries, Phishiest Hosters, Phishiest Certificate Authorities, Phishing Map, Takedown Map, Most Popular Websites, Branded Extensions, Tell a Friend, Phishing & Fraud, and Phishing Site Feed. The main content area features a preview of the Netcraft Anti-Phishing Tool in a browser window. The browser window shows the URL "www.examplebank.com" and a "Site Report" for the same domain. The report includes a "Risk rating: 0", "Country: UK", "Site rank: 311,363", "First seen: September 2000", and "Hosters: Netcraft". A "Report phish" button is visible at the bottom right of the report. Below the browser preview, the text reads "The Netcraft Extension in Google Chrome™ (Firefox version similar)". At the bottom center, there is a blue button labeled "Download the Netcraft Extension". Below the button, the system requirements are listed: "System requirements: Firefox 45.0 or later on Windows, Mac or Linux; Google Chrome 26.0 or later on Windows, Mac or Linux; Opera 15.0 or later on Windows or Mac".

Search...

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed

Netcraft Anti-Phishing Tool

www.examplebank.com

Site Report

Risk rating: 0

Country: UK Site rank: 311,363

First seen: September 2000 Hosters: Netcraft

Report phish

The Netcraft Extension in Google Chrome™ (Firefox version similar)

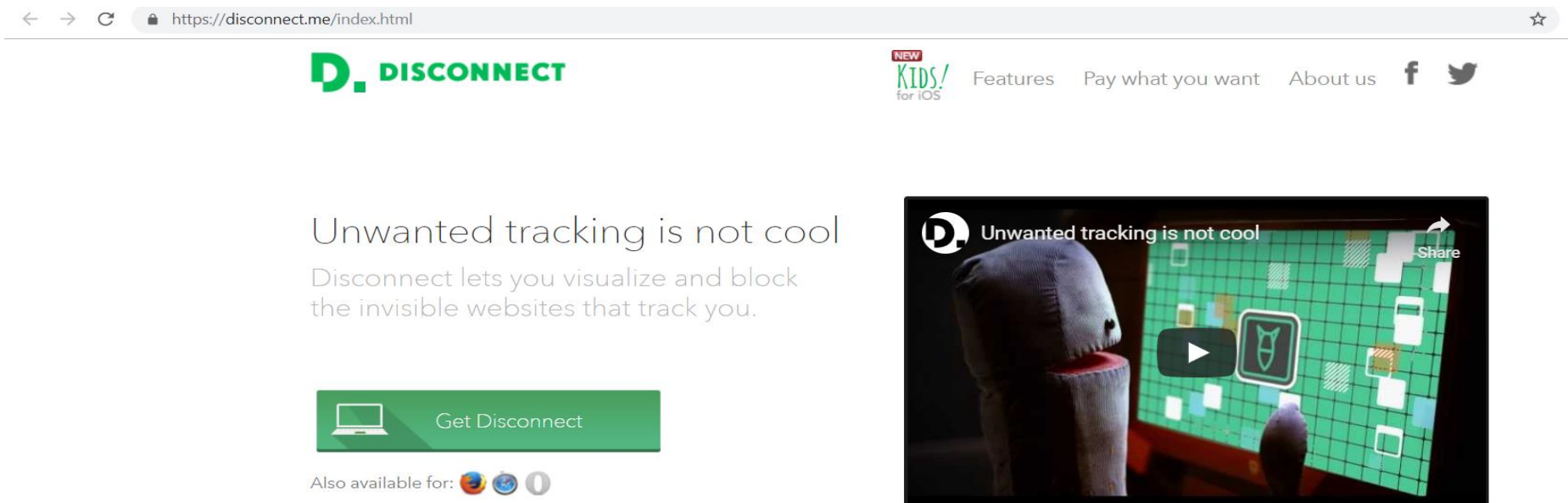
[Download the Netcraft Extension](#)

System requirements:  
Firefox 45.0 or later on Windows, Mac or Linux  
Google Chrome 26.0 or later on Windows, Mac or Linux  
Opera 15.0 or later on Windows or Mac

# Tools for Security & Privacy

- Secure yourself against tracking attack

<https://disconnect.me/index.html>



The screenshot shows the homepage of the Disconnect website. At the top, there is a navigation bar with the Disconnect logo on the left, a 'NEW KIDS! for iOS' badge, and links for 'Features', 'Pay what you want', and 'About us'. Social media icons for Facebook and Twitter are also present. The main content area features the headline 'Unwanted tracking is not cool' and a sub-headline 'Disconnect lets you visualize and block the invisible websites that track you.' Below this is a green button labeled 'Get Disconnect' with a laptop icon. Underneath the button, it says 'Also available for:' followed by icons for Chrome, Firefox, and Safari. On the right side of the page, there is a video player with a play button and a 'Share' icon. The video thumbnail shows a character looking at a screen displaying a grid of various website icons.

Next video: [How Disconnect works](#)



## Speed

Load the pages you go to an average of 27% faster.



## Privacy

Stop 2,000+ third-party sites from tracking you.



## Security

Encrypt the data you share with popular sites.

# Tools for Security & Privacy

- Secure your router against cyber attack [https://www.f-secure.com/en/web/home\\_global/router-checker](https://www.f-secure.com/en/web/home_global/router-checker)

F-Secure Corporation [FI] | [https://www.f-secure.com/en/web/home\\_global/router-checker](https://www.f-secure.com/en/web/home_global/router-checker)

F-Secure

For home For business For partners Global

Products Free tools Support Download Buy or renew Try for free My F-Secure

## F-SECURE ROUTER CHECKER

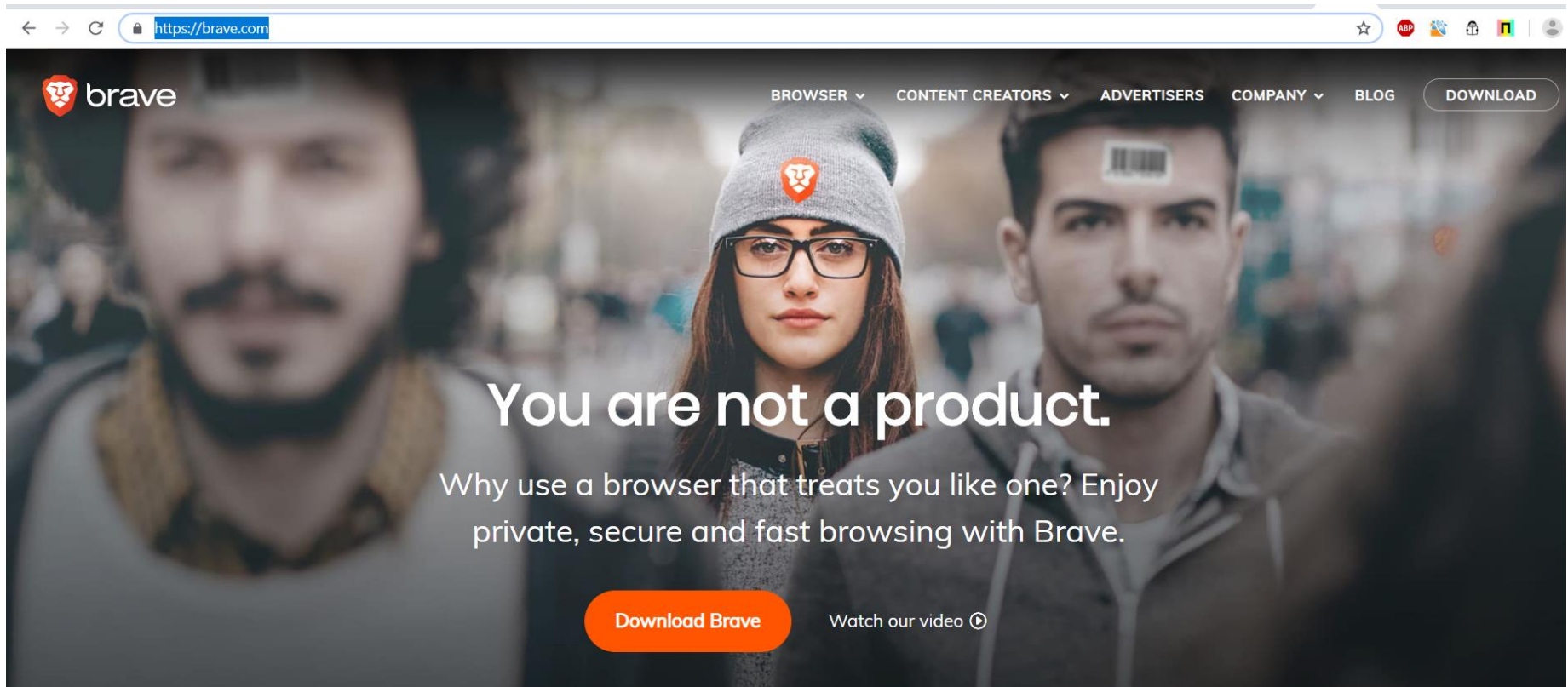
The F-Secure Router Checker is a free and instant way to see if your router has potentially been hijacked by criminals

[Check your router](#)

✓ No issues were found on your router. [View results in detail.](#)

# Tools for Security & Privacy

- Use Brave Browser for secure against tracking attack <https://brave.com/>



The image shows a screenshot of the Brave browser website homepage. The browser's address bar at the top displays "https://brave.com". The website features a navigation menu with links for "BROWSER", "CONTENT CREATORS", "ADVERTISERS", "COMPANY", and "BLOG", along with a "DOWNLOAD" button. The main visual is a woman in a grey beanie with the Brave logo, standing in a crowd. The headline reads "You are not a product." followed by the text "Why use a browser that treats you like one? Enjoy private, secure and fast browsing with Brave." At the bottom, there is an orange "Download Brave" button and a "Watch our video" link with a play icon.

# Threat Intel Map

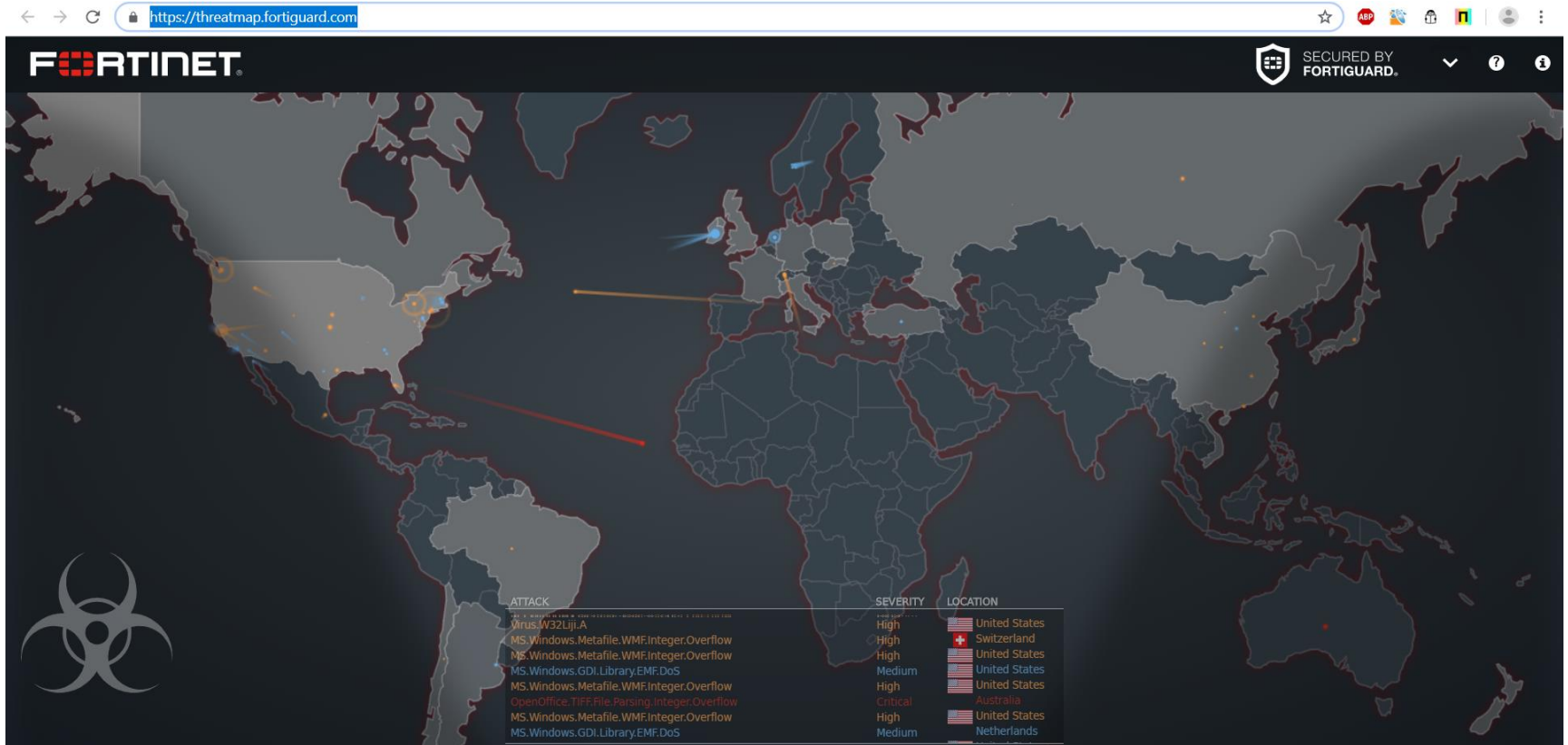
- Update your knowledge and real time intelligence via cyber threat maps <https://www.fireeye.com/cyber-map/threat-map.html>





# Threat Intel Map

- Update your knowledge and real time intelligence via cyber threat maps  
<https://threatmap.fortiguard.com/>



# Tools for Device Security & Privacy

- For Android Device following apps can be used to safeguard your privacy

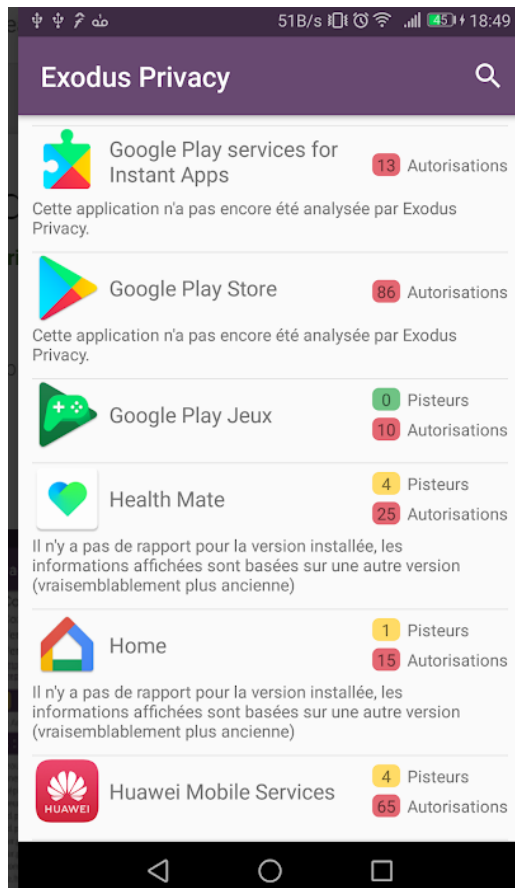


## HACKUNA (Anti-Hack)

- Can block and detect WiFi hackers
- Can also track the hackers within the area.
- It will give you all the details you need to find the hacker within the area or to report it to the authority

# Tools for Device Security & Privacy

- For Android Device following apps can be used to safeguard your privacy



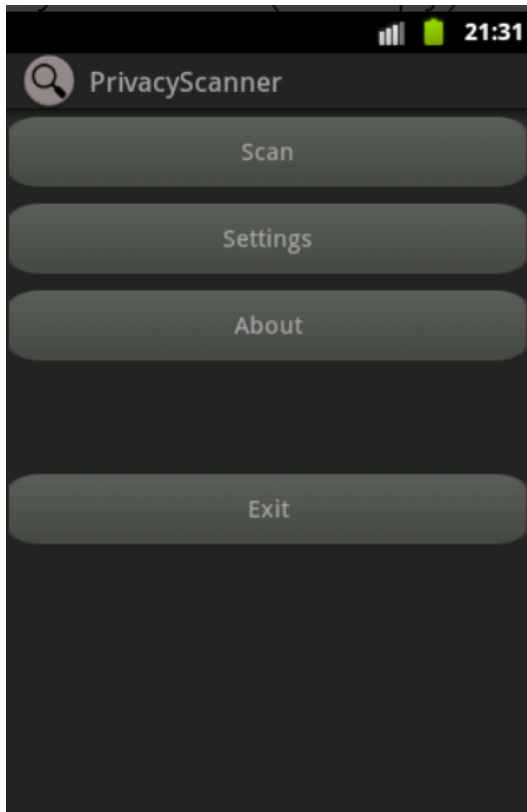
## Exodus Privacy

Exodus Privacy helps you to know which trackers and permissions are embedded in apps installed on your device.

The app downloads reports from Exodus Privacy (<https://exodus-privacy.eu.org/>) and shows them to you app by app

# Tools for Device Security & Privacy

- For Android Device following apps can be used to safeguard your privacy

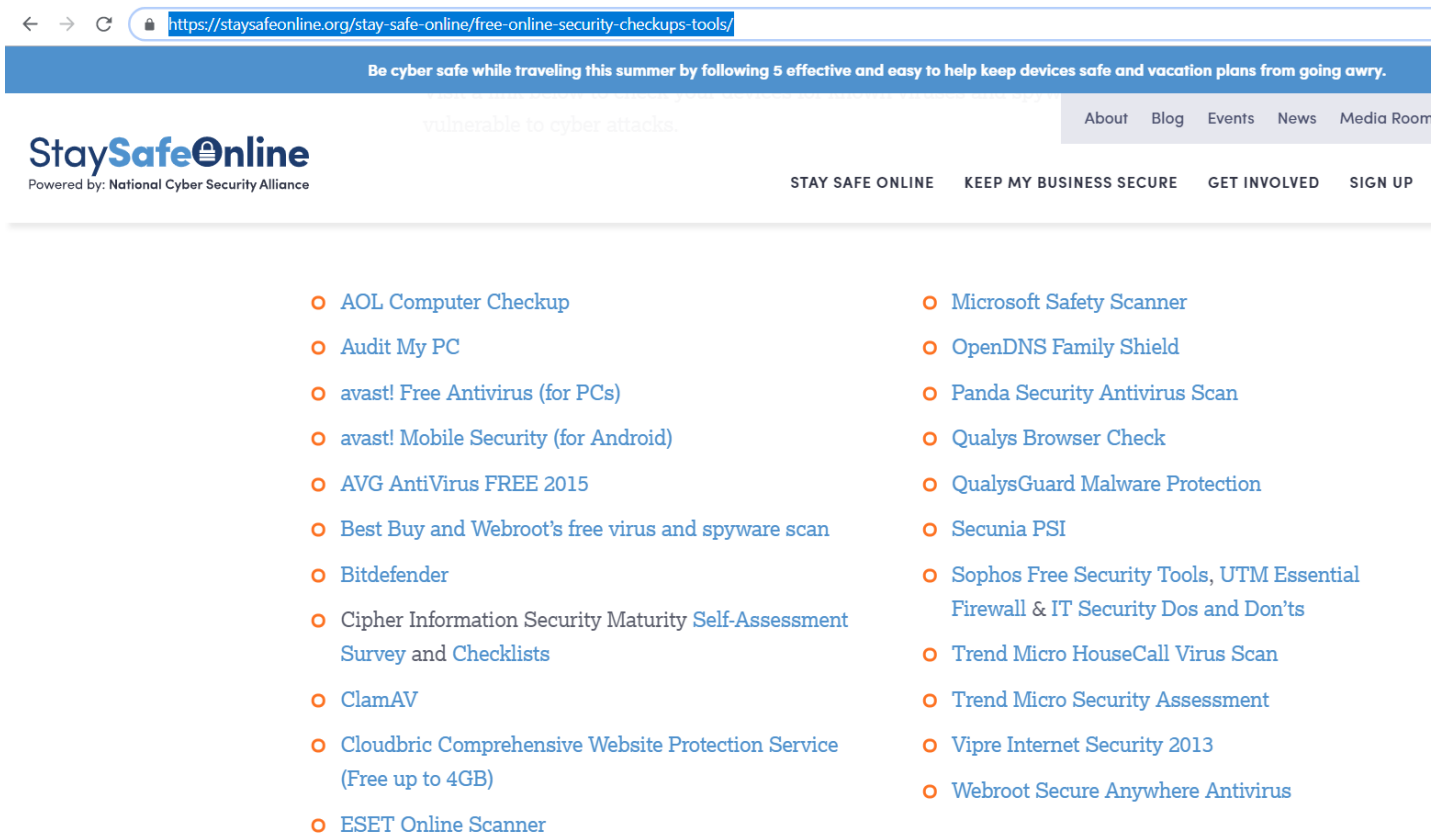


## Privacy Scanner (AntiSpy) Free

Privacy Scanner Anti Spy was created to check your smartphone whether you are really being spied on. It detects Parental Control and surveillance apps, which might be misused to spy on spouses, using GPS-Track technologies, receive and send sms, read your contacts, read your call history, reads your calendar and so on...

# Tools for Device Security & Privacy

- For PC following apps can be used to safeguard your privacy <https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/>



The screenshot shows the StaySafeOnline website. The browser address bar displays the URL <https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/>. The page header includes the StaySafeOnline logo, the tagline "vulnerable to cyber attacks.", and navigation links for "About", "Blog", "Events", "News", and "Media Room". Below the header, there are four main categories: "STAY SAFE ONLINE", "KEEP MY BUSINESS SECURE", "GET INVOLVED", and "SIGN UP". The main content area features a list of 20 security tools, each with a blue circular icon and a text link.

Be cyber safe while traveling this summer by following 5 effective and easy to help keep devices safe and vacation plans from going awry.

StaySafeOnline  
Powered by: National Cyber Security Alliance

About Blog Events News Media Room

STAY SAFE ONLINE KEEP MY BUSINESS SECURE GET INVOLVED SIGN UP

- AOL Computer Checkup
- Audit My PC
- avast! Free Antivirus (for PCs)
- avast! Mobile Security (for Android)
- AVG AntiVirus FREE 2015
- Best Buy and Webroot's free virus and spyware scan
- Bitdefender
- Cipher Information Security Maturity Self-Assessment Survey and Checklists
- ClamAV
- Cloudbric Comprehensive Website Protection Service (Free up to 4GB)
- ESET Online Scanner
- Microsoft Safety Scanner
- OpenDNS Family Shield
- Panda Security Antivirus Scan
- Qualys Browser Check
- QualysGuard Malware Protection
- Secunia PSI
- Sophos Free Security Tools, UTM Essential Firewall & IT Security Dos and Don'ts
- Trend Micro HouseCall Virus Scan
- Trend Micro Security Assessment
- Vipre Internet Security 2013
- Webroot Secure Anywhere Antivirus

Your Suggestions are always welcomed

Thanking you