Sun City Computer Club

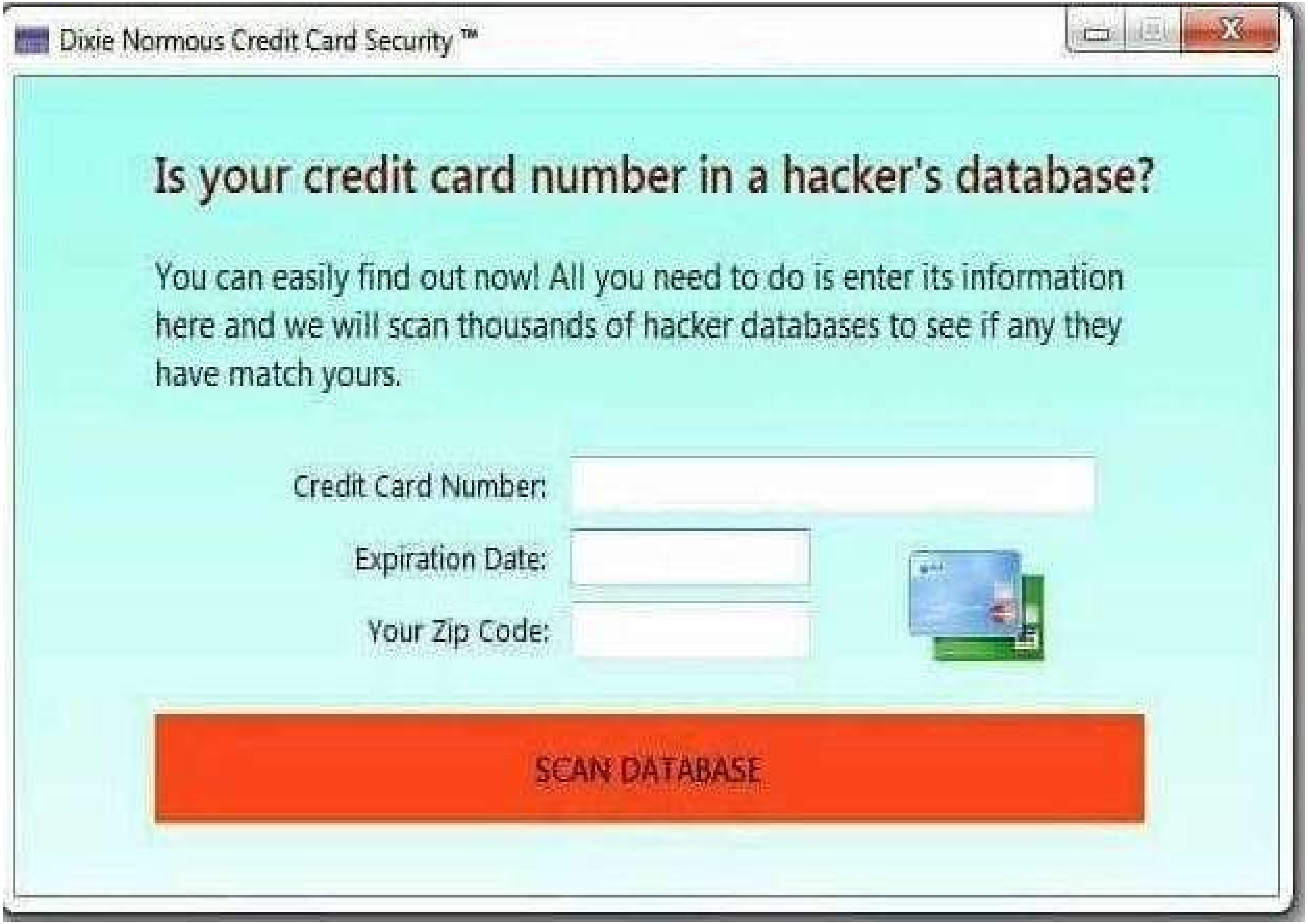
Safer WEB Browsing

Part One

- Audio Recording of this session
- Use the link above to access MP4 audio recording

- Audio Recording in Progress

- SIG attendees are required to be members of the chartered club sponsoring that SIG.
- Sun City Community Association By-law



Dixie Normous Credit Card Security ™

Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

Credit Card Number:

Expiration Date:

Your Zip Code:

Covid-19

- FBI fraud reports up way up
- Covid-19 domain registrations
- Cyber attacks against healthcare
- “They” are sheltered at home and bored and hungry
- Ransomware -> fraud, scams, attacks

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

- Any length
- Any time
- Any schedule
- Timeliness
- Pause and continue
- Pause and look up for clarity
- Skip over
- Play again and again
- Adjust video size
- Adjust audio level
- Available to new users Months from now

Advantages to PowerPoint delivery

- Presentations
- SIGs
- Newsletters
- Wiki
- Help Center
- First Time
- Classes

Sun City Computer Club Resources

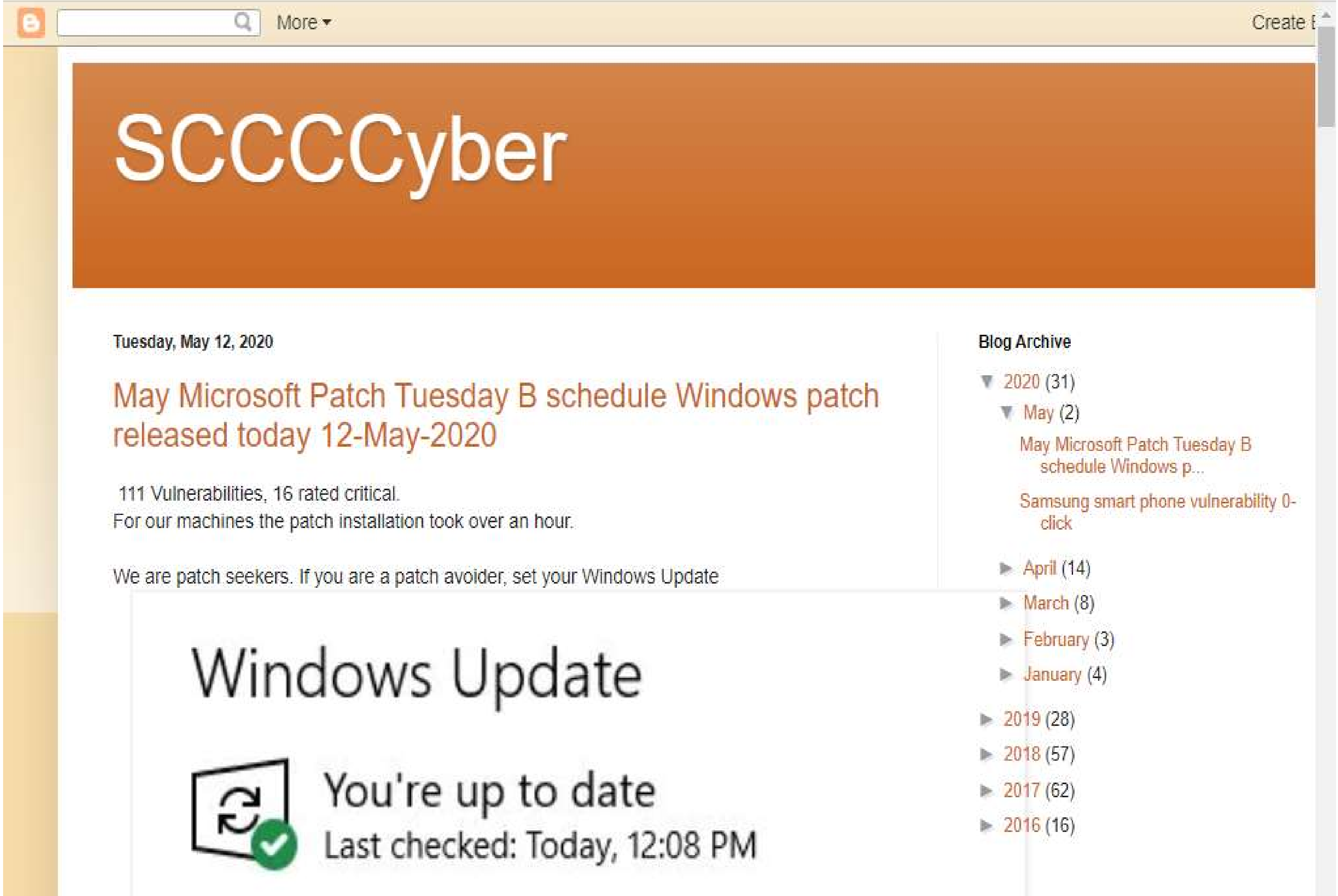
Cyber Security SIG

- Bimonthly presentations Audio recorded
- Classes

    Computer and Information Security

    Cyber War

    Safer Browsing
- Cyber Security News 196 Searchable
- News -> timely



SCCCyber

Tuesday, May 12, 2020

May Microsoft Patch Tuesday B schedule Windows patch released today 12-May-2020

111 Vulnerabilities, 16 rated critical.
For our machines the patch installation took over an hour.

We are patch seekers. If you are a patch avoider, set your Windows Update

Windows Update

You're up to date
Last checked: Today, 12:08 PM

Blog Archive

- ▼ 2020 (31)
  - ▼ May (2)
    - May Microsoft Patch Tuesday B schedule Windows p...
    - Samsung smart phone vulnerability 0-click
  - ► April (14)
  - ► March (8)
  - ► February (3)
  - ► January (4)
- ► 2019 (28)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)

- First job computing   1962
- 9 years semi-conductor manufacturer
- 30 years Cyber engineer Major Oil Co.
- Very early WEB experience
- 3 years Alyeska Pipeline
- Major Cyber Security Certifications
- Network of cyber professionals
- Computer Club presentations
- Cyber Security SIG
- Windows SIG

What does John know

Fundamental Issues

- Trust
- Convenience

- FOMO
- Curiosity

- Now any/everyone can have a voice

WEB issues

- Connectionless
- Not intended for current use
- Query & Response
- Client / Server

  either can run code on the other
- Any/everything apps, attachments, audio, video
- Interpreters/helpers
- ActiveX, Java, scripts, shells

WEB Issues

- HTTP
- HTML
- Akamai, cloud
- Increased use of third party services
- What, me worry?
- Information gives no indication of being stolen
- Information is cumulative

Journey to the Web site

- Name resolution

  Own name, Hosts file, NetBIOS, DNS

- Domain Name System

  Distributed, hierarchical, caching database

  No authentication

- BGP

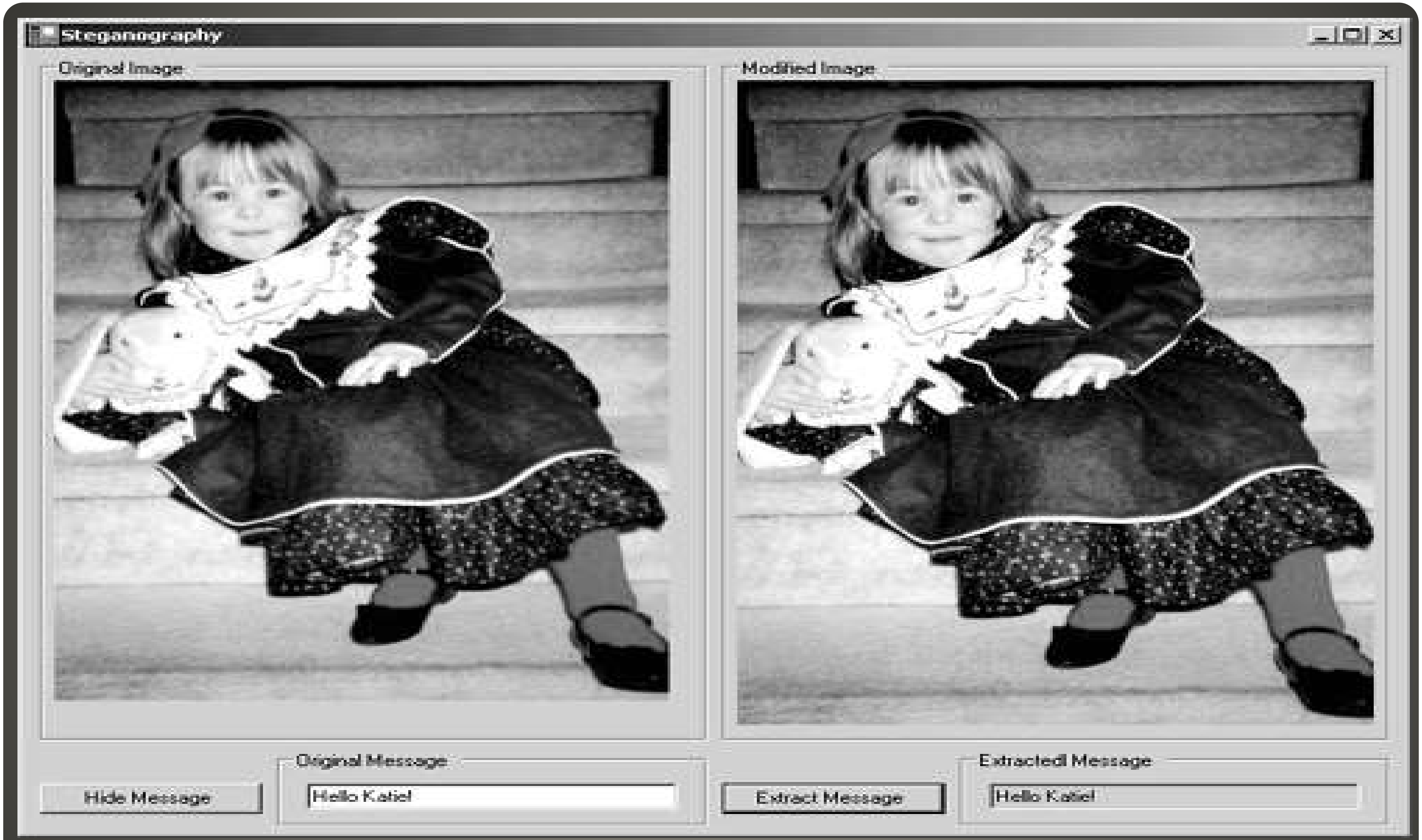
  routing, No authentication

cryptography

- 1-2-3-4
- Steganography
- Hash
- Symmetric
- Asymmetric

- 1-2-3-4
- Algorithm
- Key
- Plain text
- Cypher text

cryptography



Original Message: Hello Katie!

Extracted Message: Hello Katie!

Steganography

hash

- One way
- Fixed length output
- Any length input
- Message digests
- E.g. MD2,MD4,MD5,SHA-1,SHA-2
- Used for integrity, digital signing & passphrases

symmetric

- plain text > algorithm + key > cypher text
- cypher text > algorithm + key > plain text
- Algorithm usually public
- Key space is important larger is better
- Reversible with the one key
- Does not scale
- E.g. RC4,SEAL DES,3DES,RC5,Rijndael
- One-time pad
- Cryptanalysis
- Control

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

CIA

Asymmetric

- Public & private key
- Intractable problem
- Symmetric key exchange in presence of advisory
- Thousands of times slower
- E.g. RSA, El Gamal, ECC
- Public key distributed and verified via Digital Certificate
- Signing via digital signature

Uses of cryptography

- Code signing
- VPN
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Disk and file encryption
- IPSec
- PKI
- blockchain

- Client hello
- Server hello
- Client validation and pre-master secret
- Both sides use secret to generate session key(s)
- Web session proceeds with data in transit encrypted with symmetric key(s)
- HTTPS layered on SSL or TLS

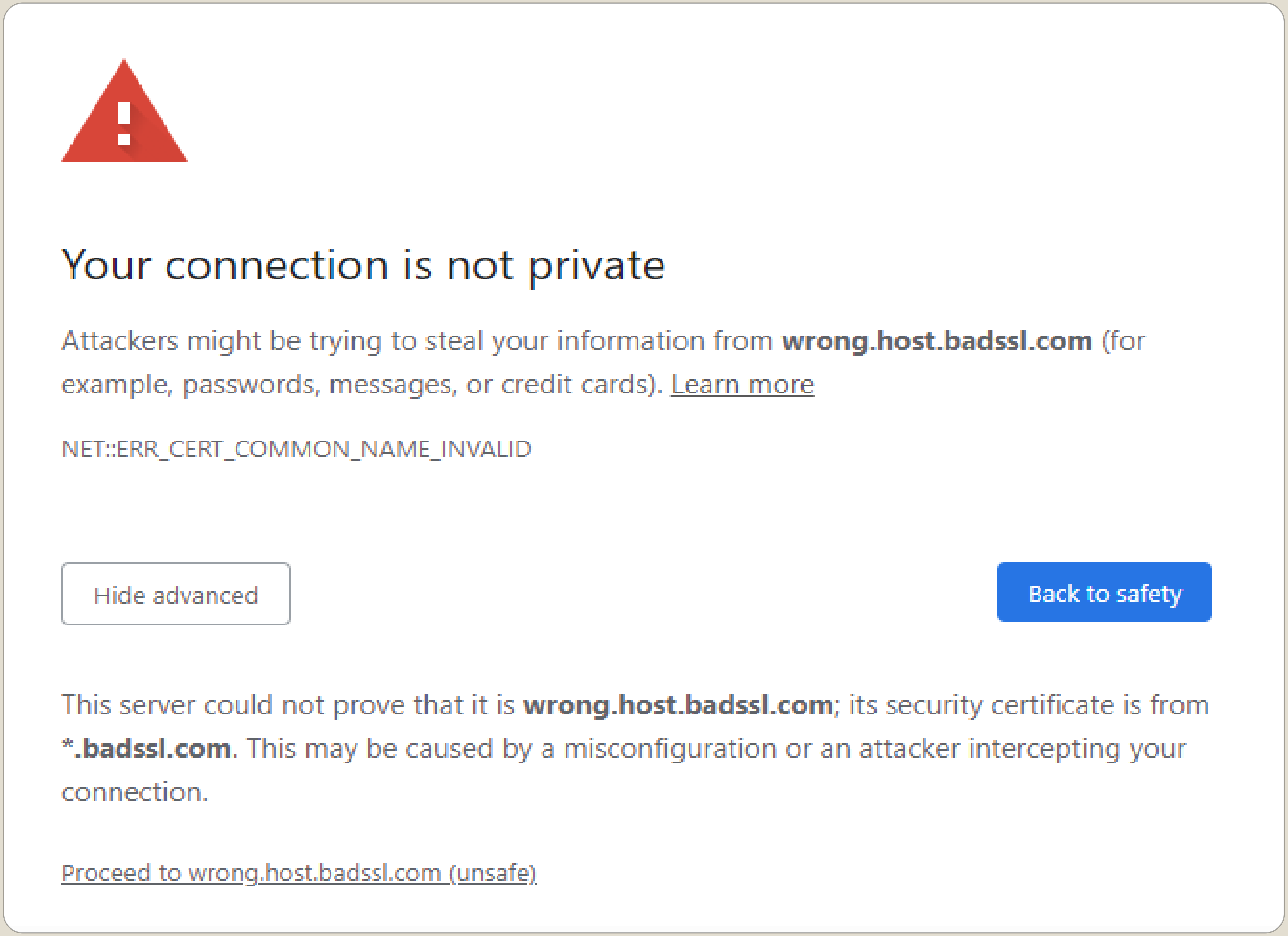
Some detail

- Part of PKI
- Binding of public key to entity
- Verified and signed by certificate authority
- Chain of trust
- X.509

Digital Certificates

WEB transit security

- SSL TLS
- Asymmetric used to exchange symmetric key
- SSL 3.0
- TLS 1.0, 1.1, 1.2, 1.3



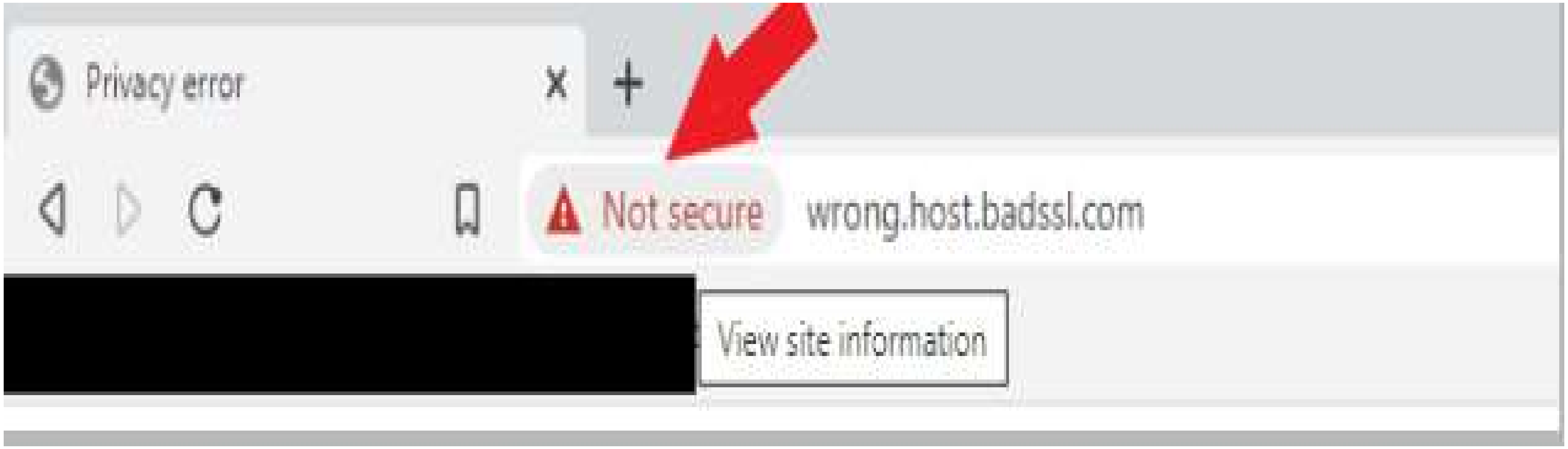
Your connection is not private

Attackers might be trying to steal your information from **wrong.host.badssl.com** (for example, passwords, messages, or credit cards). Learn more

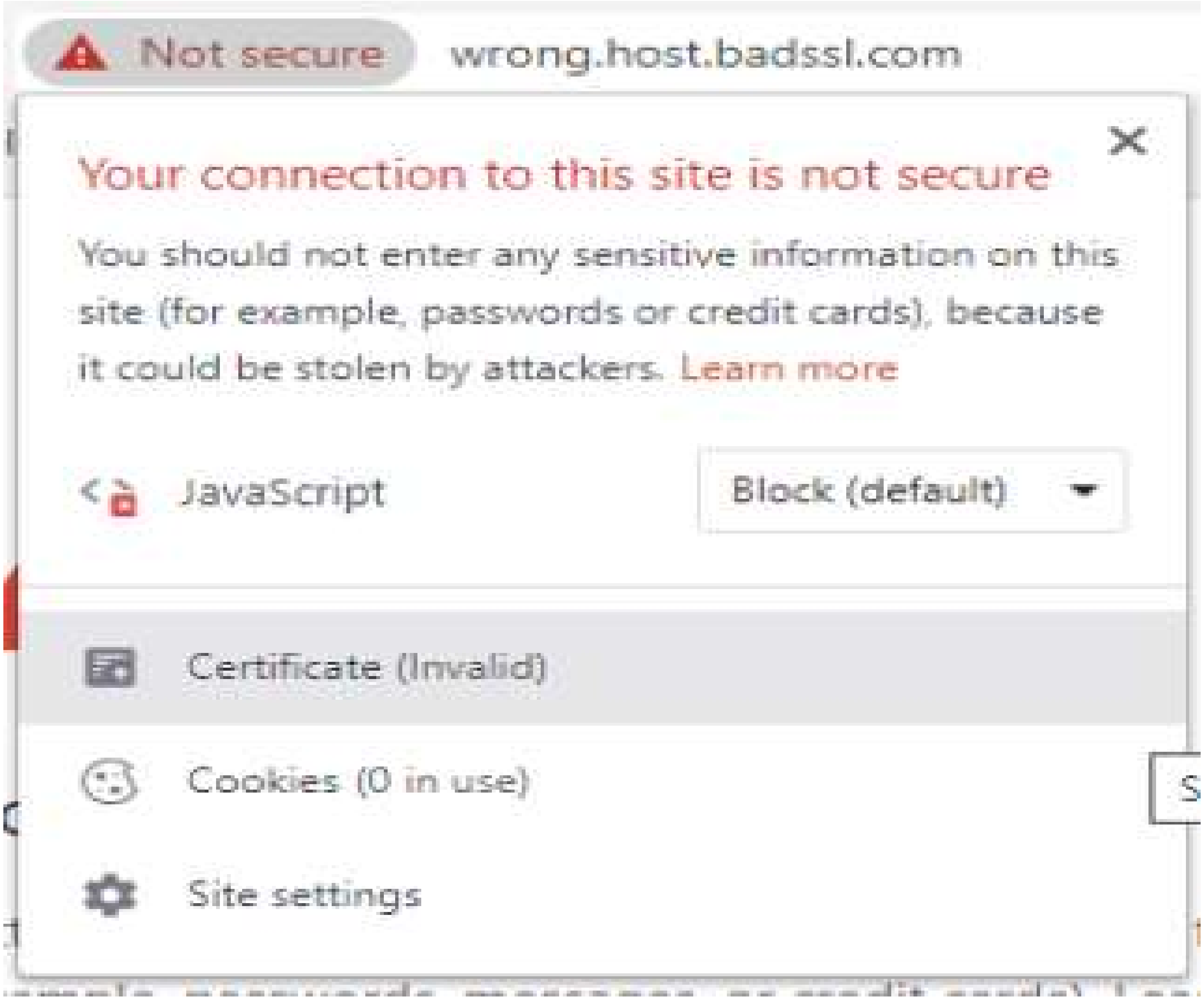
NET::ERR_CERT_COMMON_NAME_INVALID

This server could not prove that it is **wrong.host.badssl.com**; its security certificate is from ***.badssl.com**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to wrong.host.badssl.com (unsafe)


Privacy error
Not secure
wrong.host.badssl.com
View site information

[redacted]



Not secure wrong.host.badssl.com

Your connection to this site is not secure

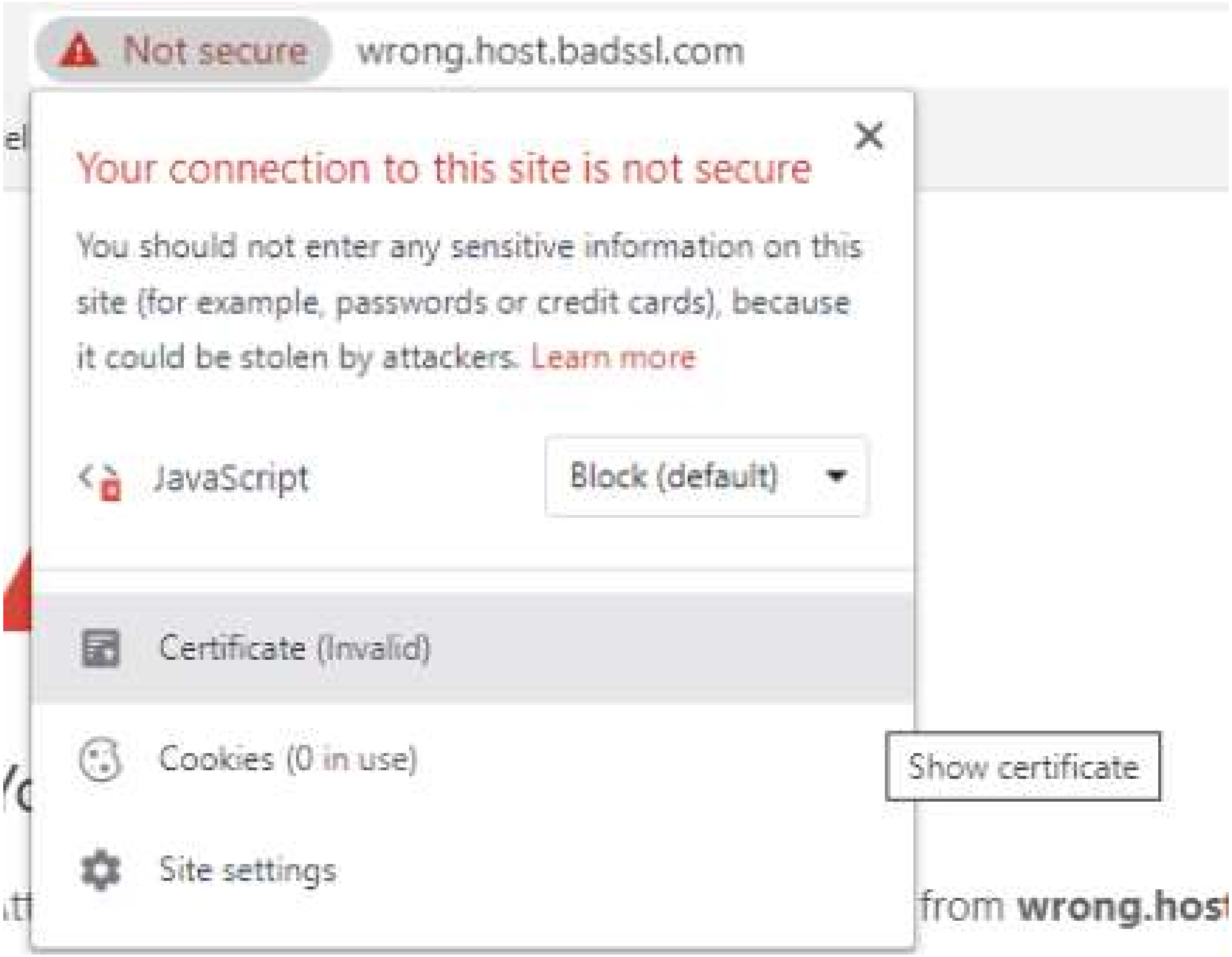
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

JavaScript Block (default)

Certificate (Invalid)

Cookies (0 in use)

Site settings

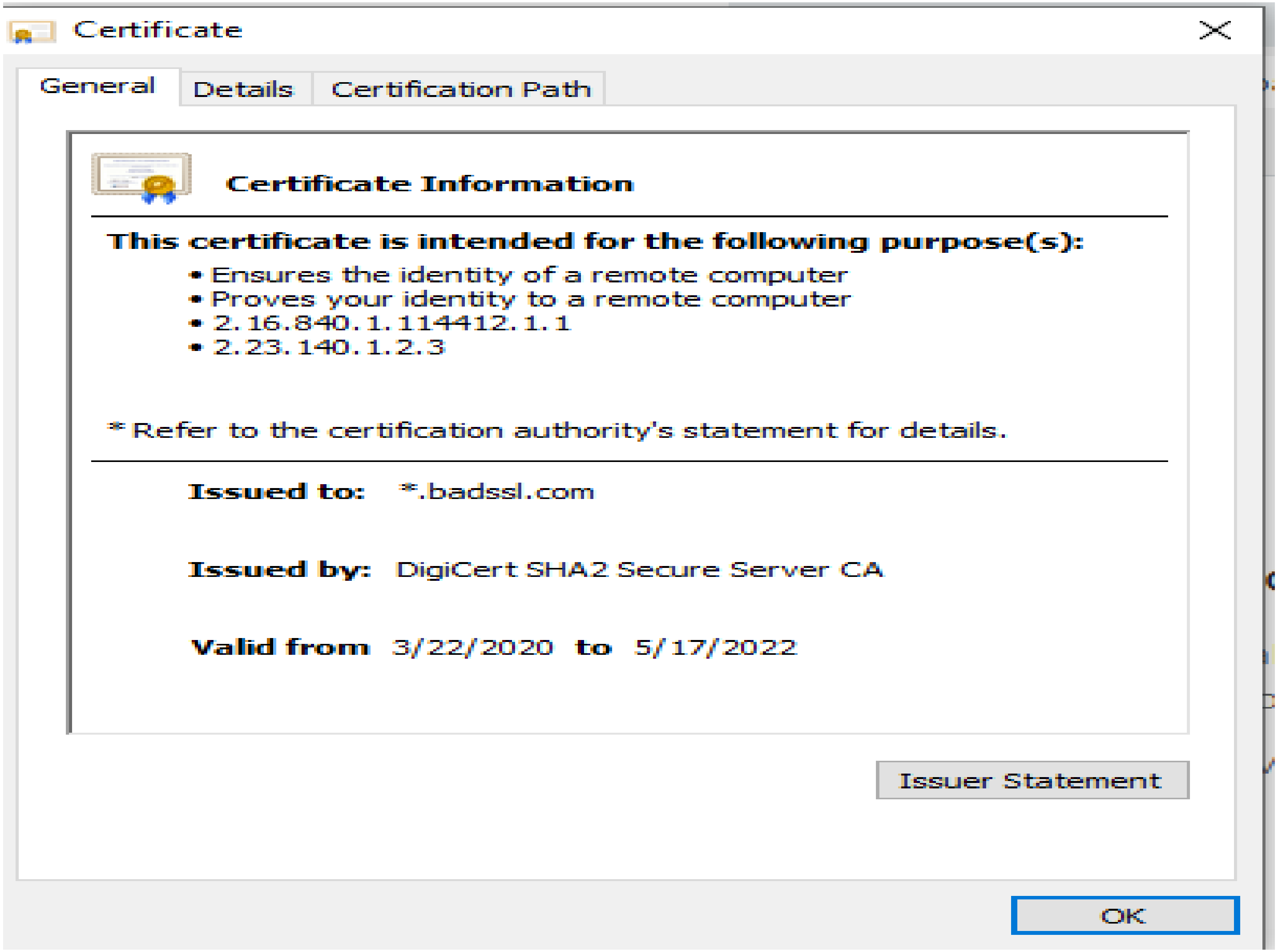


Not secure wrong.host.badssl.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

JavaScript Block (default)



Certificate Information

This certificate is intended for the following purpose(s):

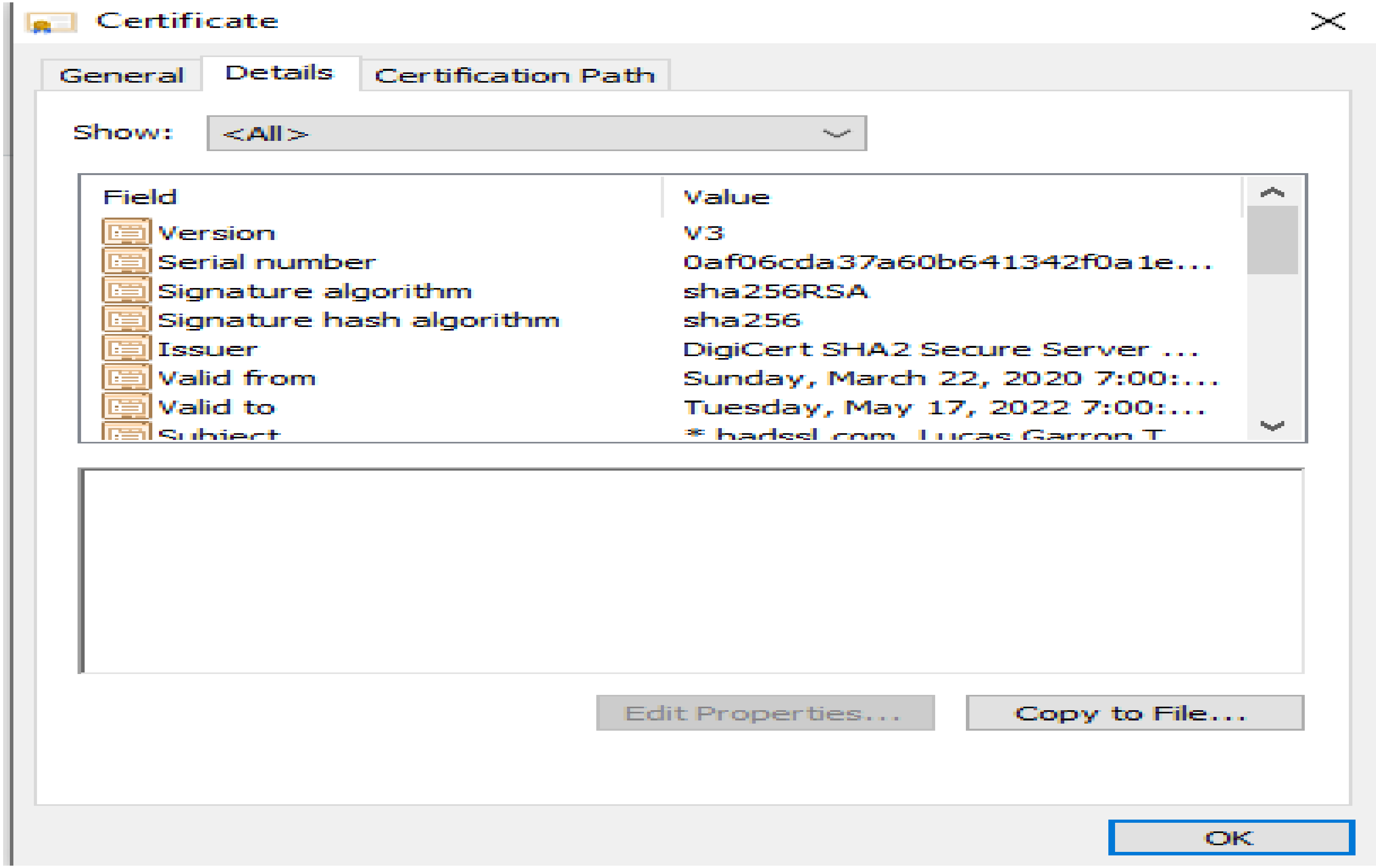
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.3

* Refer to the certification authority's statement for details.

Issued to: *.badssl.com

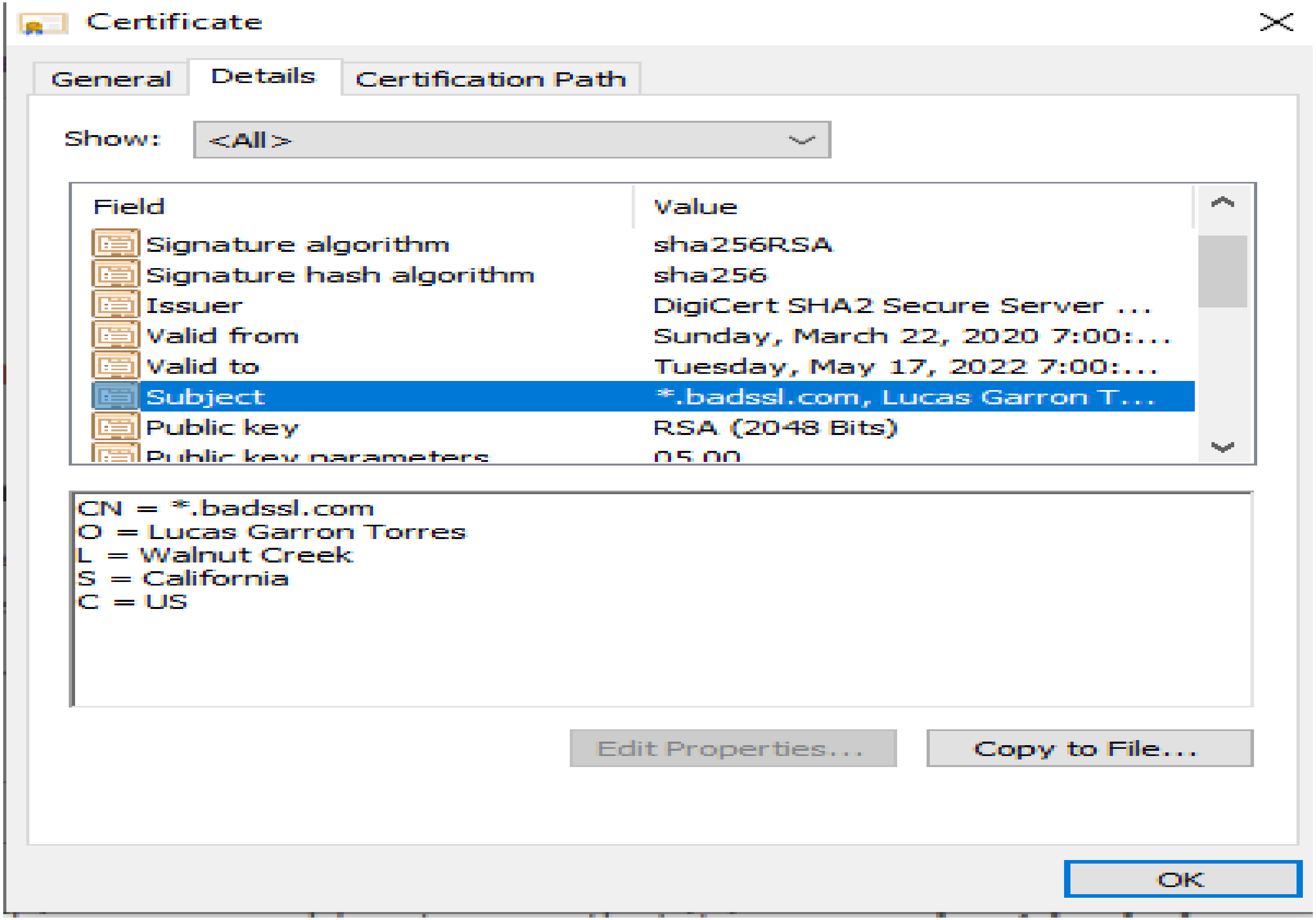
Issued by: DigiCert SHA2 Secure Server CA

Valid from 3/22/2020 **to** 5/17/2022



Show: <All>

Field	Value
Version	V3
Serial number	0af06cda37a60b641342f0a1e...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	Sunday, March 22, 2020 7:00:...
Valid to	Tuesday, May 17, 2022 7:00:...
Subject	*.badssl.com, Lucas Garron T



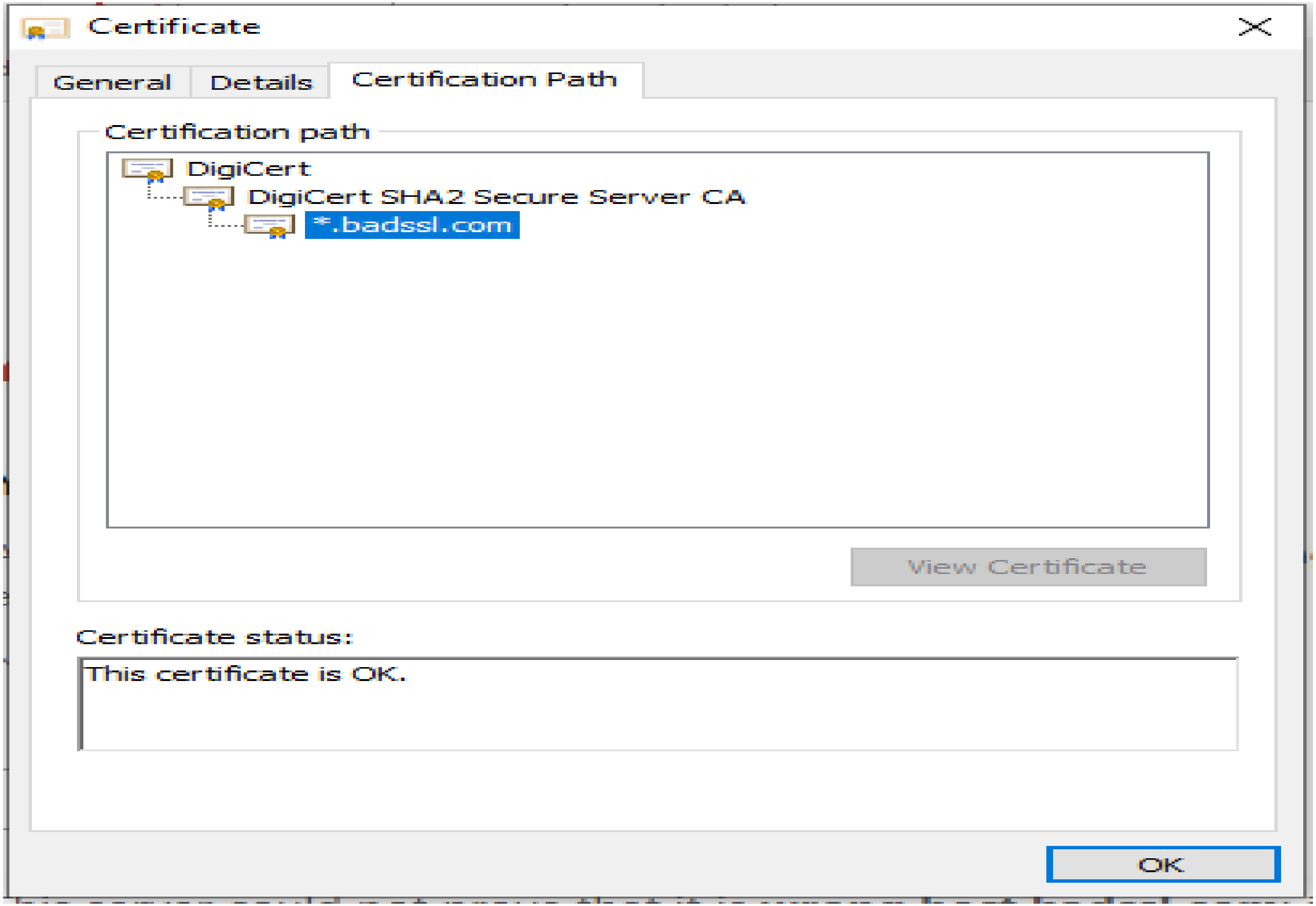
Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	Sunday, March 22, 2020 7:00:...
Valid to	Tuesday, May 17, 2022 7:00:...
Subject	*.badssl.com, Lucas Garron T...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
CN = *.badssl.com
O = Lucas Garron Torres
L = Walnut Creek
S = California
C = US
```

Certificate Issues

- Dates Issue from Issue to
- Signature algorithm Hash algorithm
- Subject



Certification path

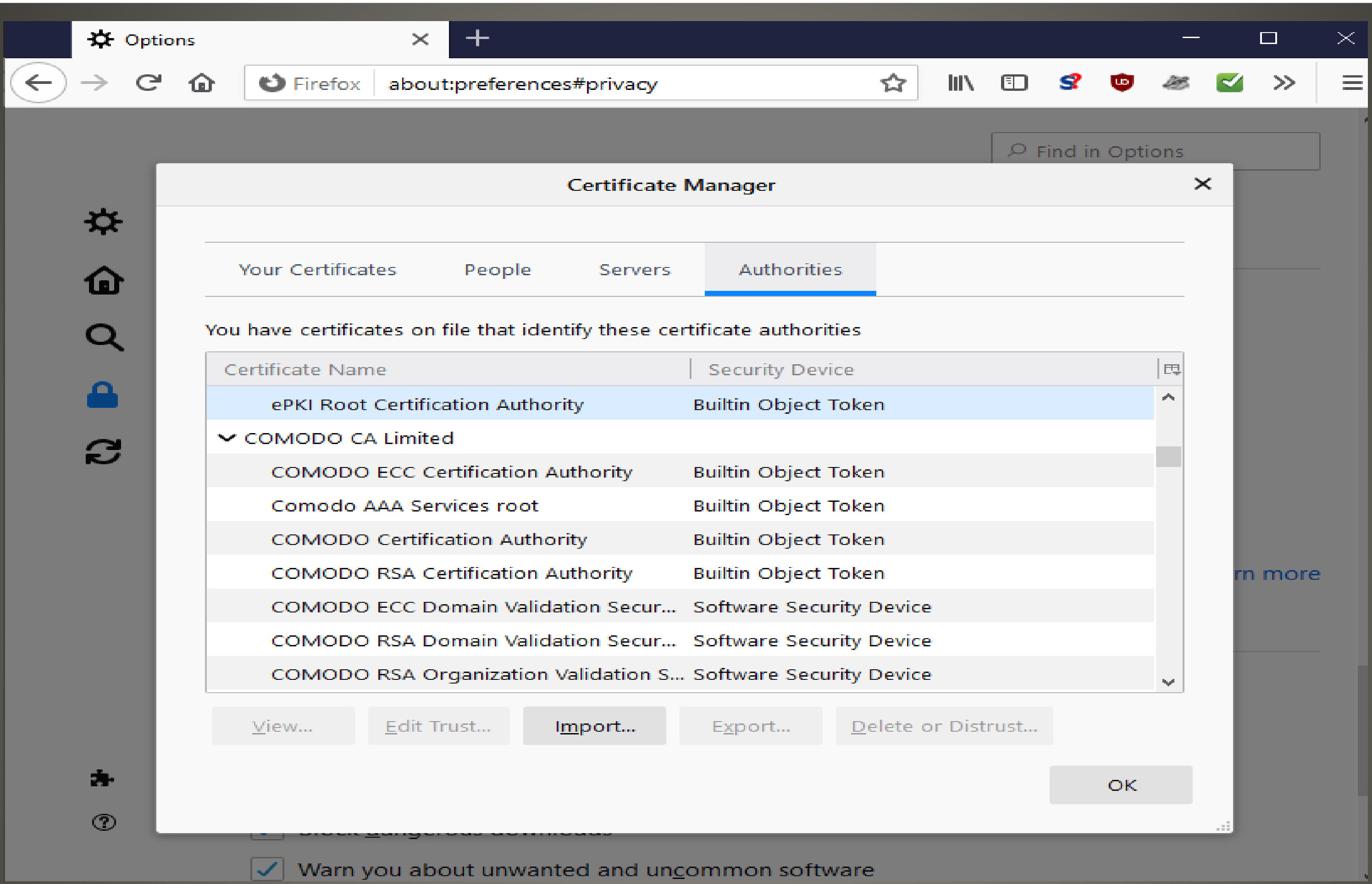
- DigiCert
  - DigiCert SHA2 Secure Server CA
    - *.badssl.com

Certificate status:

This certificate is OK.

- Microsoft, Apple, Mozilla, Android
- ADMINISTRATOR rights & privilege
- Past certificate chain compromises
- Certificate Revocation Lists (CRL)
- Malware can and does manipulate certificate chains
- Chain of Trust
- Certificate binding of Public key to IDentity

Certificate Chain of Trust

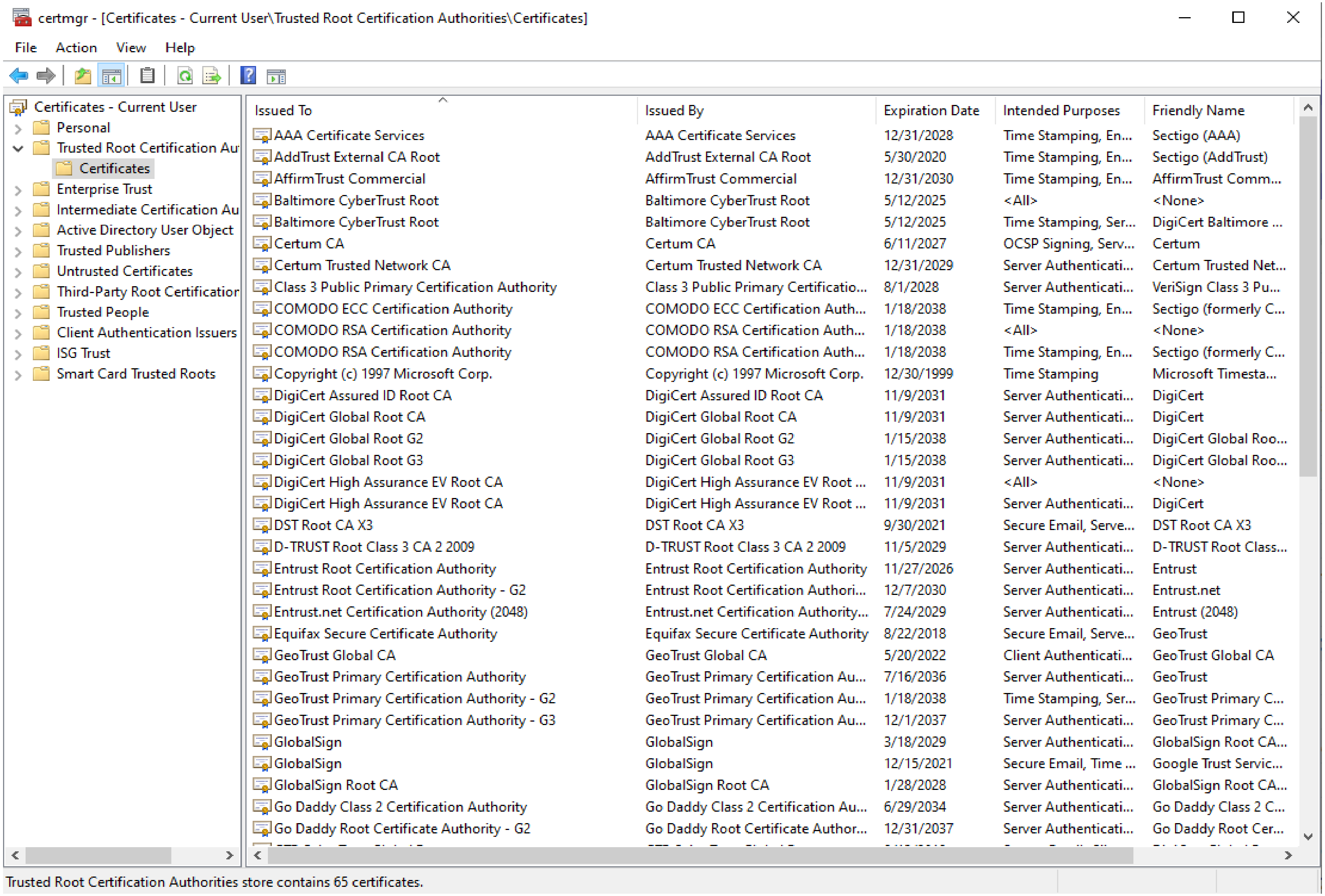


You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
ePKI Root Certification Authority	Builtin Object Token
COMODO CA Limited	
COMODO ECC Certification Authority	Builtin Object Token
Comodo AAA Services root	Builtin Object Token
COMODO Certification Authority	Builtin Object Token
COMODO RSA Certification Authority	Builtin Object Token
COMODO ECC Domain Validation Secur...	Software Security Device
COMODO RSA Domain Validation Secur...	Software Security Device
COMODO RSA Organization Validation S...	Software Security Device

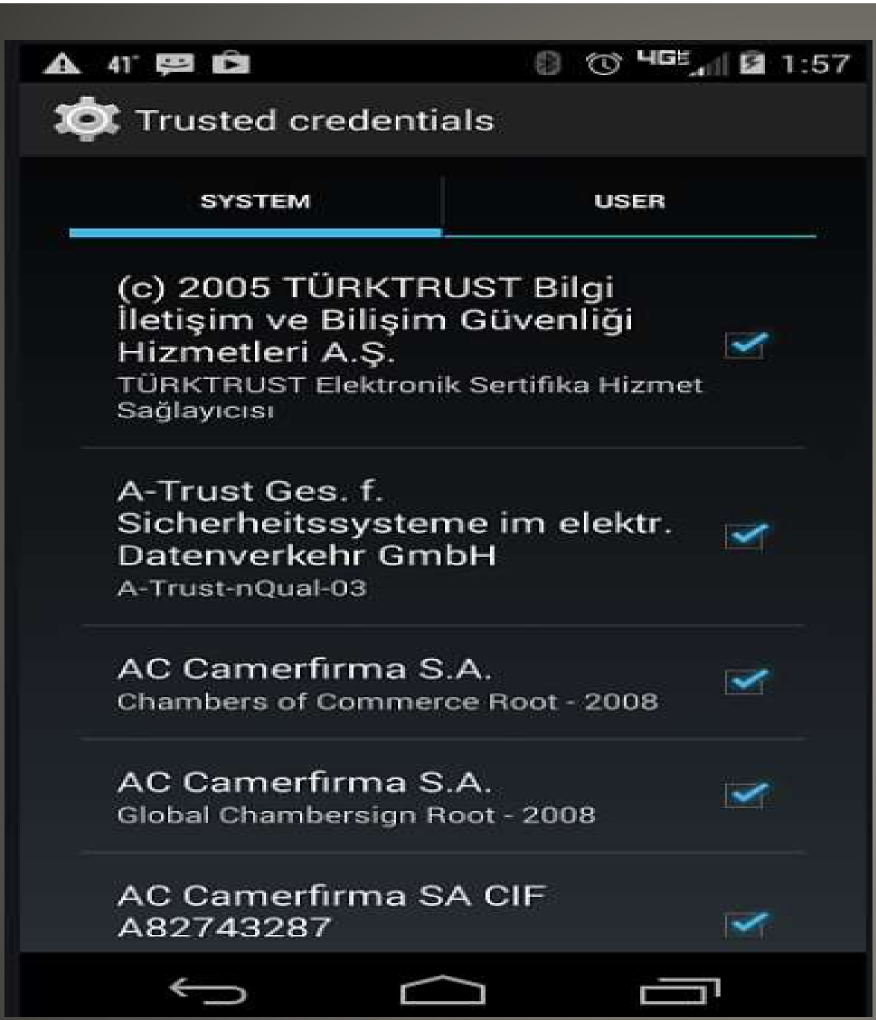
☑ Warn you about unwanted and uncommon software

Mozilla


certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
ISG Trust
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	12/31/2028	Time Stamping, En...	Sectigo (AAA)
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Time Stamping, En...	Sectigo (AddTrust)
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030	Time Stamping, En...	AffirmTrust Comm...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	<All>	<None>
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Time Stamping, Ser...	DigiCert Baltimore ...
Certum CA	Certum CA	6/11/2027	OCSP Signing, Serv...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Certum Trusted Net...
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	8/1/2028	Server Authenticati...	VeriSign Class 3 Pu...
COMODO ECC Certification Authority	COMODO ECC Certification Auth...	1/18/2038	Time Stamping, En...	Sectigo (formerly C...
COMODO RSA Certification Authority	COMODO RSA Certification Auth...	1/18/2038	<All>	<None>
COMODO RSA Certification Authority	COMODO RSA Certification Auth...	1/18/2038	Time Stamping, En...	Sectigo (formerly C...
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticati...	DigiCert Global Roo...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Server Authenticati...	DigiCert Global Roo...
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root ...	11/9/2031	<All>	<None>
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DST Root CA X3
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	11/5/2029	Server Authenticati...	D-TRUST Root Class...
Entrust Root Certification Authority	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust
Entrust Root Certification Authority - G2	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Entrust.net
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Client Authenticati...	GeoTrust Global CA
GeoTrust Primary Certification Authority	GeoTrust Primary Certification Au...	7/16/2036	Server Authenticati...	GeoTrust
GeoTrust Primary Certification Authority - G2	GeoTrust Primary Certification Au...	1/18/2038	Time Stamping, Ser...	GeoTrust Primary C...
GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Au...	12/1/2037	Server Authenticati...	GeoTrust Primary C...
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	GlobalSign Root CA...
GlobalSign	GlobalSign	12/15/2021	Secure Email, Time ...	Google Trust Servic...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign Root CA...
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Author...	12/31/2037	Server Authenticati...	Go Daddy Root Cer...

Trusted Root Certification Authorities store contains 65 certificates.



Trusted credentials

SYSTEM USER

(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı ☑

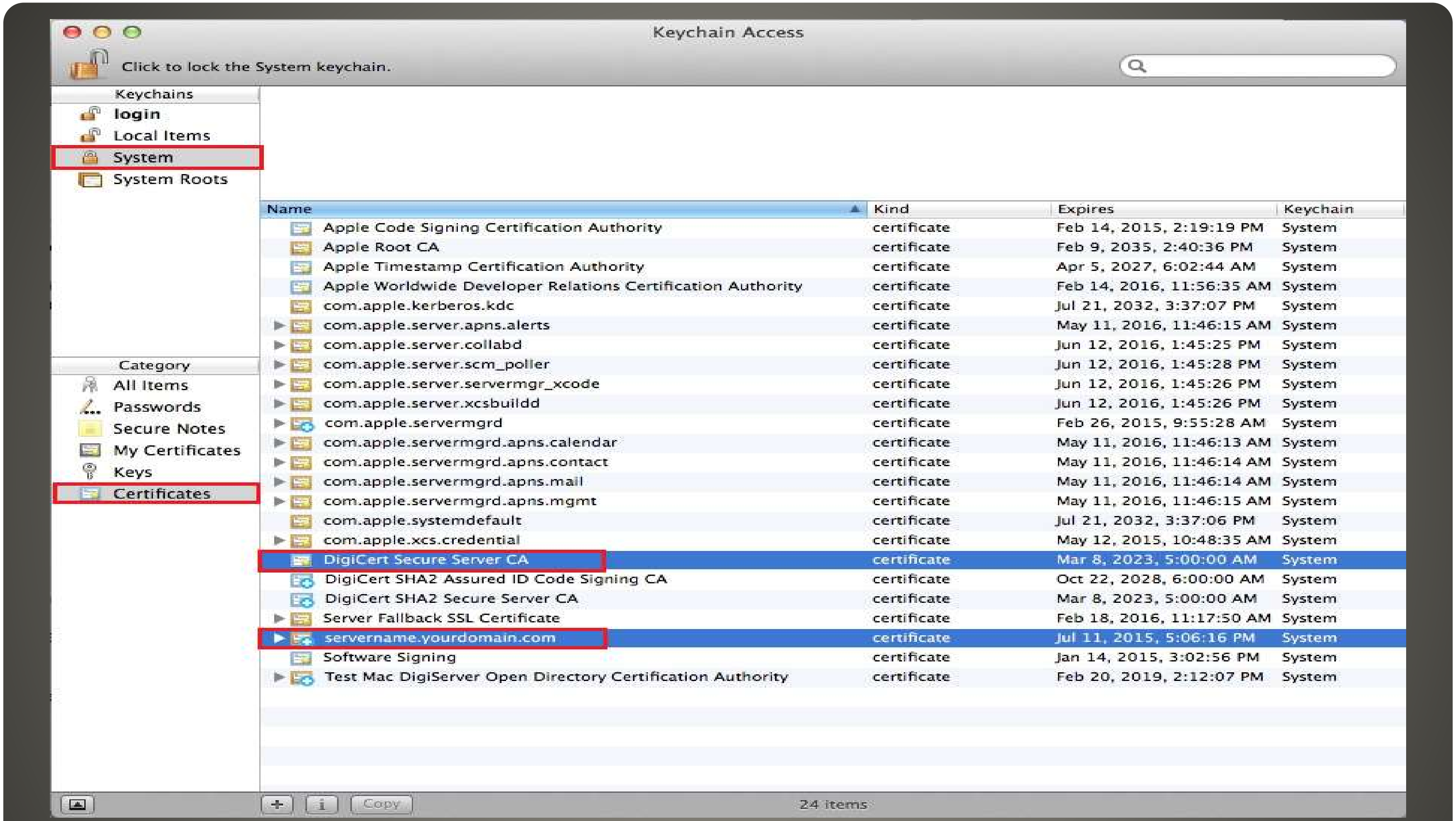
A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
A-Trust-nQual-03 ☑

AC Camerfirma S.A.
Chambers of Commerce Root - 2008 ☑

AC Camerfirma S.A.
Global Chambersign Root - 2008 ☑

AC Camerfirma SA CIF A82743287 ☑

Android

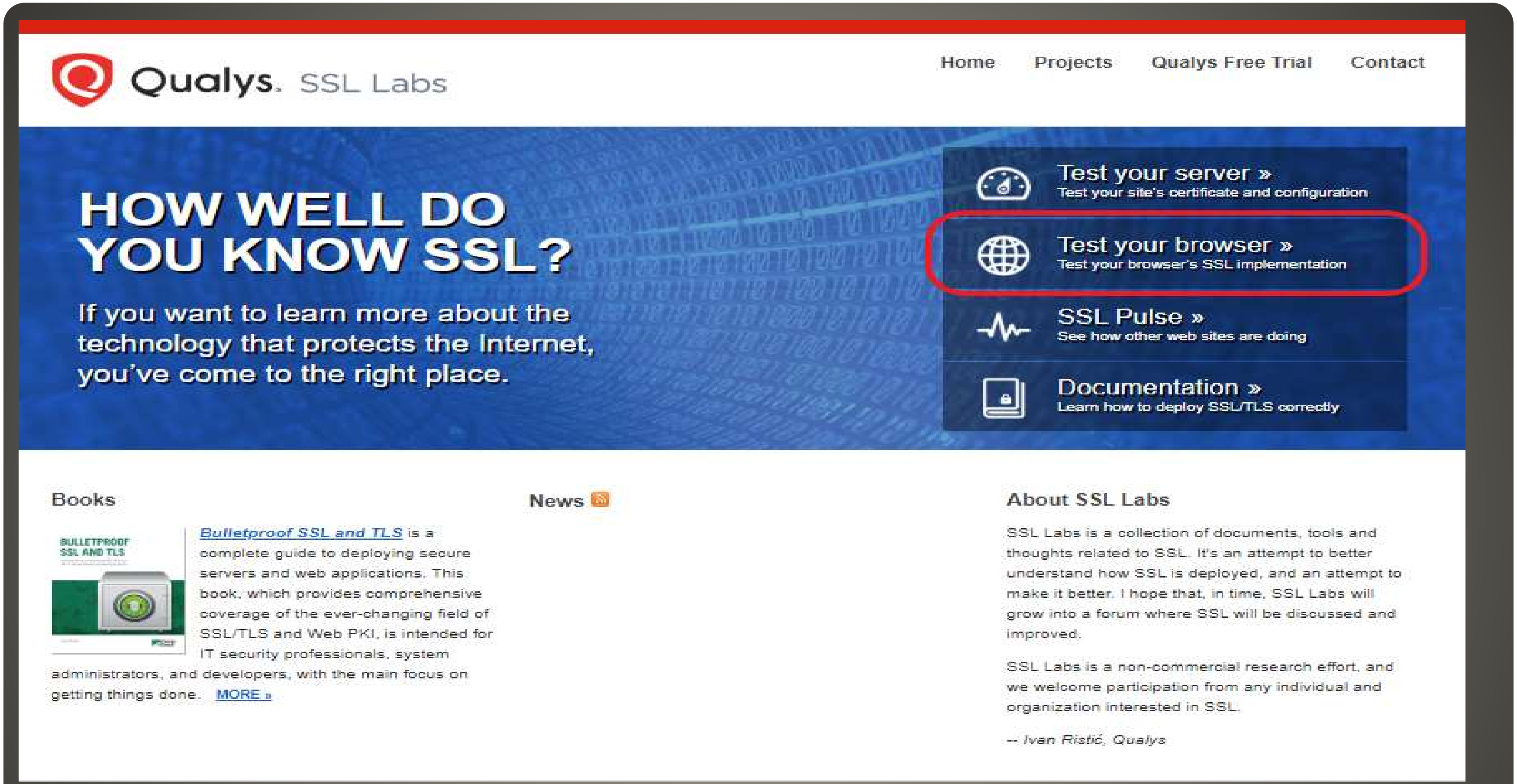


Name	Kind	Expires	Keychain
Apple Code Signing Certification Authority	certificate	Feb 14, 2015, 2:19:19 PM	System
Apple Root CA	certificate	Feb 9, 2035, 2:40:36 PM	System
Apple Timestamp Certification Authority	certificate	Apr 5, 2027, 6:02:44 AM	System
Apple Worldwide Developer Relations Certification Authority	certificate	Feb 14, 2016, 11:56:35 AM	System
com.apple.kerberos.kdc	certificate	Jul 21, 2032, 3:37:07 PM	System
com.apple.server.apns.alerts	certificate	May 11, 2016, 11:46:15 AM	System
com.apple.server.collabd	certificate	Jun 12, 2016, 1:45:25 PM	System
com.apple.server.scm_poller	certificate	Jun 12, 2016, 1:45:28 PM	System
com.apple.server.servermgr_xcode	certificate	Jun 12, 2016, 1:45:26 PM	System
com.apple.server.xcsbuildd	certificate	Jun 12, 2016, 1:45:26 PM	System
com.apple.servermgrd	certificate	Feb 26, 2015, 9:55:28 AM	System
com.apple.servermgrd.apns.calendar	certificate	May 11, 2016, 11:46:13 AM	System
com.apple.servermgrd.apns.contact	certificate	May 11, 2016, 11:46:14 AM	System
com.apple.servermgrd.apns.mail	certificate	May 11, 2016, 11:46:14 AM	System
com.apple.servermgrd.apns.mgmt	certificate	May 11, 2016, 11:46:15 AM	System
com.apple.systemdefault	certificate	Jul 21, 2032, 3:37:06 PM	System
com.apple.xcs.credential	certificate	May 12, 2015, 10:48:35 AM	System
DigiCert Secure Server CA	certificate	Mar 8, 2023, 5:00:00 AM	System
DigiCert SHA2 Assured ID Code Signing CA	certificate	Oct 22, 2028, 6:00:00 AM	System
DigiCert SHA2 Secure Server CA	certificate	Mar 8, 2023, 5:00:00 AM	System
Server Fallback SSL Certificate	certificate	Feb 18, 2016, 11:17:50 AM	System
servername.yourdomain.com	certificate	Jul 11, 2015, 5:06:16 PM	System
Software Signing	certificate	Jan 14, 2015, 3:02:56 PM	System
Test Mac DigiServer Open Directory Certification Authority	certificate	Feb 20, 2019, 2:12:07 PM	System

MacOS

- Unable to remove any certificates
- Ability to add Config Profile with Added certificates
- Administrator caution Does Not Apply

iOS



HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Test your server »
Test your site's certificate and configuration

Test your browser »
Test your browser's SSL implementation

SSL Pulse »
See how other web sites are doing

Documentation »
Learn how to deploy SSL/TLS correctly

Books

Bulletproof SSL and TLS is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system administrators, and developers, with the main focus on getting things done. MORE »

News

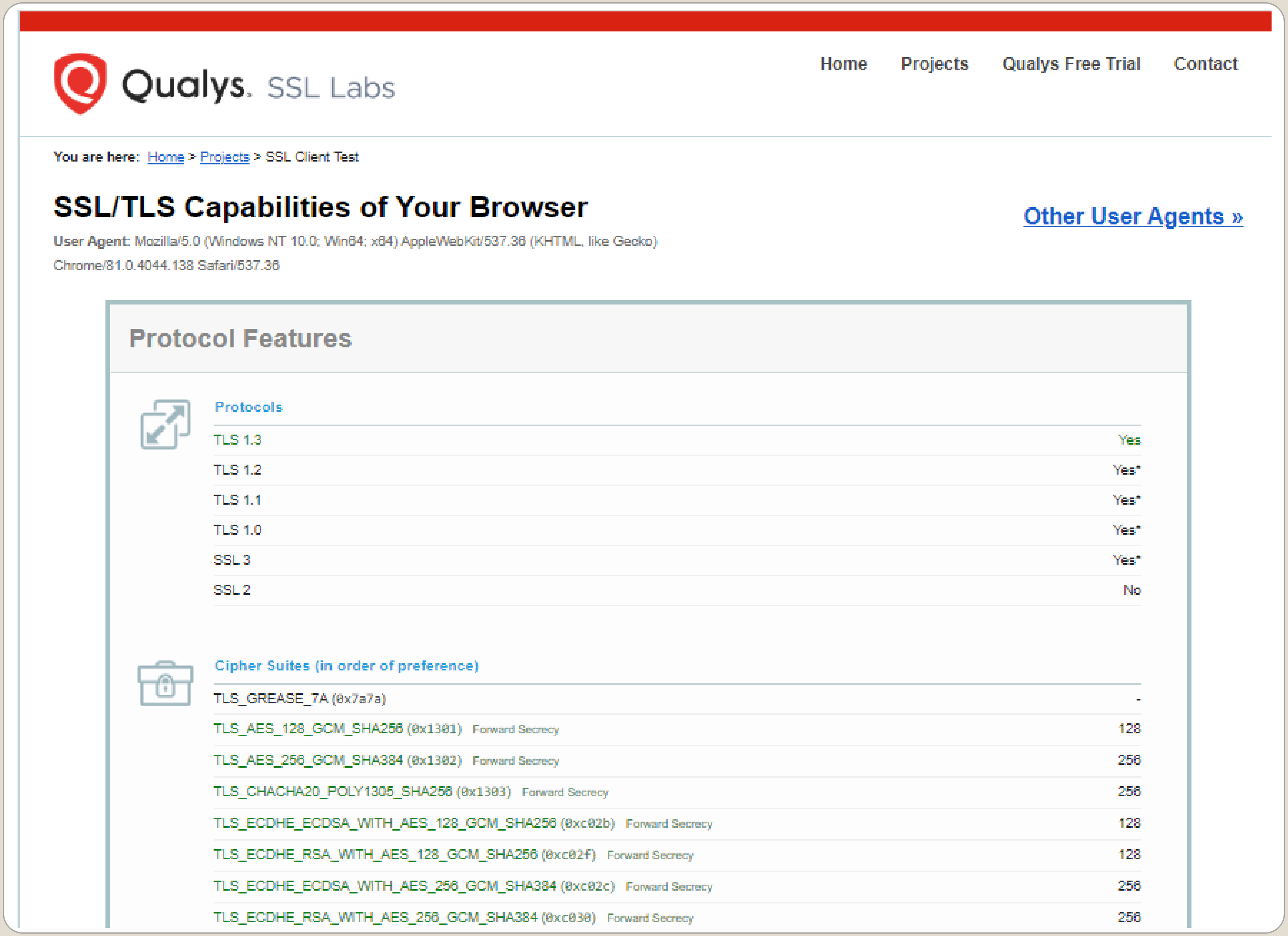
About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristić, Qualys

ssllabs.com



You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36

Protocol Features

Protocols

TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	Yes*
TLS 1.0	Yes*
SSL 3	Yes*
SSL 2	No

Cipher Suites (in order of preference)

TLS_GREASE_7A (0x7a7a)	-
TLS_AES_128_GCM_SHA256 (0x1301) Forward Secrecy	128
TLS_AES_256_GCM_SHA384 (0x1302) Forward Secrecy	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256

- Tails
- Linux
- Virtual machines   Linux
- Live CD/DVD
- Check for updates before each sensitive session
- New browser for each sensitive session
- Clickjacking
- Cross Site Scripting
- Cross Site Request Forgery
- “Private” sessions

Safer Browsing

Gotchas

- Overlay Lock Icon
- Overlay https://
- Sites can and do revert to http
- Browser extension to force https
- Complete Window overlay

Certificate & Encryption

HTML

- Methods
  POST, GET, PUT, PATCH, DELETE
- Response
  1xx Informational
  2xx success
  3xx redirection
  4xx client error
  5xx server error
- Referrer
- Redirect
- F12
- Cookies
  tracking, 3rd party, super, flash, HTML5, etc.
- Authentication cookie

- Cookies
- IP Address
- History
- Local logs
- Browser User Agent string
- Fingerprinting
- Referrer
- “I am not a robot”
- Anything coders can think of …

Tracking

Maintaining State

- URL

https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J6U1w&.rand=1655841https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J69qU1w&.rand=165584188&nsc88&nsc

- Hidden Form Fields

```
<form action="myform.cgi">
<input type="file" name="fileupload" value="fileupload"
id="fileupload">
<label for="fileupload"> Select a file to upload</label>
<input type="hidden" id="ipaddr" name="ipaddr" value="<?php echo
$_SERVER['REMOTE_ADDR']; ?>">
<input type="hidden" id="referer" name="referer" value="<?php echo
$_SERVER['HTTP_REFERER']; ?>">
<input type="submit" value="submit">
</form>
```

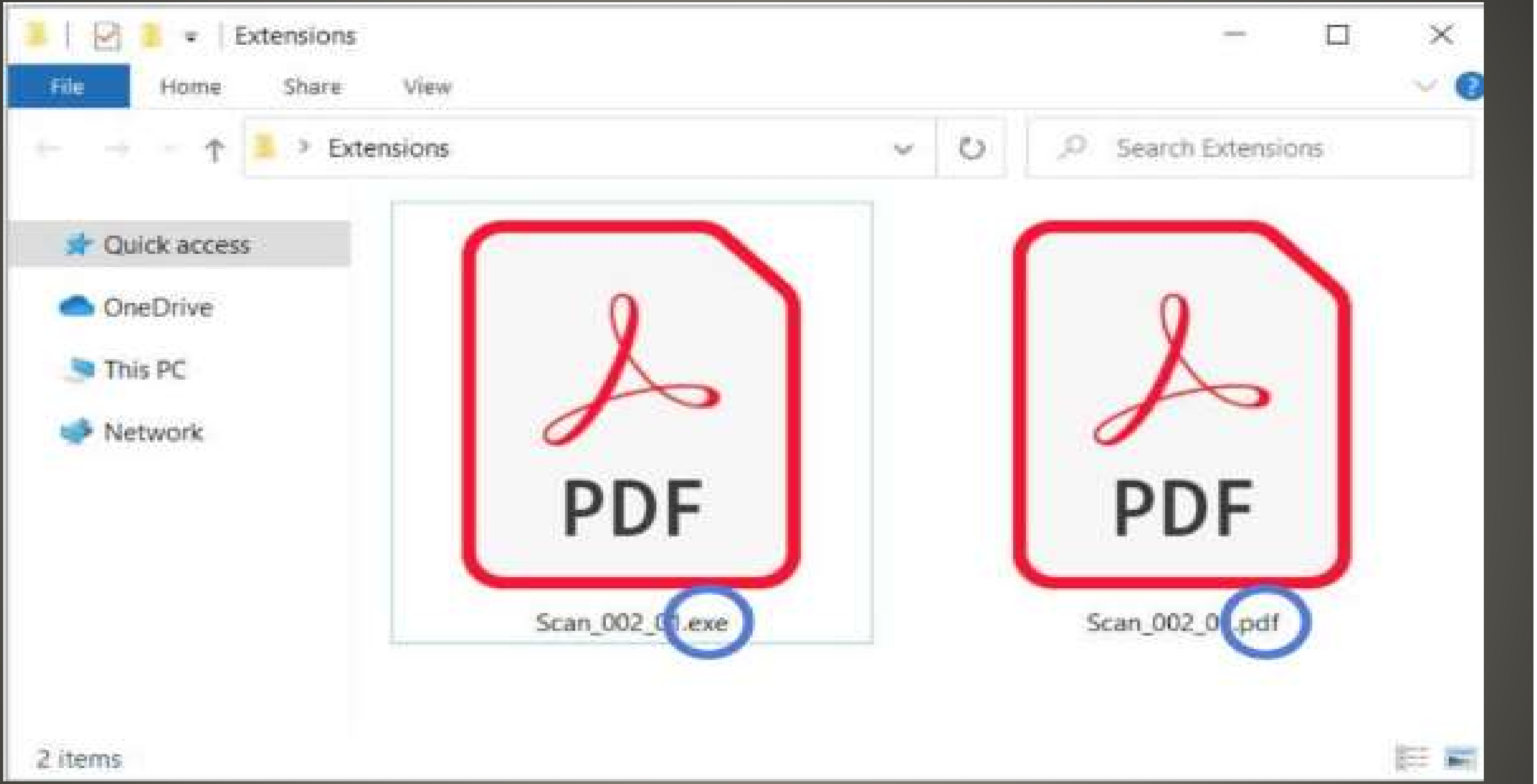
- Cookies

Search Engines without tracking

- DuckDuckGo
- WolframAlpha
- Startpage
- Privatelee
- Yippy
- Hulbee
- Gibiru
- Disconnect Search
- Lukol
- MetaGer

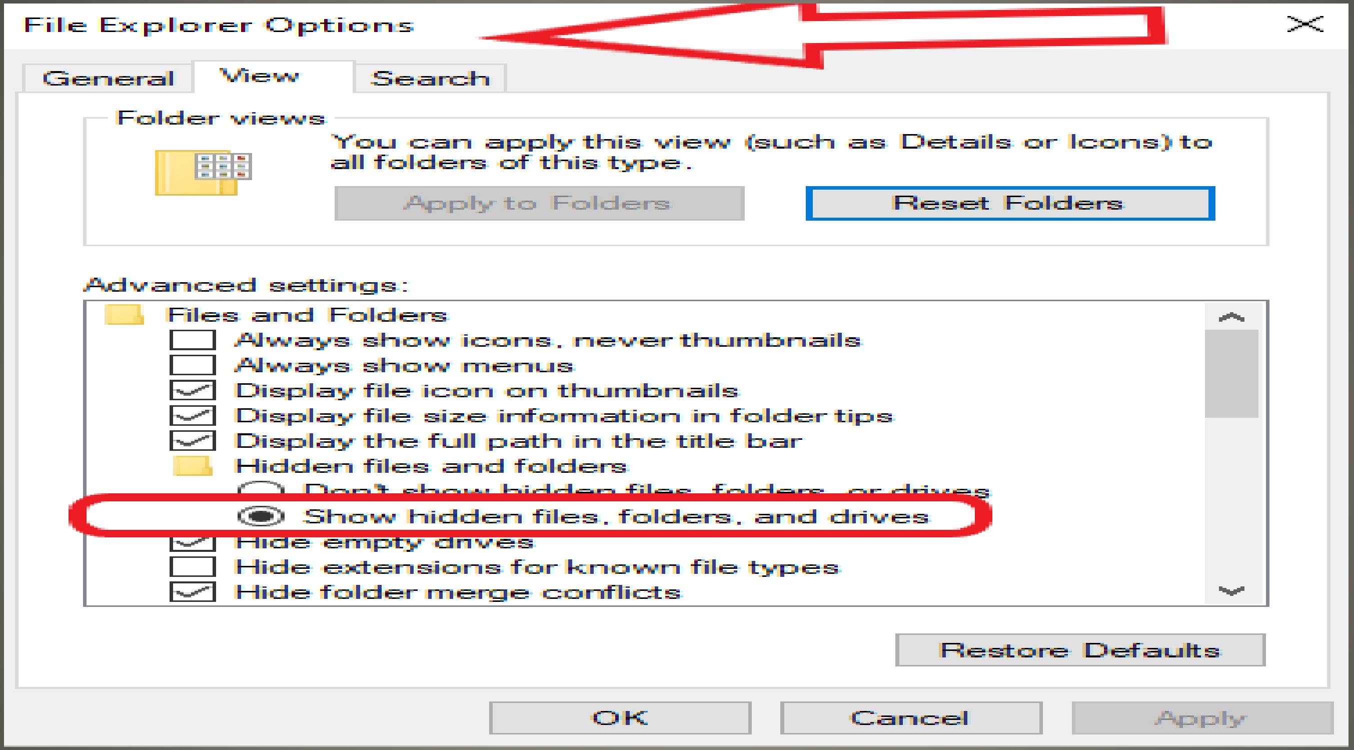
- Over a BILLION web sites
- Over 4 billion users on Internet
- If you can see them, they can see you

- Credential Spraying
- Facial Recognition Face covering



File extension

- File Explorer Options



Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

Files and Folders

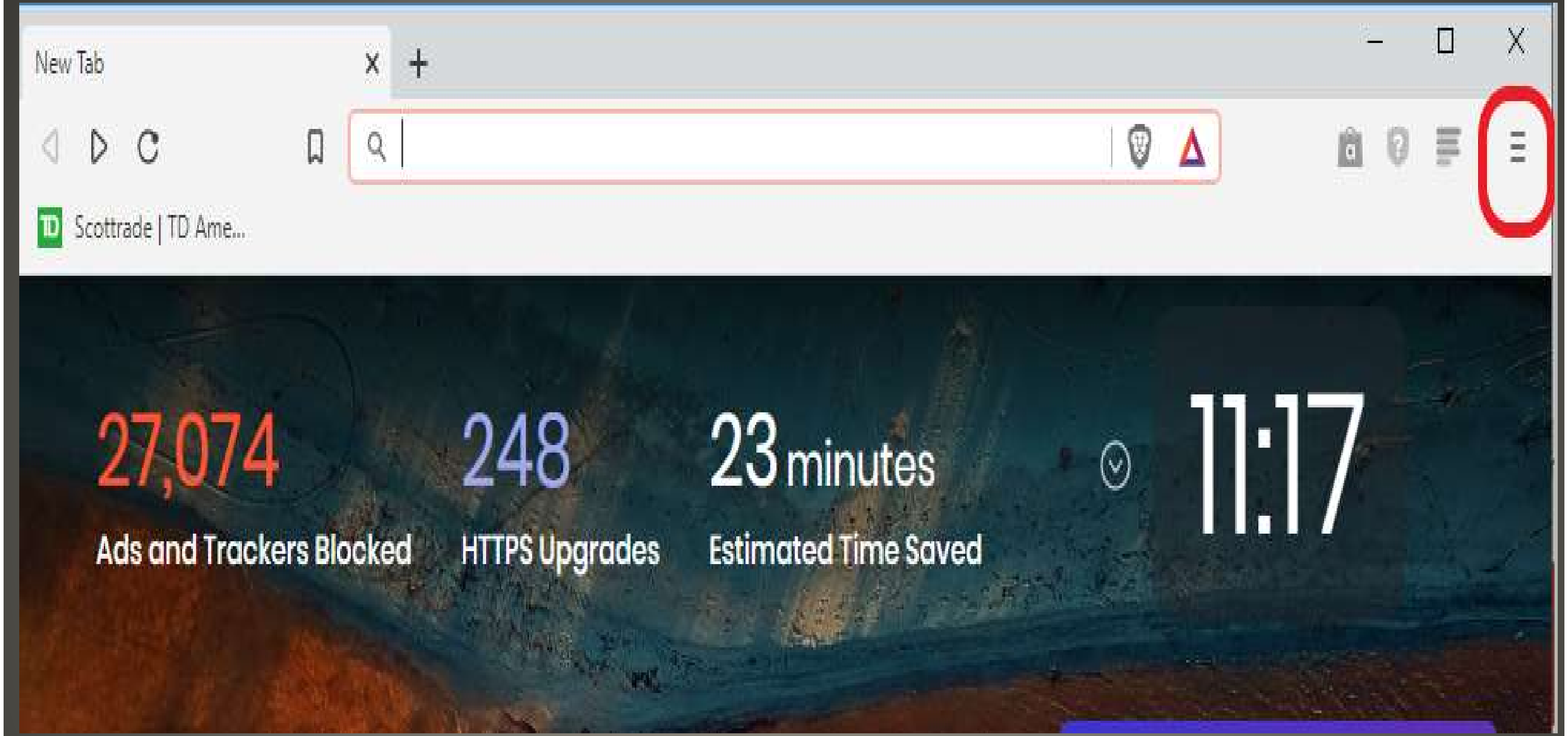
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- ☑ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives
- □ Hide extensions for known file types
- ☑ Hide folder merge conflicts

Un Hide File Extensions

- Clear cookies & history before booking
- See the top 10 __________ in every state!
- VPN to see less adds, reduce trackers

  GDPR California

- USE BROWSER TO UPDATE BROWSER



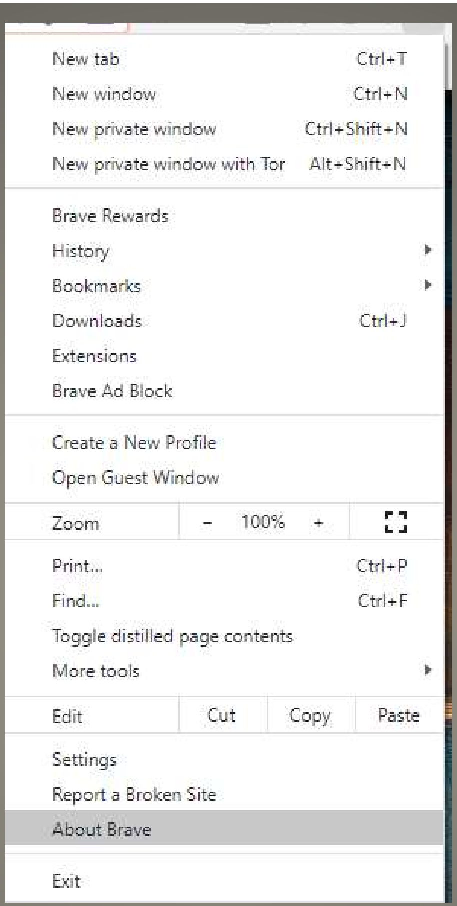
27,074 Ads and Trackers Blocked

248 HTTPS Upgrades

23 minutes Estimated Time Saved

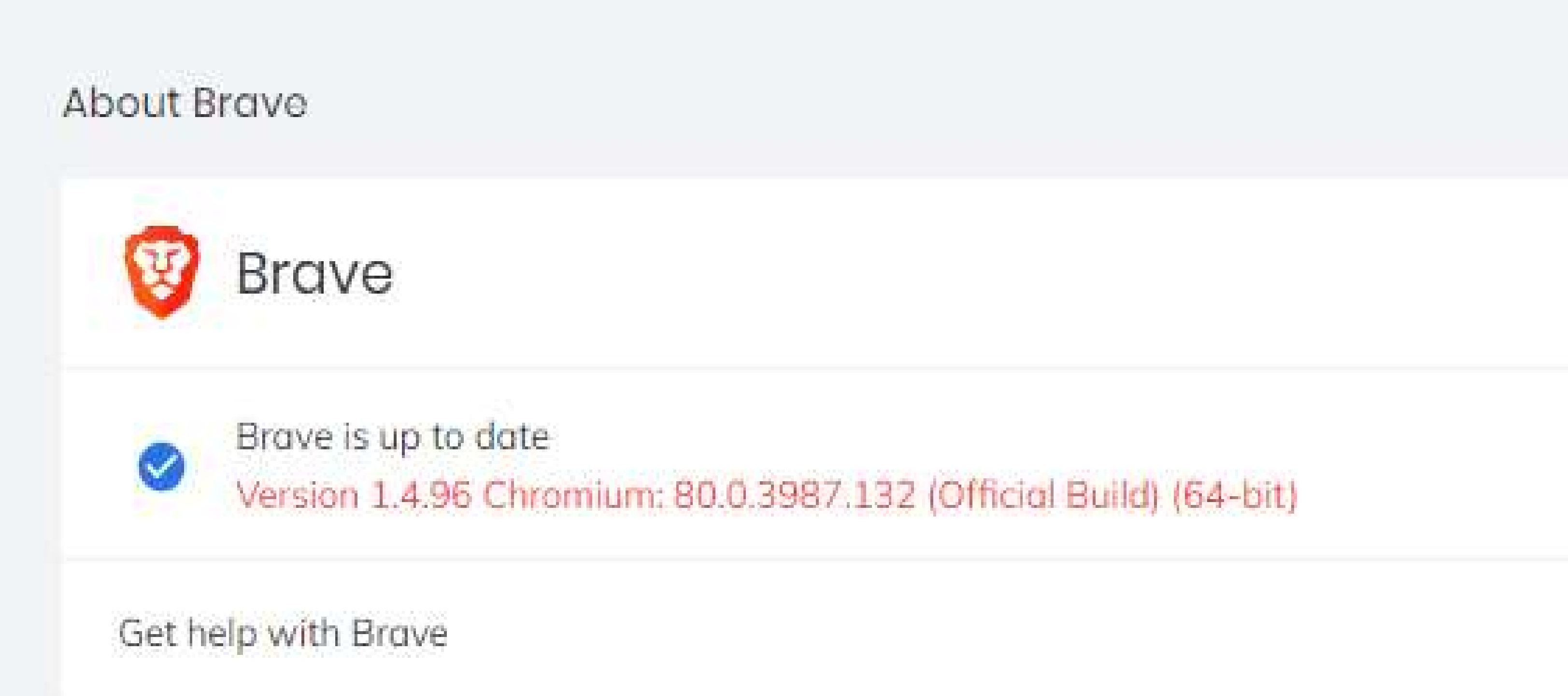
11:17

Brave



New tab Ctrl+T
New window Ctrl+N
New private window Ctrl+Shift+N
New private window with Tor Alt+Shift+N
Brave Rewards
History
Bookmarks
Downloads Ctrl+J
Extensions
Brave Ad Block
Create a New Profile
Open Guest Window
Zoom – 100% +
Print... Ctrl+P
Find... Ctrl+F
Toggle distilled page contents
More tools
Edit Cut Copy Paste
Settings
Report a Broken Site
About Brave
Exit

Brave



About Brave

Brave

Brave is up to date

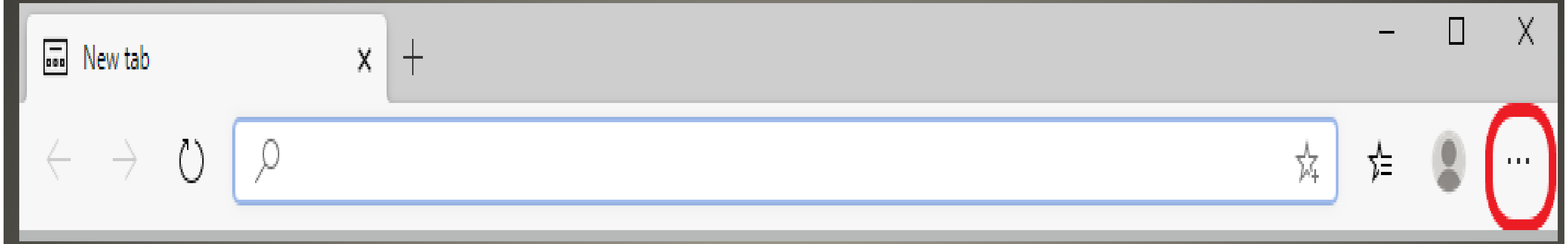
Version 1.4.96 Chromium: 80.0.3987.132 (Official Build) (64-bit)

Get help with Brave

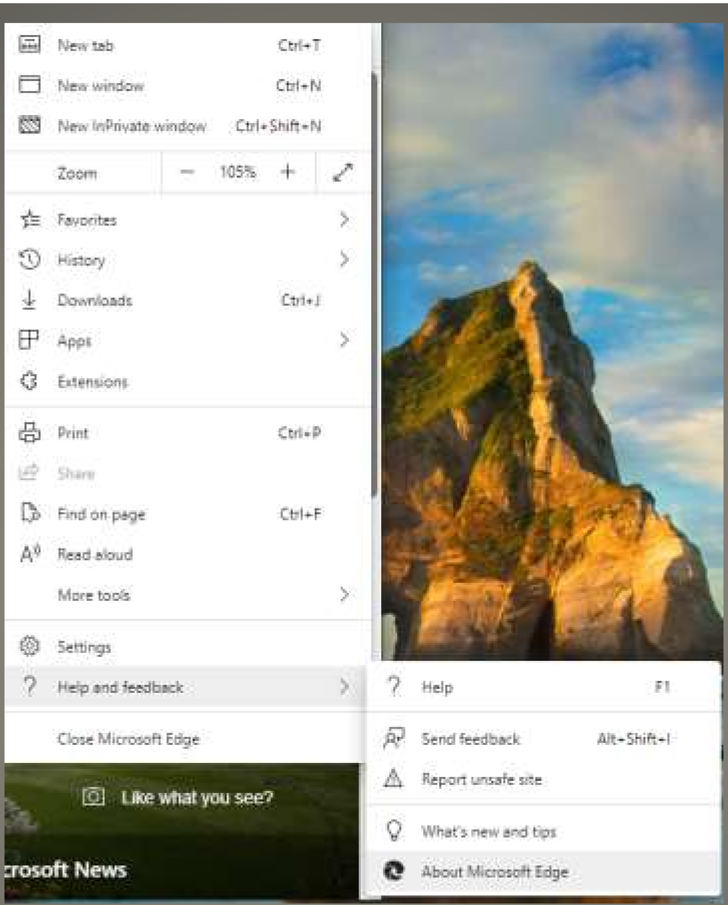
Brave

- Safari Updated with MacOS
- Beta tester

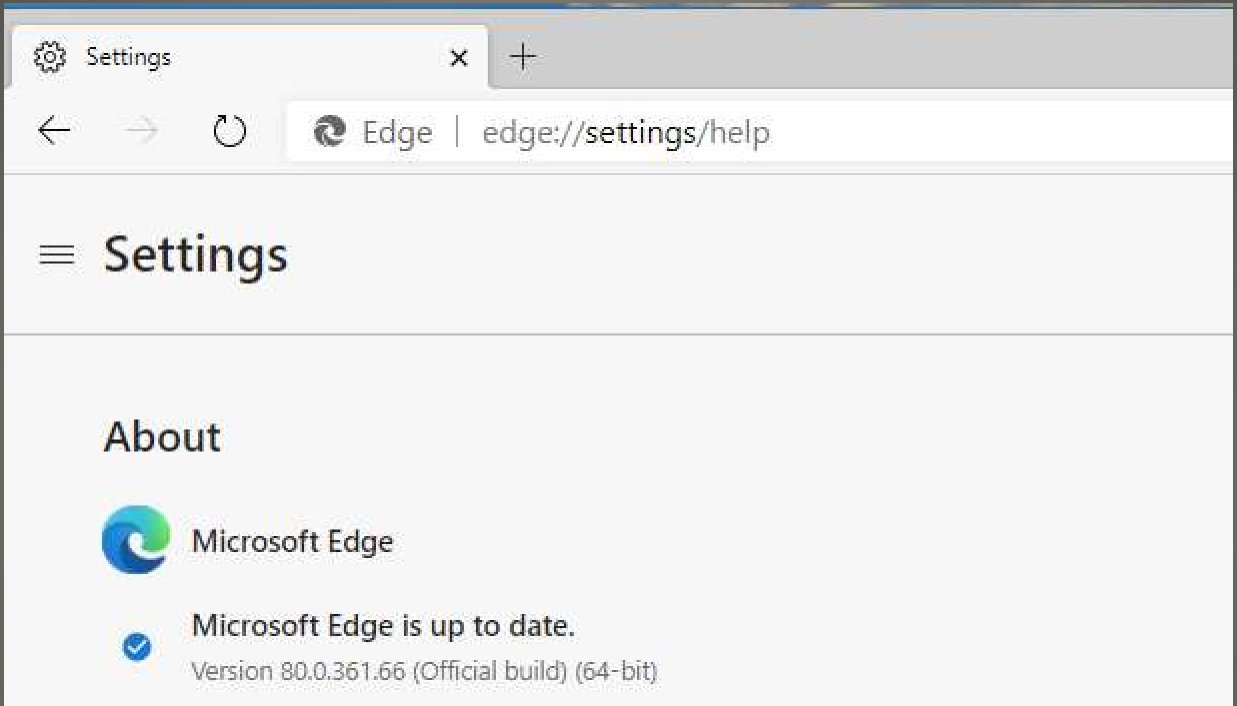
Safari



Edge


New tab Ctrl+T
New window Ctrl+N
New InPrivate window Ctrl+Shift+N
Zoom — 105% +
Favorites
History
Downloads Ctrl+J
Apps
Extensions
Print Ctrl+P
Share
Find on page Ctrl+F
Read aloud
More tools
Settings
Help and feedback
Close Microsoft Edge
Like what you see?
crosoft News
Help F1
Send feedback Alt+Shift+I
Report unsafe site
What's new and tips
About Microsoft Edge

Edge



Settings

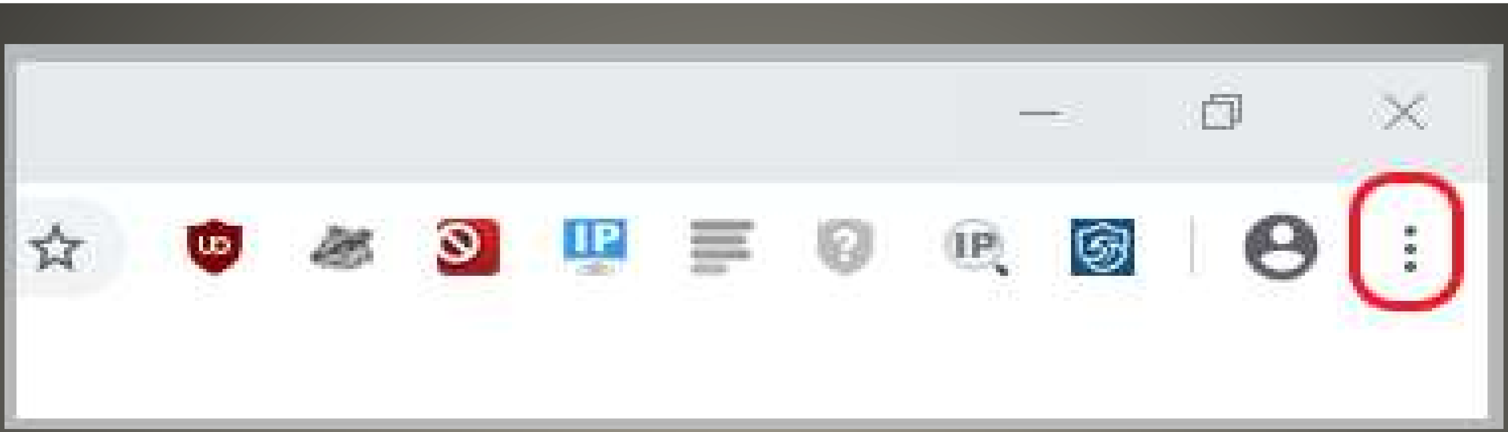
About

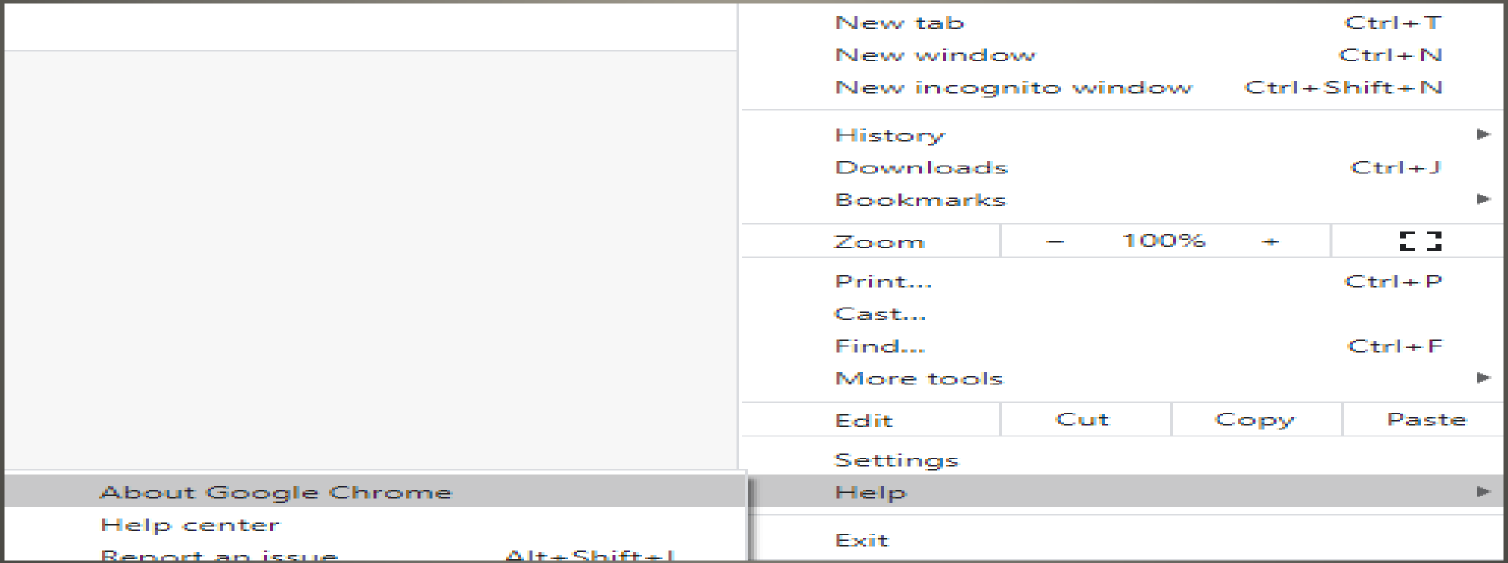
Microsoft Edge

Microsoft Edge is up to date.

Version 80.0.361.66 (Official build) (64-bit)

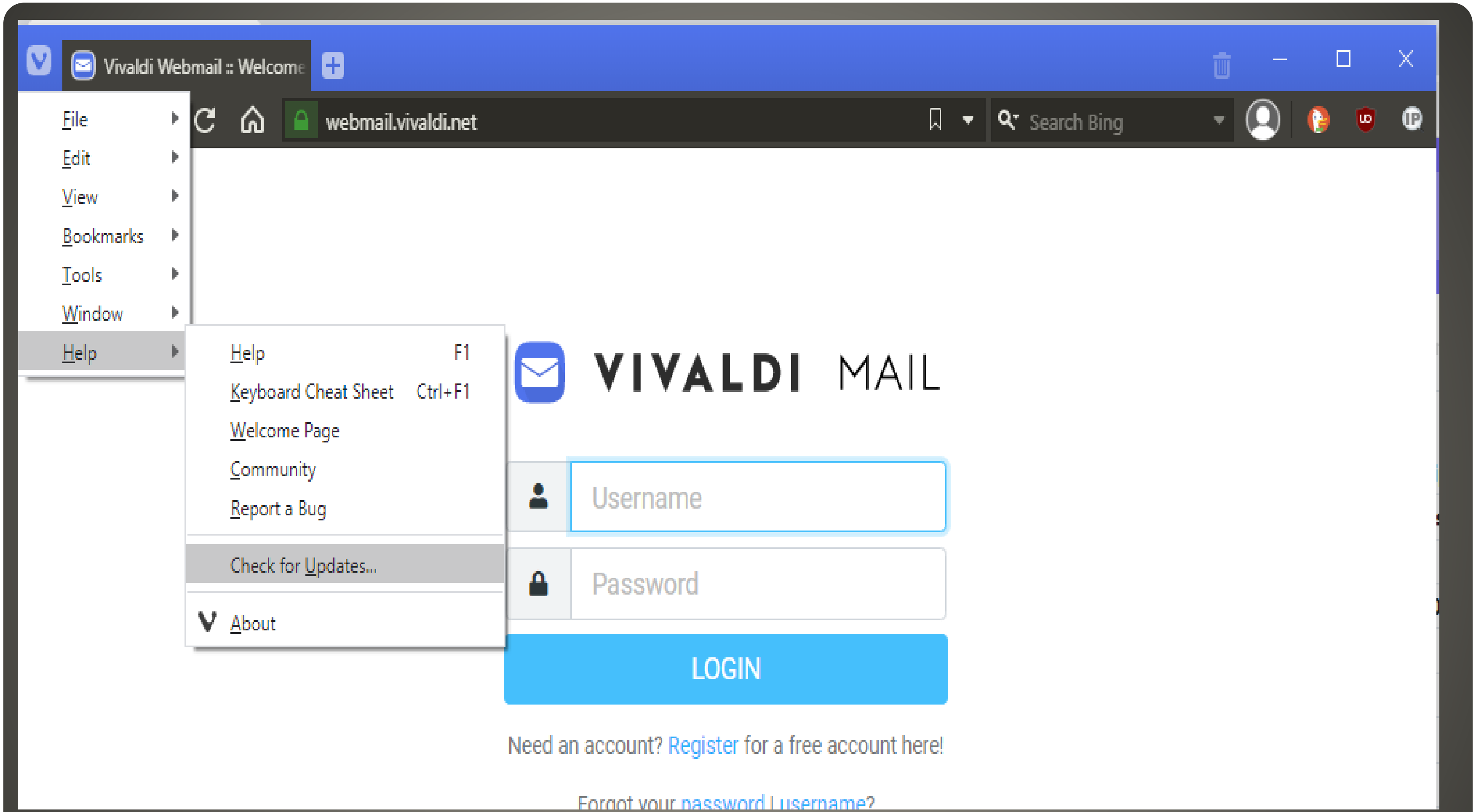
Edge




New tab Ctrl+T
New window Ctrl+N
New incognito window Ctrl+Shift+N
History
Downloads Ctrl+J
Bookmarks
Zoom – 100% +
Print... Ctrl+P
Cast...
Find... Ctrl+F
More tools
Edit Cut Copy Paste
Settings
Help
Exit
About Google Chrome
Help center
Report an issue Alt+Shift+I

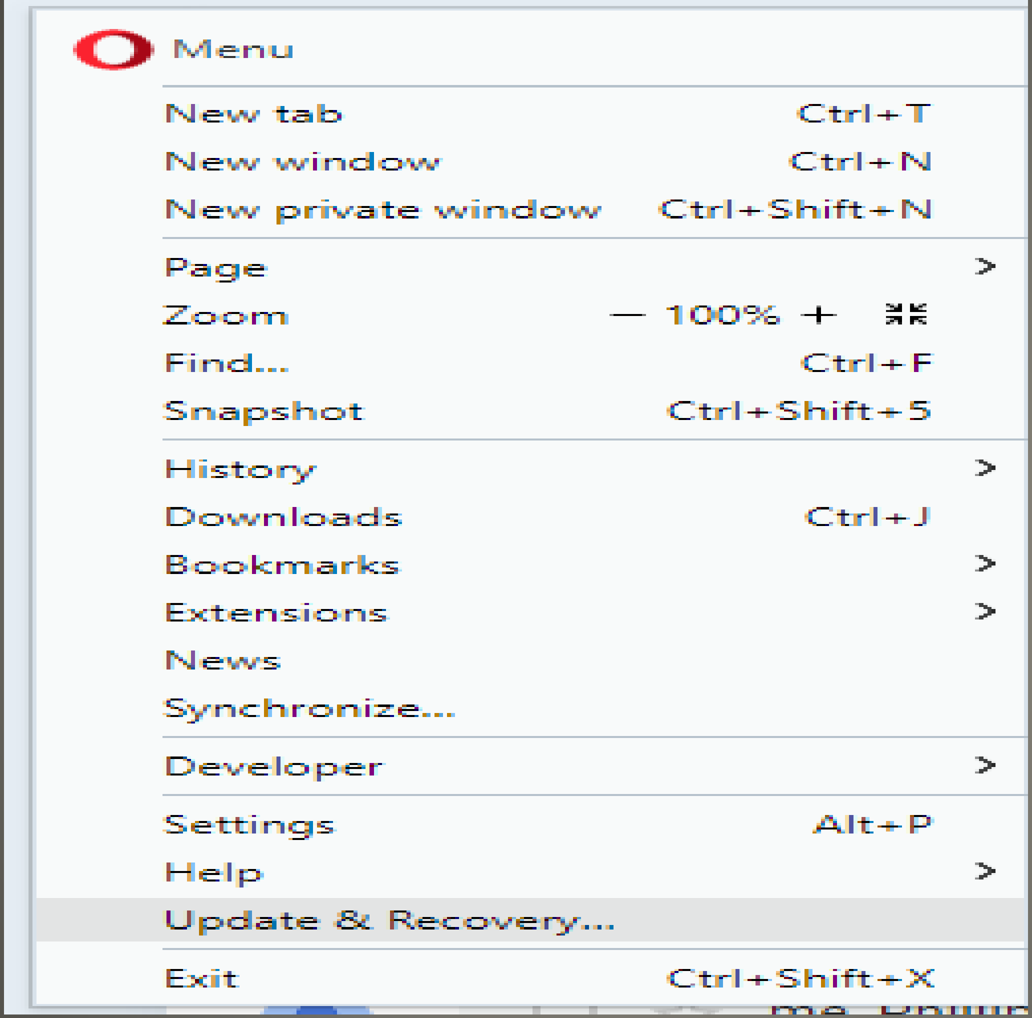
Chrome

Vivaldi

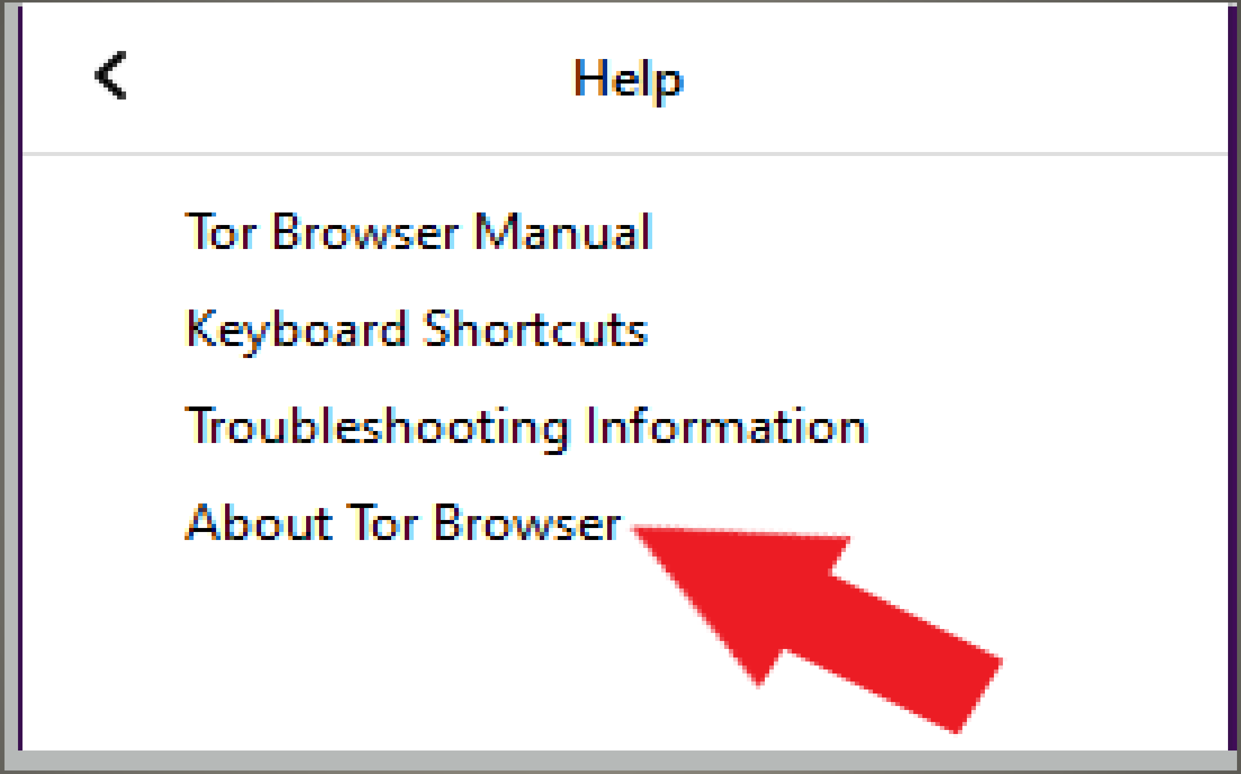


Need an account? Register for a free account here!

Forgot your password | username?


Menu
New tab Ctrl+T
New window Ctrl+N
New private window Ctrl+Shift+N
Page >
Zoom — 100% +
Find... Ctrl+F
Snapshot Ctrl+Shift+5
History >
Downloads Ctrl+J
Bookmarks >
Extensions >
News
Synchronize...
Developer >
Settings Alt+P
Help >
Update & Recovery...
Exit Ctrl+Shift+X

Opera



Help

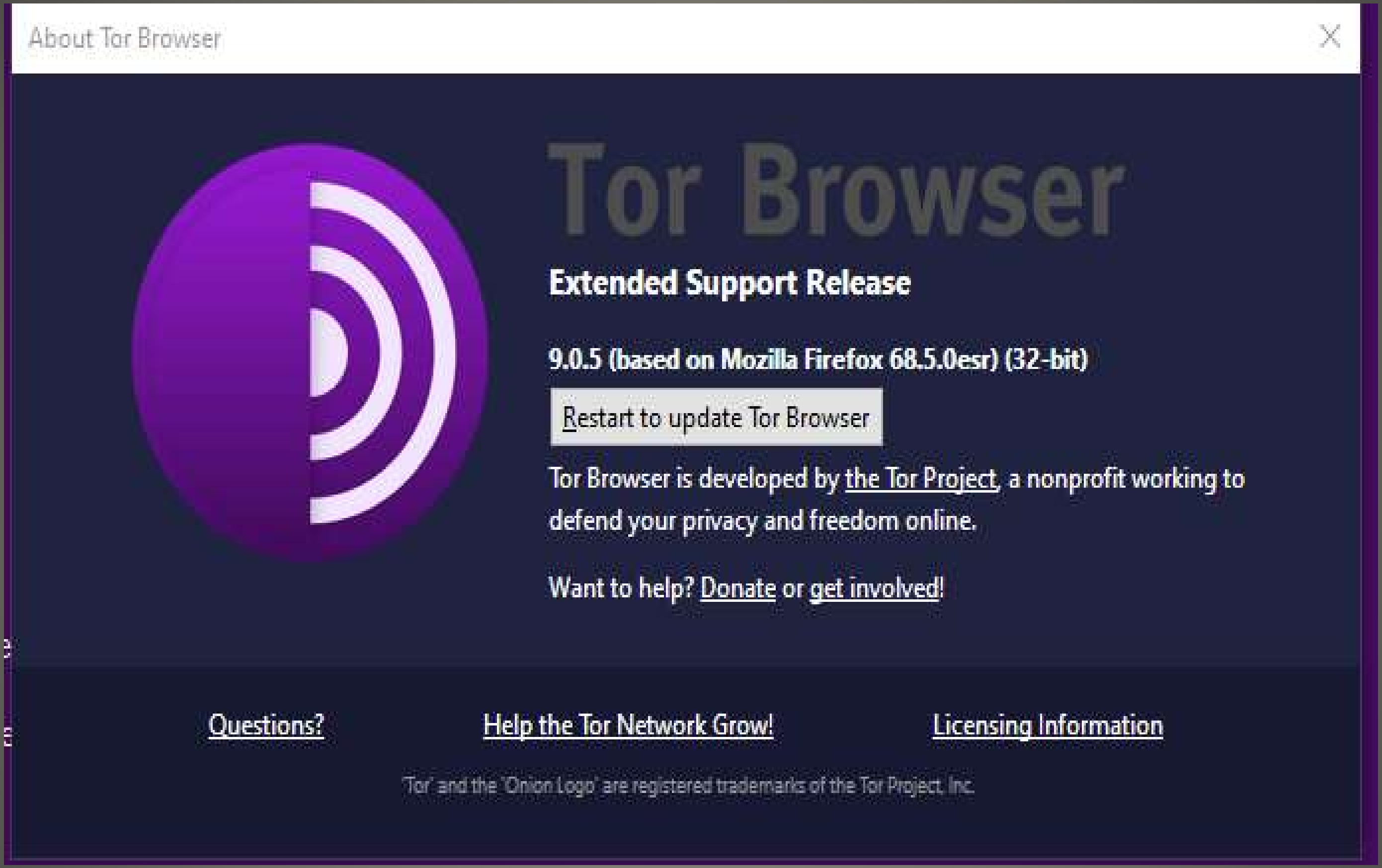
Tor Browser Manual

Keyboard Shortcuts

Troubleshooting Information

About Tor Browser

Tor



Tor Browser

Extended Support Release

9.0.5 (based on Mozilla Firefox 68.5.0esr) (32-bit)

Tor Browser is developed by the Tor Project, a nonprofit working to defend your privacy and freedom online.

Want to help? Donate or get involved!

'Tor' and the 'Onion Logo' are registered trademarks of the Tor Project, Inc.

Tor

Browser Choices

- Chrome
- Firefox
- Opera
- Safari
- Edge
- Vivaldi
- Brave
- Tor

Multiple

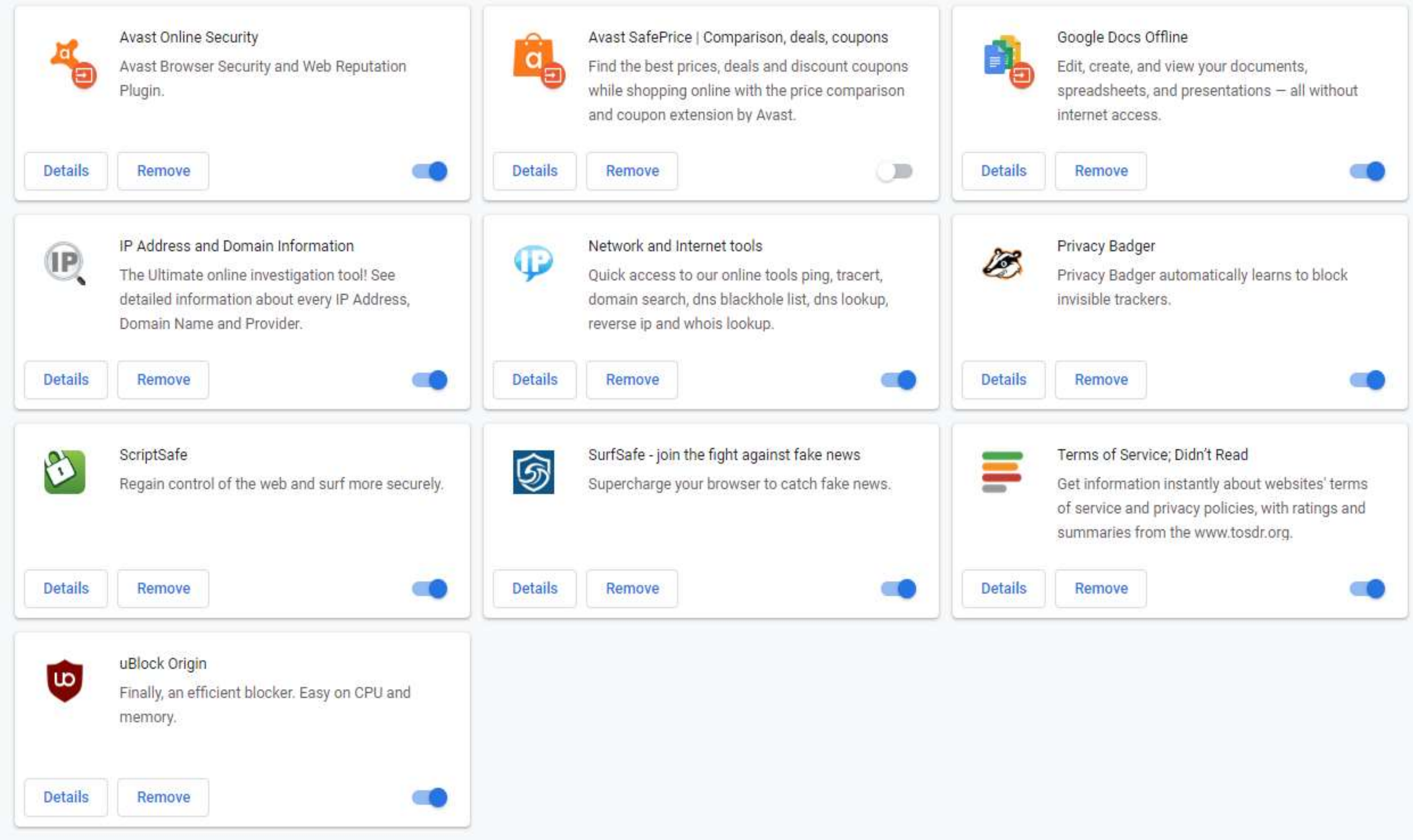
- Browsers
- eMail accounts/addresses
- Phone numbers Land Line
- IDentities

- Default browser vs OS browser

Windows & MacOS

- Private mode
- InPrivate Window
- Incognito window

- Limits displayed history



Avast Online Security

Avast Browser Security and Web Reputation Plugin.

Avast SafePrice | Comparison, deals, coupons

Find the best prices, deals and discount coupons while shopping online with the price comparison and coupon extension by Avast.

Google Docs Offline

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

IP Address and Domain Information

The Ultimate online investigation tool! See detailed information about every IP Address, Domain Name and Provider.

Network and Internet tools

Quick access to our online tools ping, tracert, domain search, dns blackhole list, dns lookup, reverse ip and whois lookup.

Privacy Badger

Privacy Badger automatically learns to block invisible trackers.

ScriptSafe

Regain control of the web and surf more securely.

SurfSafe - join the fight against fake news

Supercharge your browser to catch fake news.

Terms of Service; Didn't Read

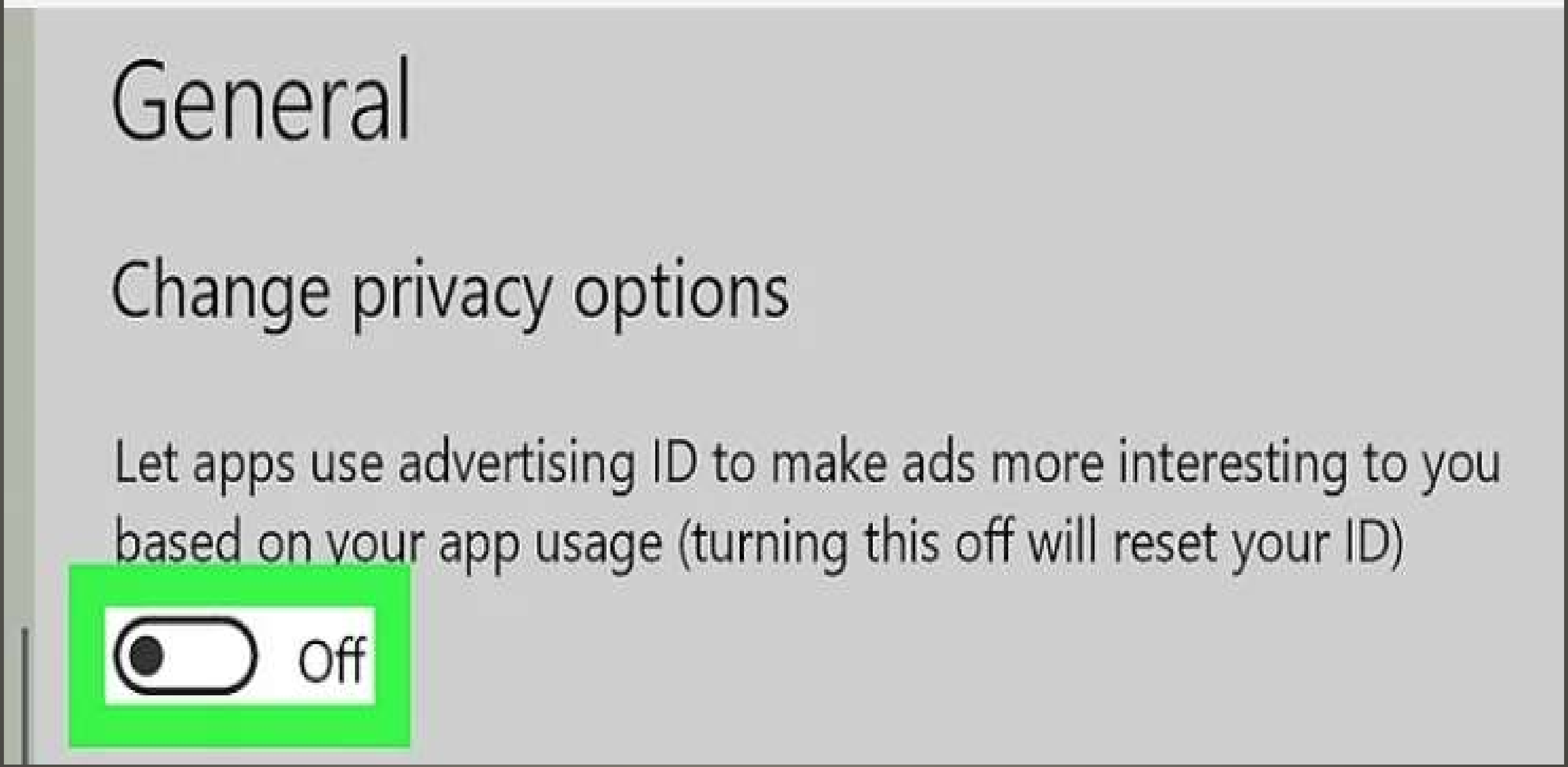
Get information instantly about websites' terms of service and privacy policies, with ratings and summaries from the www.tosdr.org.

uBlock Origin

Finally, an efficient blocker. Easy on CPU and memory.

Add-ons & plug-ins

- Settings > Privacy > General



General

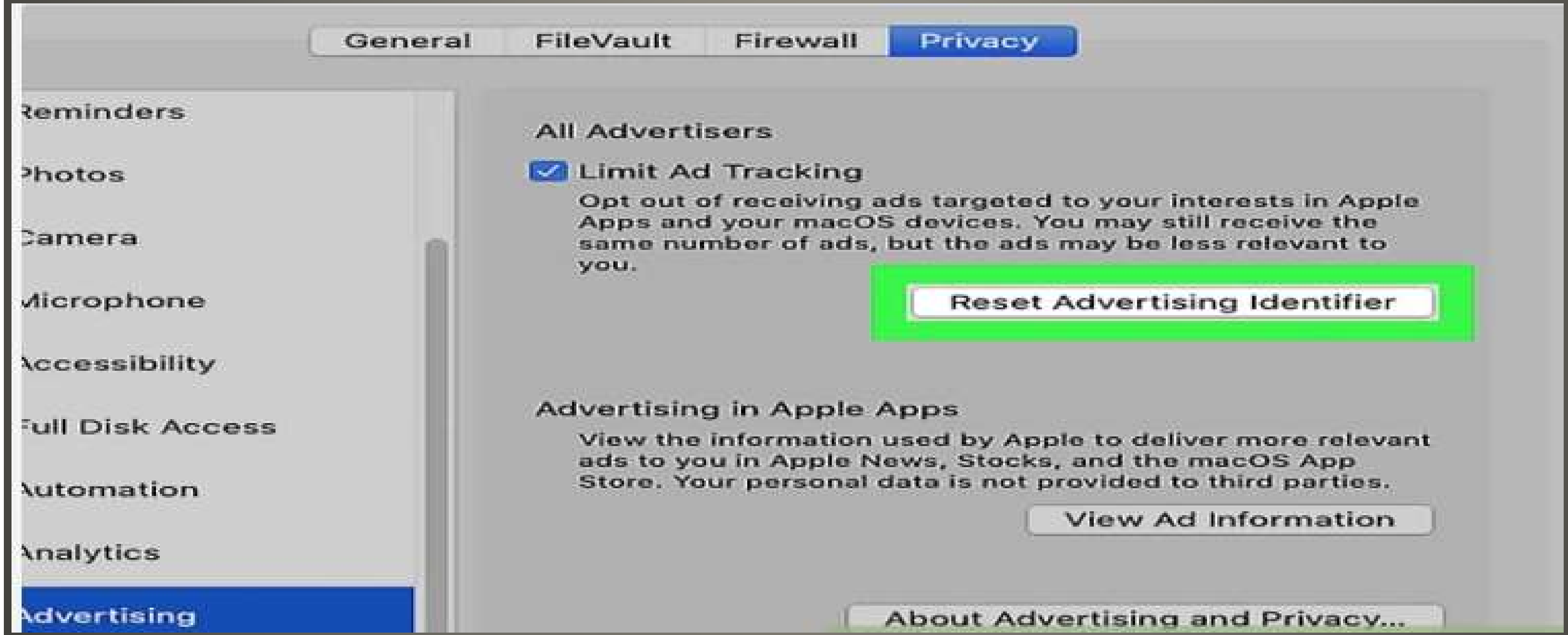
Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

Off

Advertiser ID Windows

- System Preferences > Security & Privacy > Privacy > Advertising



All Advertisers

☑ Limit Ad Tracking

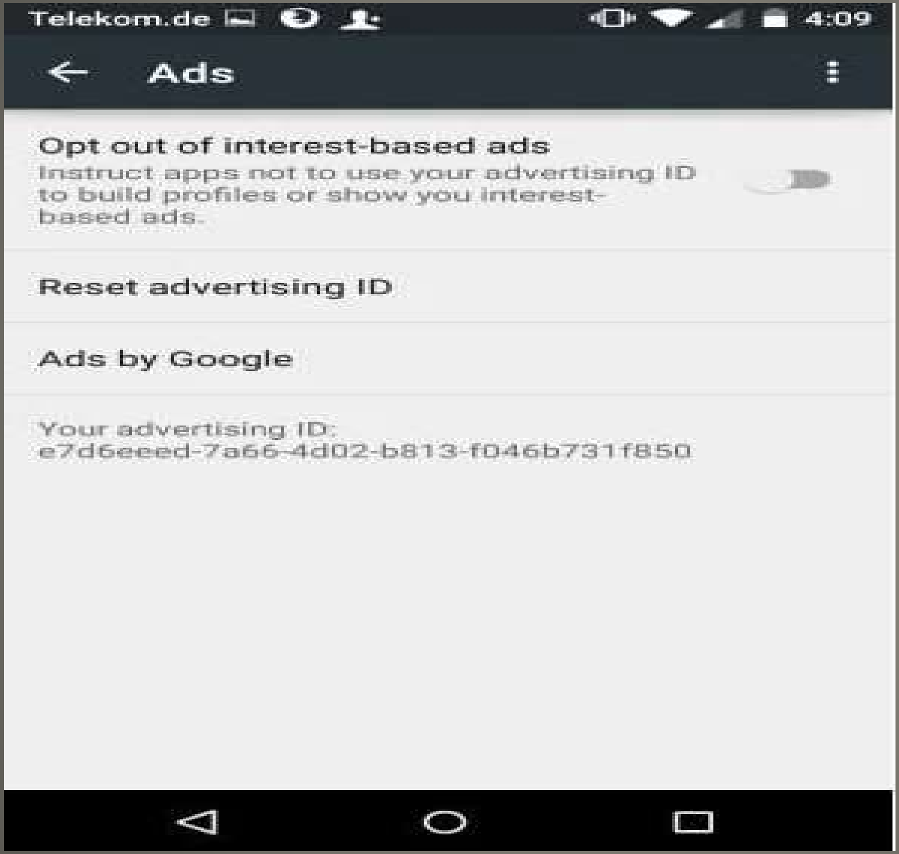
Opt out of receiving ads targeted to your interests in Apple Apps and your macOS devices. You may still receive the same number of ads, but the ads may be less relevant to you.

Advertising in Apple Apps

View the information used by Apple to deliver more relevant ads to you in Apple News, Stocks, and the macOS App Store. Your personal data is not provided to third parties.

Advertiser ID MacOS

- Settings > Ads



Opt out of interest-based ads

Instruct apps not to use your advertising ID to build profiles or show you interest-based ads.

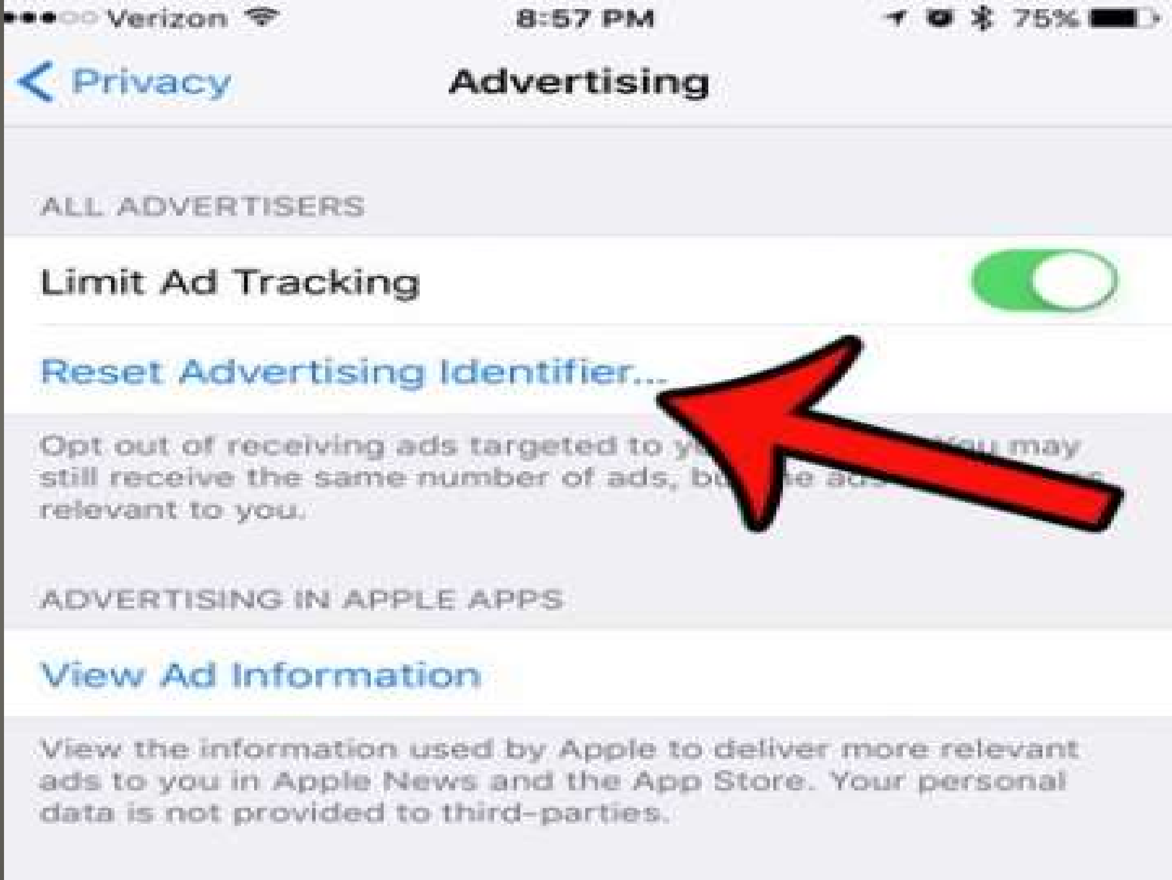
Reset advertising ID

Ads by Google

Your advertising ID:
e7d6eeed-7a66-4d02-b813-f046b731f850

Advertising ID Android

- Settings > Privacy > Advertising



Verizon 8:57 PM 75%

< Privacy Advertising

ALL ADVERTISERS

Limit Ad Tracking ●

Reset Advertising Identifier...

Opt out of receiving ads targeted to y ou may still receive the same number of ads, bu e ad relevant to you.

ADVERTISING IN APPLE APPS

View Ad Information

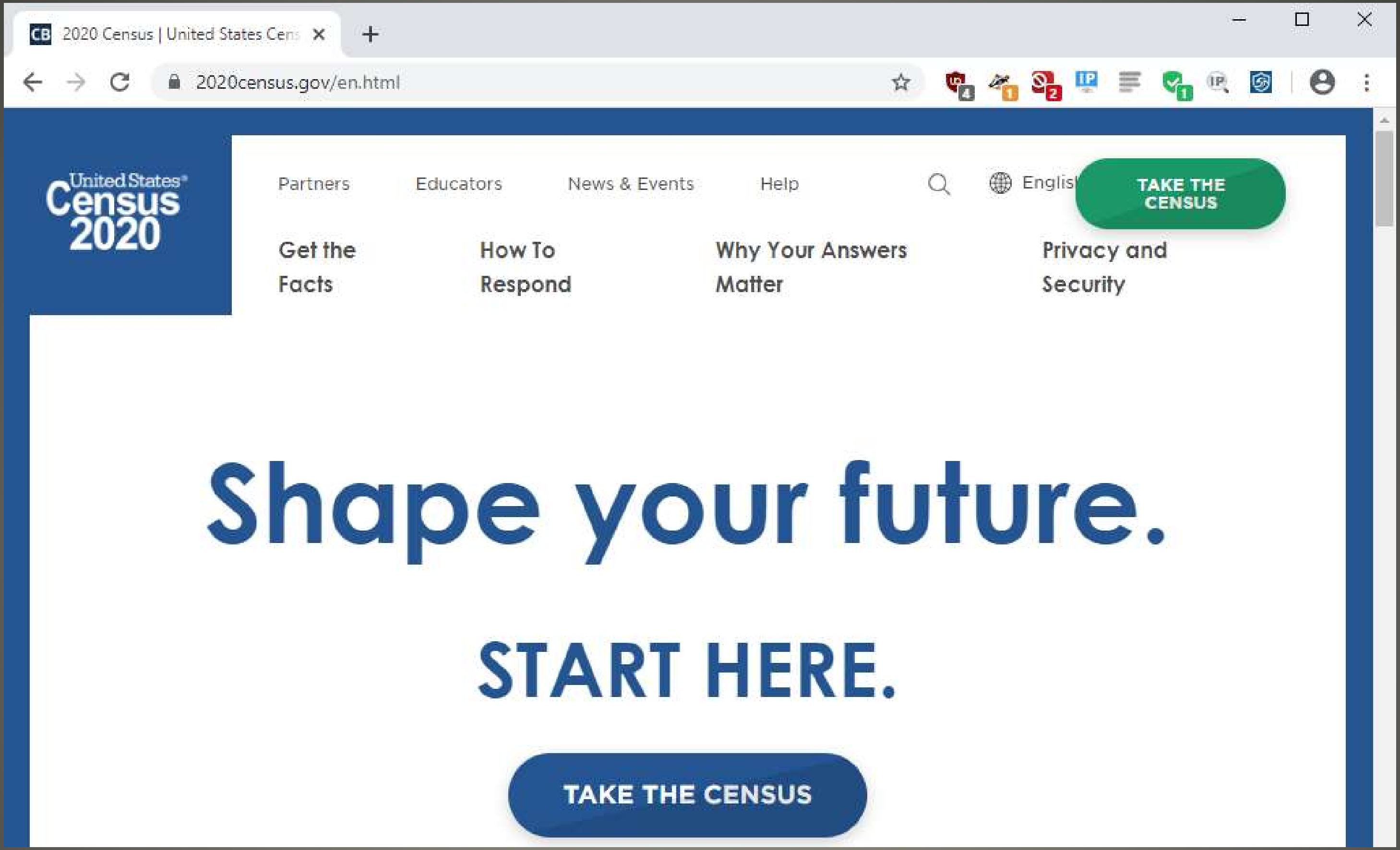
View the information used by Apple to deliver more relevant ads to you in Apple News and the App Store. Your personal data is not provided to third-parties.

Advertising ID iPhone

- Clear cookies BEFORE purchase
- LIVE Linux with USB tether

  smartphone with Wi-Fi & Bluetooth OFF

  TAILS
- User Agent String
- Finger Printing Browser, OS,
- Avoid links use URL bookmark



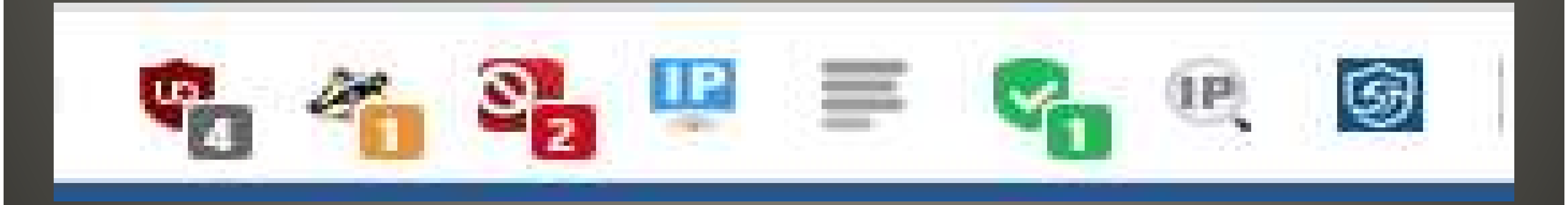
Shape your future.

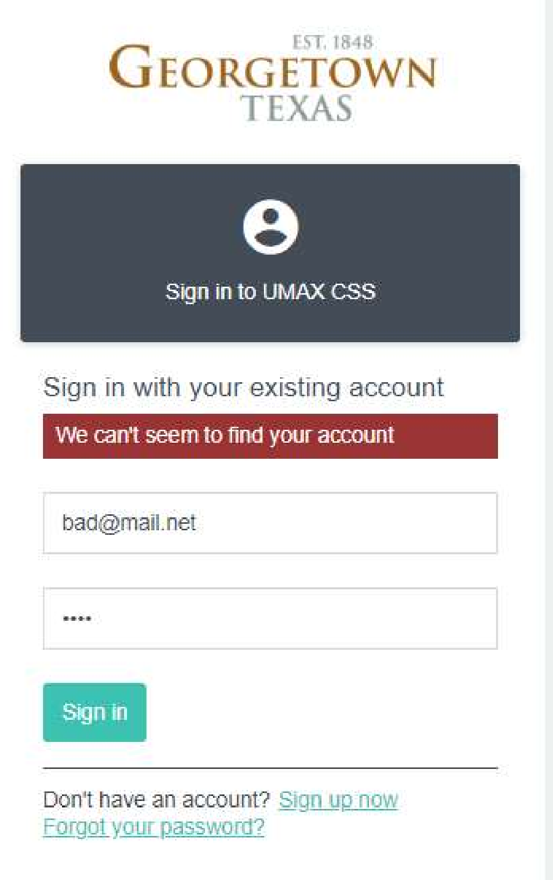
START HERE.

https & www missing now

Extensions

- uBlock Origin
- Privacy Badger
- ScriptSafe
- Network and Internet Tools
- Terms of Service; Didn’t Read
- Avast
- IP Address and Domain Information
- SurfSafe





EST. 1848 GEORGETOWN TEXAS

Sign in to UMAX CSS

Sign in with your existing account

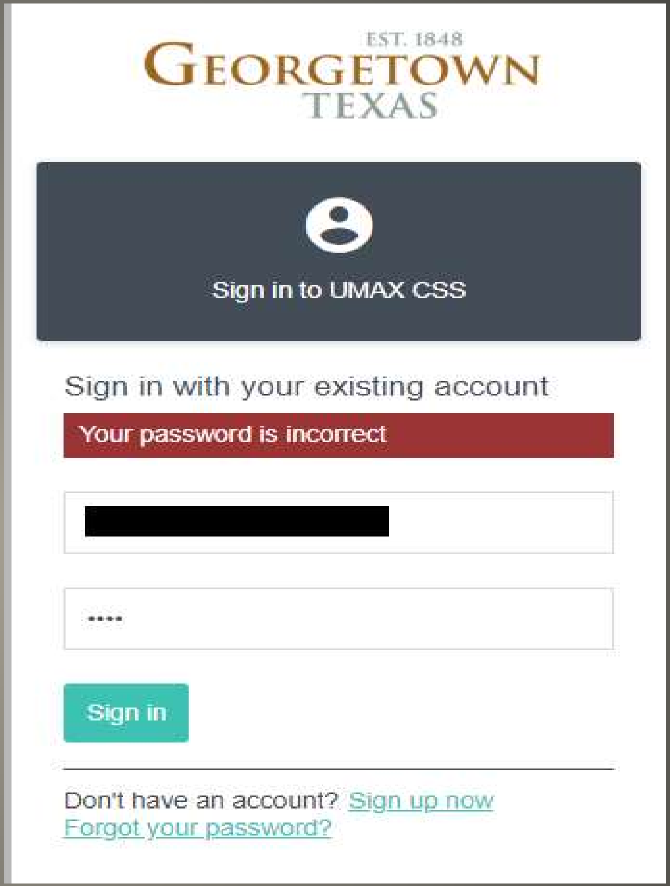
We can't seem to find your account

bad@mail.net

••••

Sign in

Don't have an account? Sign up now
Forgot your password?



EST. 1848 GEORGETOWN TEXAS

Sign in to UMAX CSS

Sign in with your existing account

Your password is incorrect

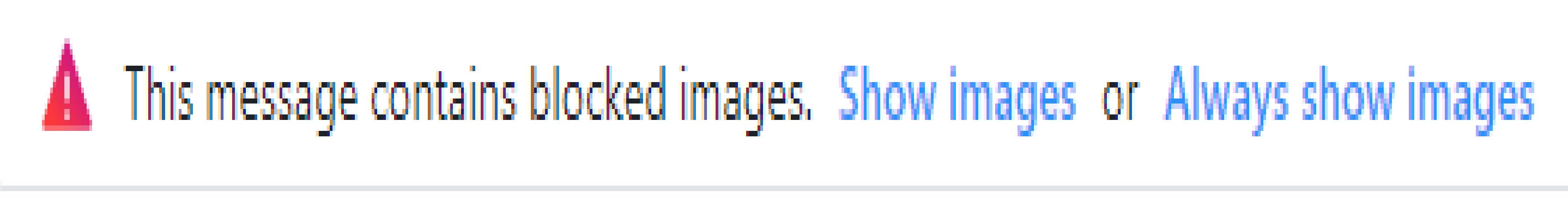
[redacted]

••••

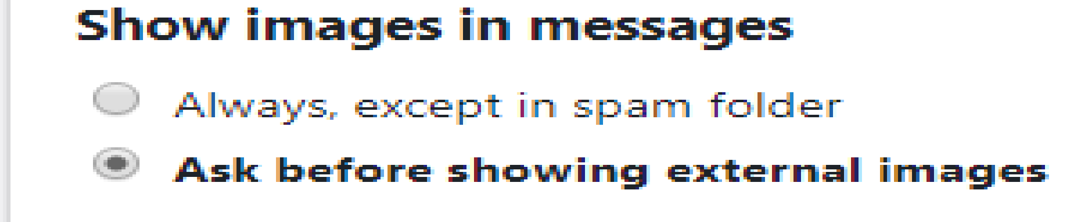
Sign in

Don't have an account? Sign up now
Forgot your password?

Information leak



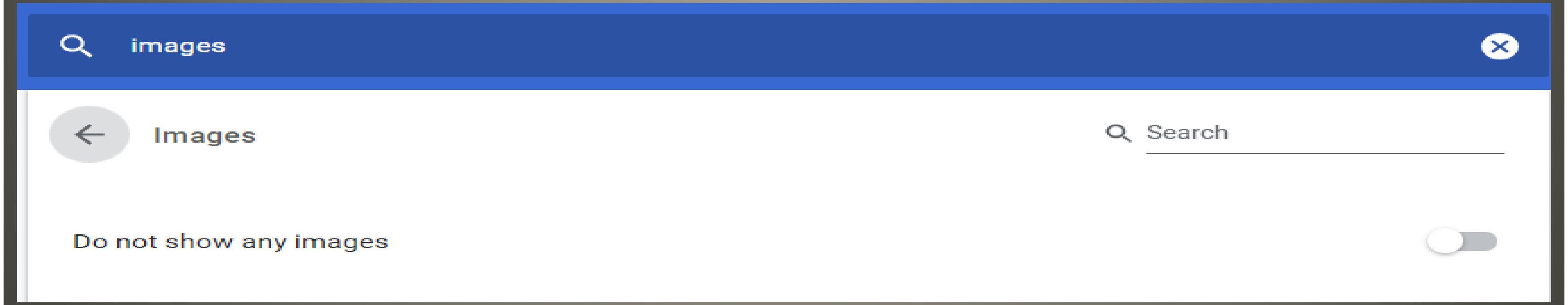
This message contains blocked images. Show images or Always show images



Show images in messages

○ Always, except in spam folder

● Ask before showing external images



images

Do not show any images ○

Images email browser

Analytics

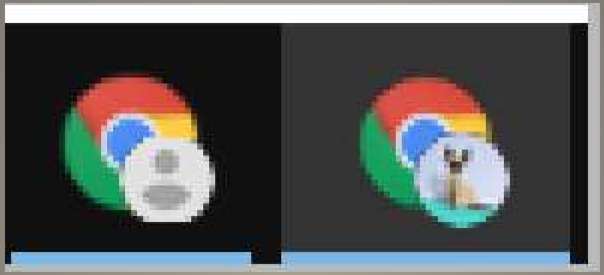
- LARGE part of WEB traffic
- Adblockers and script disablers half effective
- Host file

  analytics.google.com
  www.google-analytics.com
  google-analytics.com
  ssl.google-analytics.com
- Windows c:\windows\system32\drivers\etc\hosts
- MacOS

  /private/etc/hosts

Browser Profiles

- NOT for data segmentation or security
- Same browser, same user, a profile
- Work & Home
- Club 1 Club 2 Golf To Go Food …
- Separate history, cookies, bookmarks, site blocks, extensions, add-ons, …
- Shopping, travel, price adjustments
- Sync and Don’t Sync



Chrome profile

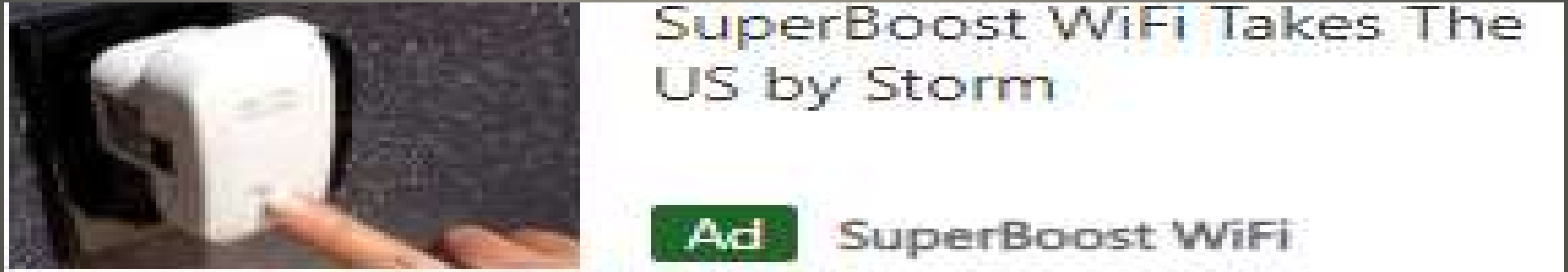
- Vero
- Terms of Service; Didn’t Read

Terms & Conditions

- https://isitdown.me
- https://www.isitdownrightnow.com
- https://down.com

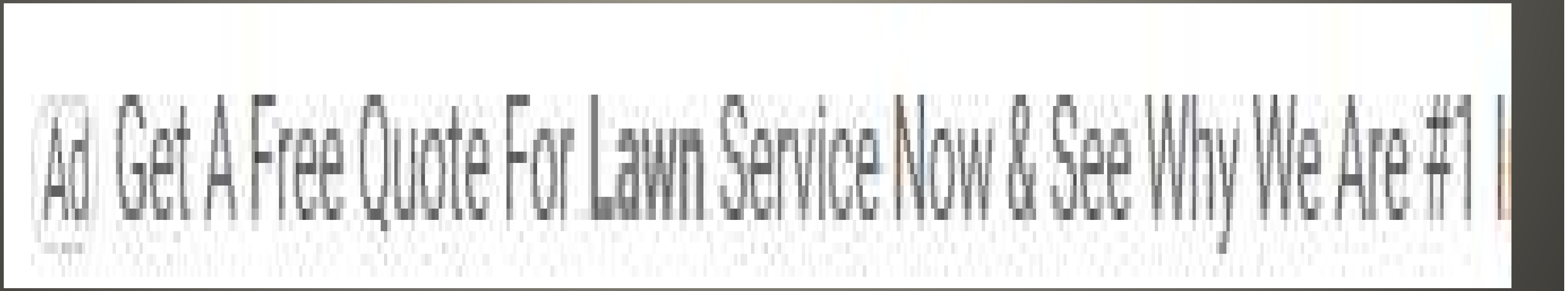
Is it just me?

- You won’t believe …
- Top ten
- Look for Ad badge



SuperBoost WiFi Takes The US by Storm

Ad SuperBoost WiFi



Ad Get A Free Quote For Lawn Service Now & See Why We Are #1

Lure

- HTTP over TLS
- HTTP over SSL
- Authentication
- Confidentiality
- Integrity

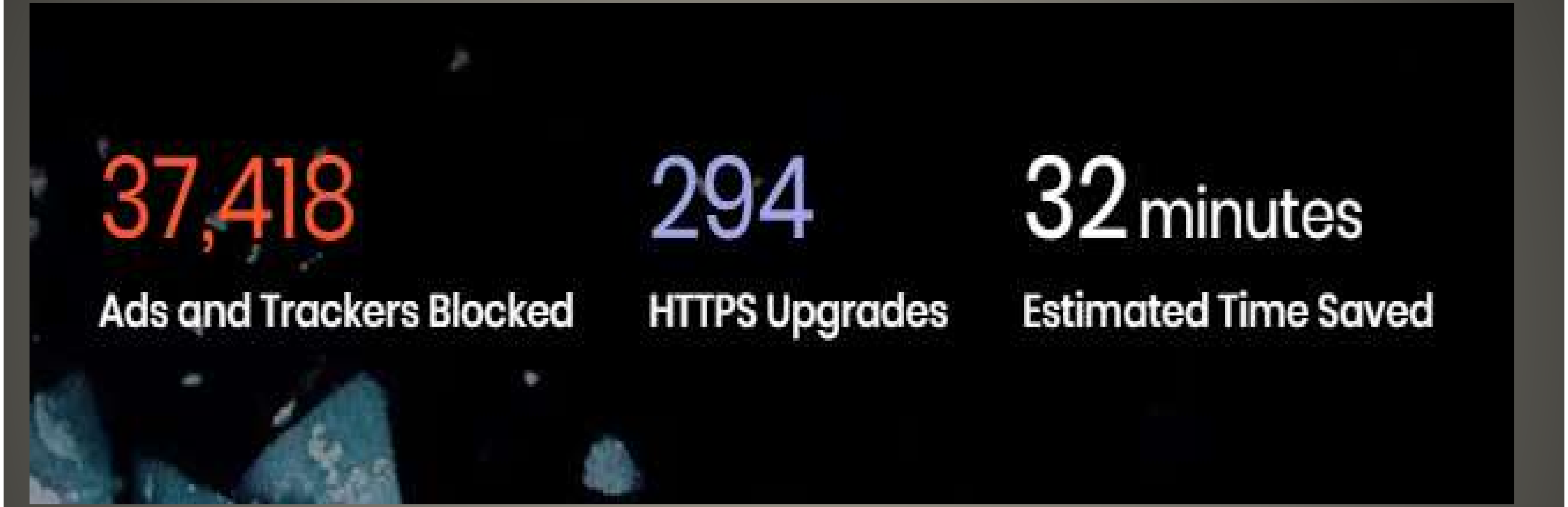
HTTPS

- Attempt to detect human
- Slow down automated registration “bots”
- I’m not a robot

Captcha

WEB Proxy

- Client <> Proxy <> Server
- “Transparent”
- Policy Based Routing
- Analyze downloads Virtual Machine
- ADMINISTRATOR rights & privilege
- Hard to detect
- Manipulation of certificate store



37,418
Ads and Trackers Blocked

294
HTTPS Upgrades

32 minutes
Estimated Time Saved

Brave Browser statistics

- 1 PC
- Dial up modem with acoustic coupler
- Dial up modem sharing phone line
- Internet with tablets, multiple PCs

- Very expensive entry costs
- Many servers, facility space, staff,
- Build and run my web business for $1.00/mo

Used to be

Safer Browsing

- Browser wars
- Brave, Lynx
- Add-ons and extensions

  uBlock Origin, NoScript, uMatrix, AdBlocker
- MultiFactor Authentication
- Maintain state

  URL, Hidden form fields, cookies
- Proxy
- TOR
- Business Practices IRS – Phone Bank - PIN

- VMs
- Live CD/DVD/USB
- Sandbox
- Search Engine
- Hover Over
- Multiple Browsers
- Multiple security configurations
- VPN
- Tiny URL expansion
- Popups
- Certificate warnings
- Drive By
- Sites with user supplied WEB content
- EULA
- Deliberate mistakes
- Become informed, aware, suspicious

Safer

Safer

- Search engines
- Browser indicators
- Hover Over
- URL inspection
- Professionalism
- Surveys & Account creation
- Google Transparency Report
- Lynx
- F12
- BBB
- Intent & AutoFill
- Security Images
- Multi Factor Authentication

- Update Update Update Update
- 3-2-1 Backup
- Security Suites   Defense in Depth
- MultiFactor authentication
- https
- VPN
- Deliberate mistakes on Data Entry
- Awareness

Safer

- Questions, suggestions, comments?

SCCCCyber@gmail.com