सी-डैक
CDAC

SESSION
ON
BROWSE SAFELY, RESPONSIBLE ONLINE BEHAVIOR AND PROTECTING ONLINE ACCOUNTS

Dr. Neha Bajpai
C-DAC, Noida

प्रगत संगणन विकास केन्द्र
Centre for Development of Advanced Computing
अनुसंधान भवन, सी-56/1, संस्थागत क्षेत्र, सैक्टर- 62, नोएडा- 201307 (उ.प्र.) भारत
Anusandhan Bhawan, C-56/1, Institutional Area, Sector- 62, Noida- 201307 (U.P.) India

A web application or web service is a software application that is accessible using a web browser or HTTP(s) user agent.

INFORMATION A USER SHARES

- Photos and other media
- Age and gender
- Biographical information (education, employment history, hometown, etc.)
- Status updates (also known as posts)
- Contacts
- Interests
- Geographical location
- Credentials

HOW DOES GOOGLE TRACK YOU ?

IG @HITECHHACKING

CHROME

Browser history,
website visited

YOUTUBE

Videos watched,
uploaded

MAPS

Locations visited,
place searched

HANGOUTS

Contacts,
conversations

PHOTOS

People and
places tagged

CALENDER

Upcoming plans,
appointments

SEARCH

Queries searched

GMAIL

Contacts, emails
sent, email content

SHOPPING

Prodects searched .
clicked on

ADS

Ads clicked,
topic intrested in

NEWS

News sites viewed,
stories read

DIGITAL FOOTPRINTS

It is the information that exists online about you and your activity.

Be Careful About –

- What you share
- Where you share
- With whom you share

DIGITAL FOOTPRINTS

There are two kinds of Digital Footprints -

- **Passive Digital Footprint**
- **Active Digital Footprint**

Be Smart About –

-**Sites you visit**

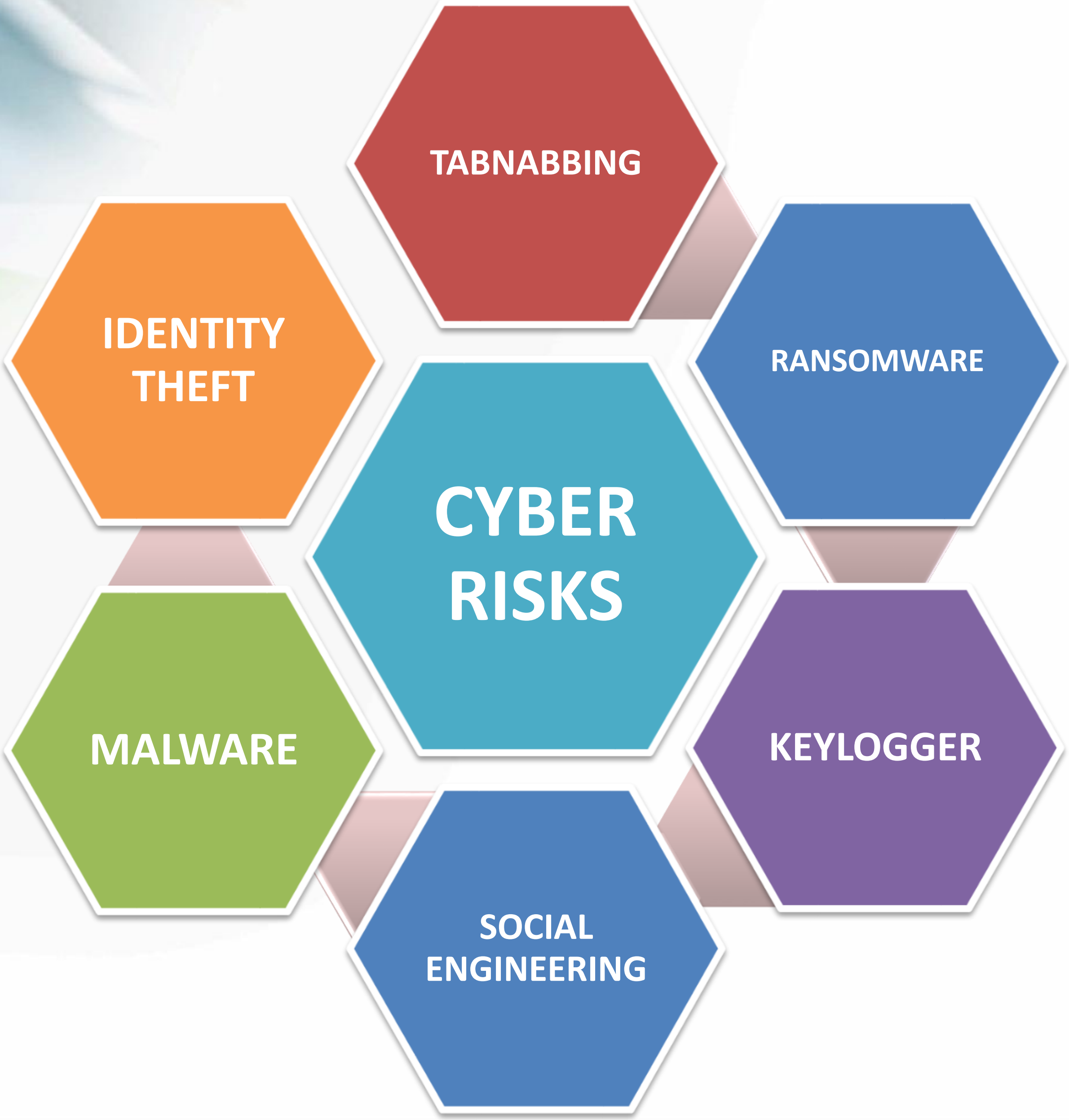
-**Emails you open**

-**Links you click**

HOW TO PRESERVE YOUR DIGITAL FOOTPRINT?

- Always think long term before posting.
- Avoid Making Virtual or Online Friends.
- Keep your personal information private.
- Verify the profile on different platforms like Linkedin, Twitter, Instagram and Facebook.
- Use privacy settings on social networking pages
- Protect your privacy by updating the settings on the Browser

CYBER RISKS



CYBER RISKS

TABNABBING

RANSOMWARE

KEYLOGGER

SOCIAL ENGINEERING

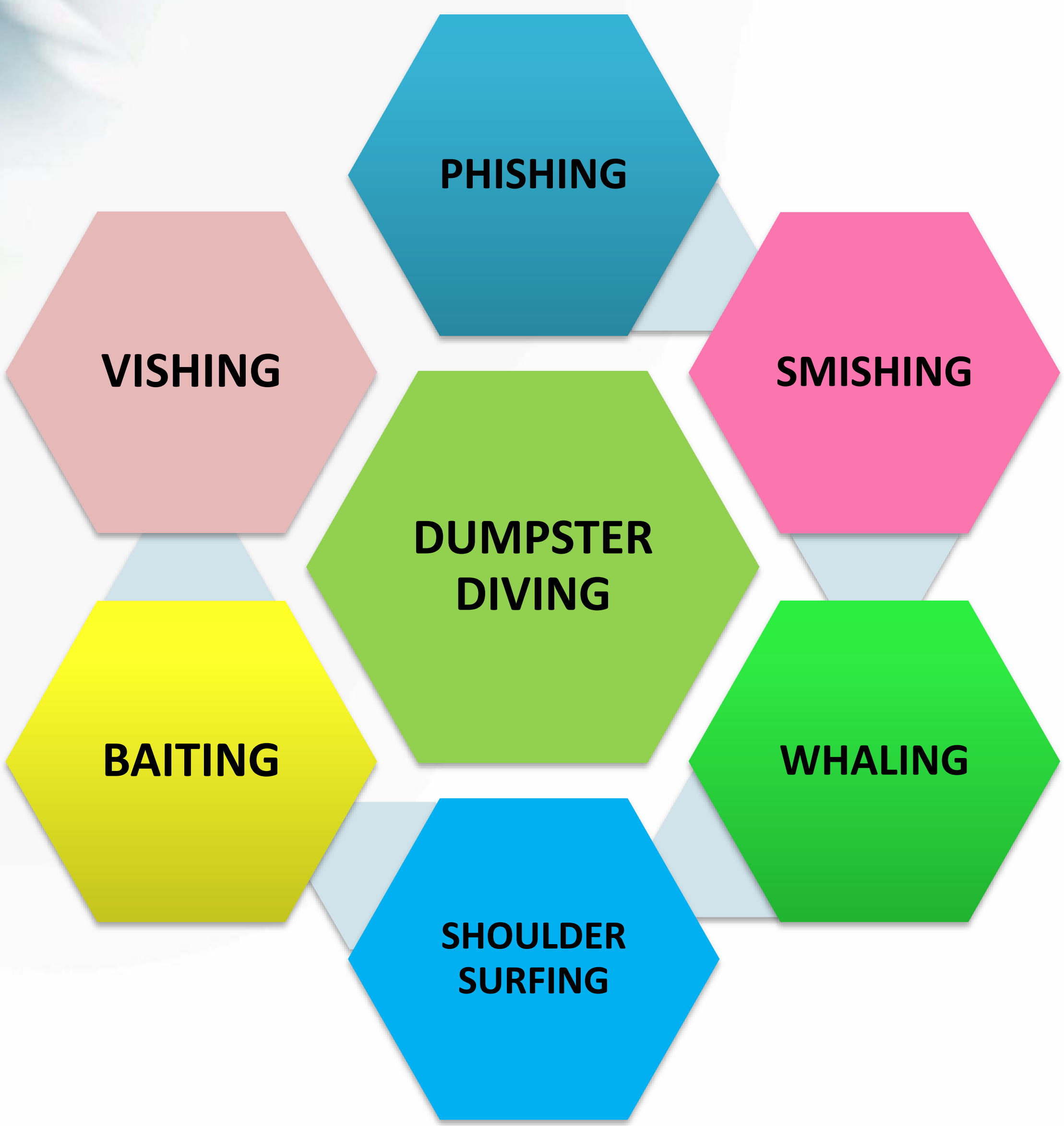
MALWARE

IDENTITY THEFT

Safe Browsing

- Use/Install Most Secure Internet Browser
- Customize Your Security Settings
- Block pop-up windows
- Confirm Site’s Security (https vs. http, green colored padlock)
- Be wary of clicking links in email or instant messages.
- Only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them.
- Keep your browsers up to date
- Use Incognito Window or Private Browsing
- Block pop-ups, plug-ins and phishing sites

SOCIAL ENGINEERING



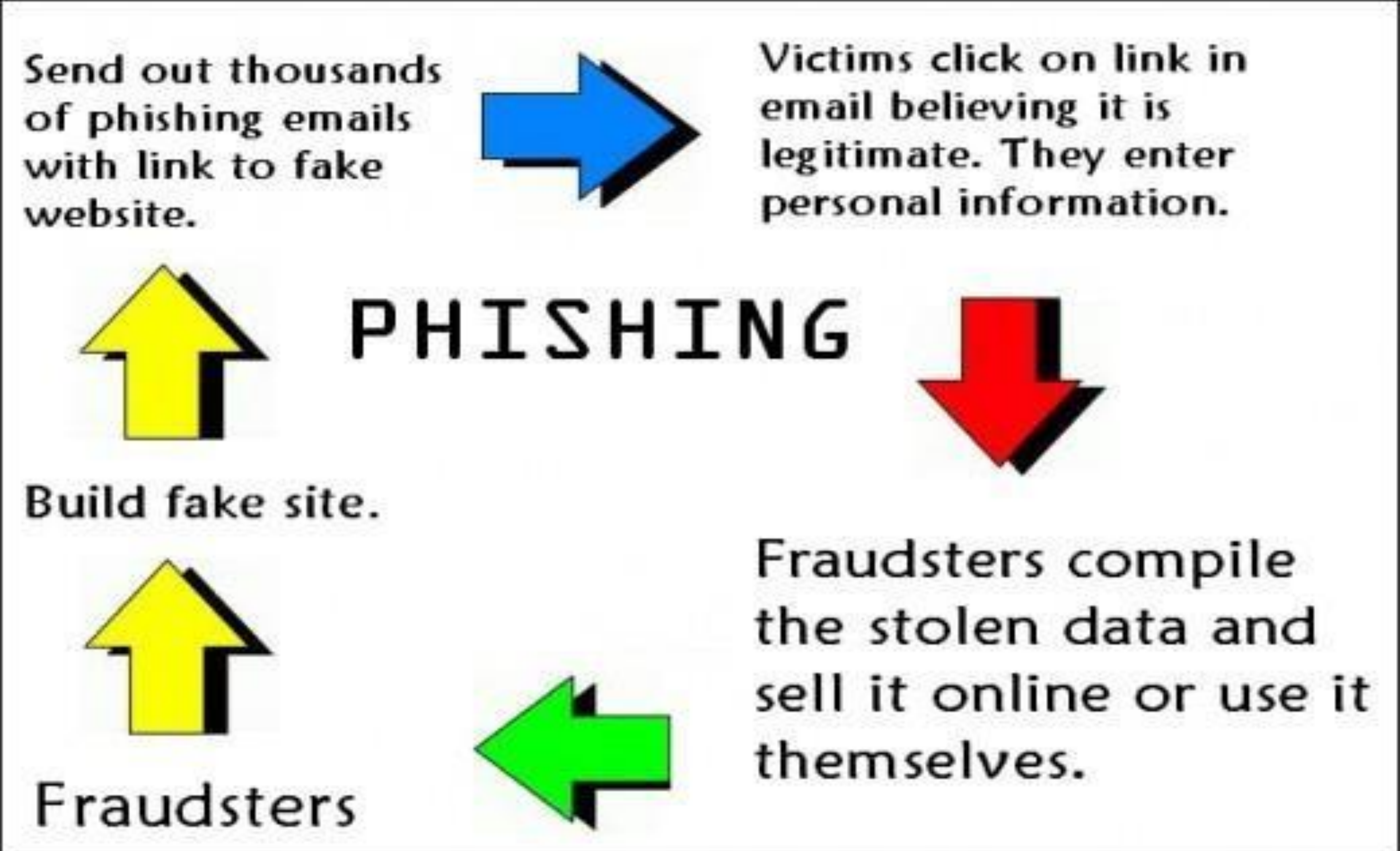
PHISHING

- E-mail sent by online criminals to trick you into going to fake Web sites and revealing personal information.
- In other words, It is the criminal attempting to acquire sensitive information such as-
  - **usernames**
  - **passwords**
  - **credit card details**

EXAMPLES OF PHISHING WEBSITES

- www.gmai1.com
- www.icici6ank.com
- www.bank0findia.com
- www.yah00.com

HOW IT HAPPENS?



PHISHING

Fraudsters

Build fake site.

Send out thousands of phishing emails with link to fake website.

Victims click on link in email believing it is legitimate. They enter personal information.

Fraudsters compile the stolen data and sell it online or use it themselves.

How To Identify Fake Phishing Website?

- Verify the URL of the webpage.
- Check the Padlock symbol.

- Establish the authenticity of the website by verifying its digital certificate.
- To do so,

Double click on the Padlock symbol at the upper right or bottom corner of your browser window.

HOW TO CHECK A WEBSITE IS GENUINE OR NOT?

Website Reputation Checker

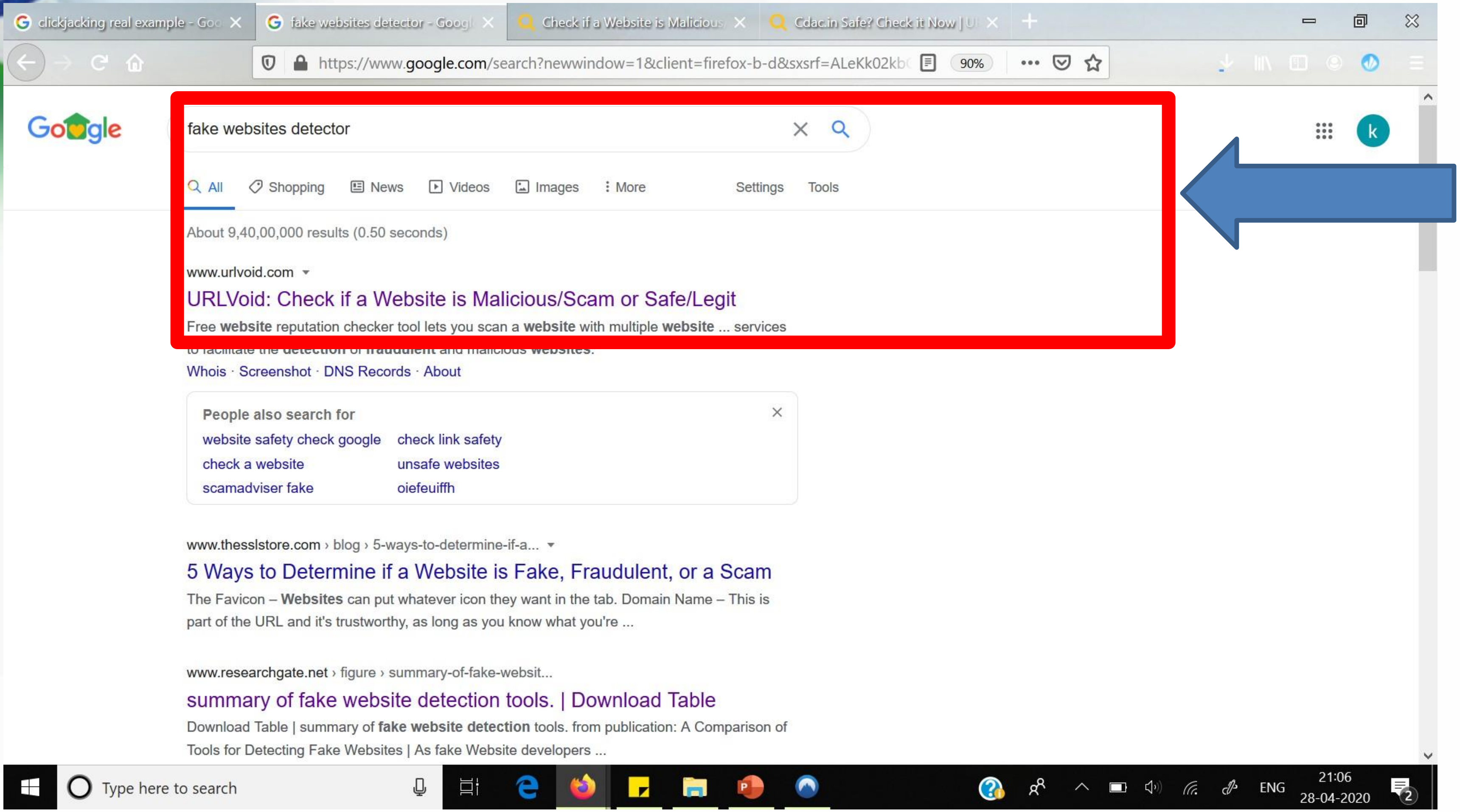
Free website reputation checker tool lets you scan a website with multiple website services to facilitate the detection of fraudulent and malicious websites.

- https://www.urlvoid.com/

➢**FEATURES**

- Multiple Blacklists
- Threat Analysis
- Safety Report

TYPE URLVoid in GOOGLE



fake websites detector

About 9,40,00,000 results (0.50 seconds)

www.urlvoid.com

URLVoid: Check if a Website is Malicious/Scam or Safe/Legit

Free **website** reputation checker tool lets you scan a **website** with multiple **website** ... services to facilitate the **detection** of **fraudulent** and malicious **websites**.

Whois · Screenshot · DNS Records · About

People also search for

website safety check google

check link safety

check a website

unsafe websites

scamadviser fake

oiefeuiffh

www.thesslstore.com › blog › 5-ways-to-determine-if-a...

5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam

The Favicon – **Websites** can put whatever icon they want in the tab. Domain Name – This is part of the URL and it's trustworthy, as long as you know what you're ...

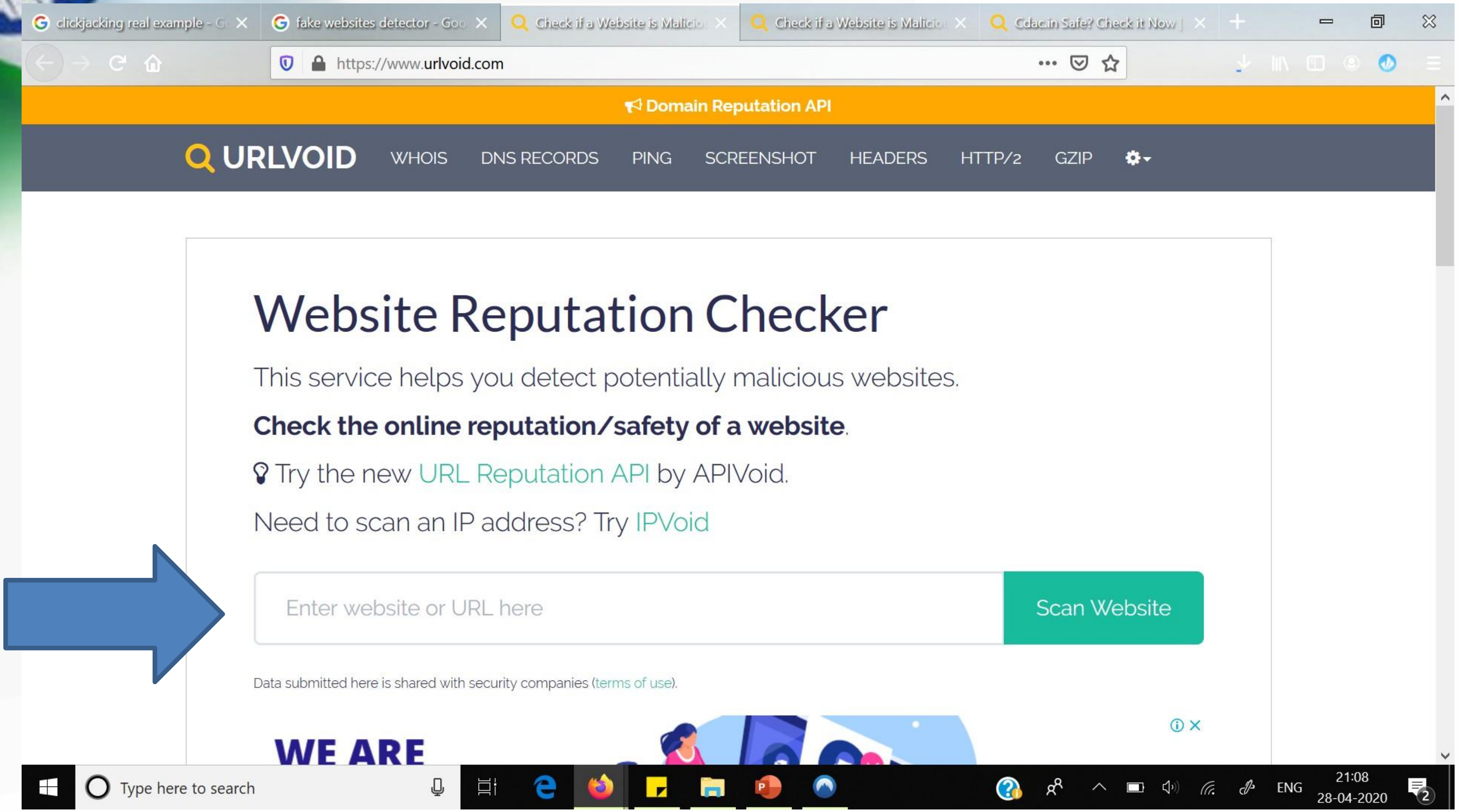
www.researchgate.net › figure › summary-of-fake-websit...

summary of fake website detection tools. | Download Table

Download Table | summary of **fake website detection** tools. from publication: A Comparison of Tools for Detecting Fake Websites | As fake Website developers ...

clickjacking real example - Goo
fake websites detector - Googl
Check if a Website is Malicious
Cdac.in Safe? Check it Now | U
https://www.google.com/search?newwindow=1&client=firefox-b-d&sxsrf=ALeKk02kb
90%
All
Shopping
News
Videos
Images
More
Settings
Tools
k
Type here to search
ENG
21:06
28-04-2020

TYPE THE WEBSITE URL



Website Reputation Checker

This service helps you detect potentially malicious websites.

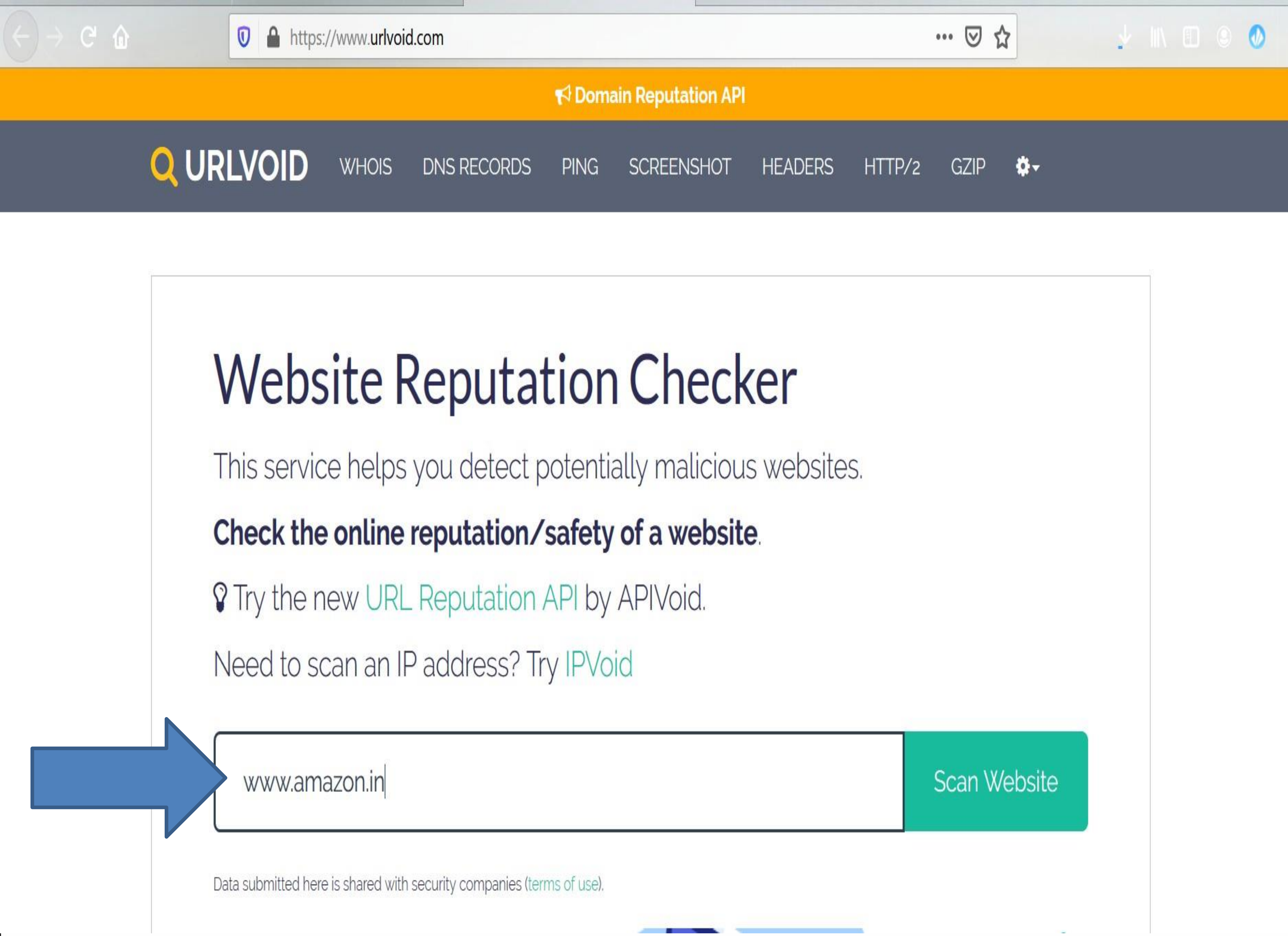
Check the online reputation/safety of a website.

Try the new URL Reputation API by APIVoid.

Need to scan an IP address? Try IPVoid

Enter website or URL here

Data submitted here is shared with security companies (terms of use).



Website Reputation Checker

This service helps you detect potentially malicious websites.

Check the online reputation/safety of a website.

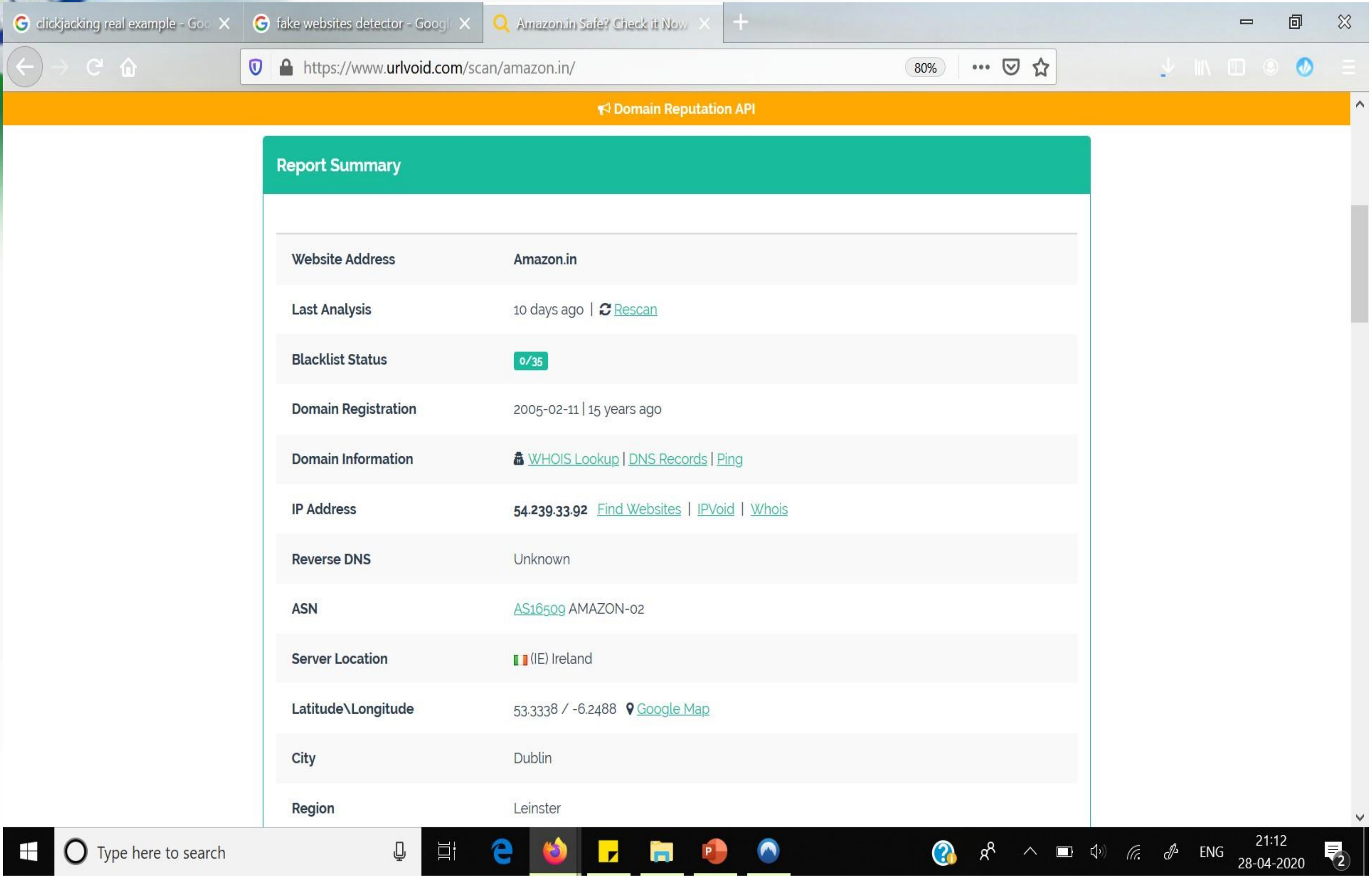
Try the new URL Reputation API by APIVoid.

Need to scan an IP address? Try IPVoid

www.amazon.in

Data submitted here is shared with security companies (terms of use).

REPORT SUMMARY


clickjacking real example - Goo
fake websites detector - Googl
Amazon.in Safe? Check it Now
https://www.urlvoid.com/scan/amazon.in/
80%
Domain Reputation API
Type here to search
ENG
21:12
28-04-2020

Report Summary

Website Address	Amazon.in
Last Analysis	10 days ago | Rescan
Blacklist Status	0/35
Domain Registration	2005-02-11 | 15 years ago
Domain Information	WHOIS Lookup | DNS Records | Ping
IP Address	54.239.33.92 Find Websites | IPVoid | Whois
Reverse DNS	Unknown
ASN	AS16509 AMAZON-02
Server Location	(IE) Ireland
Latitude\Longitude	53.3338 / -6.2488 Google Map
City	Dublin
Region	Leinster

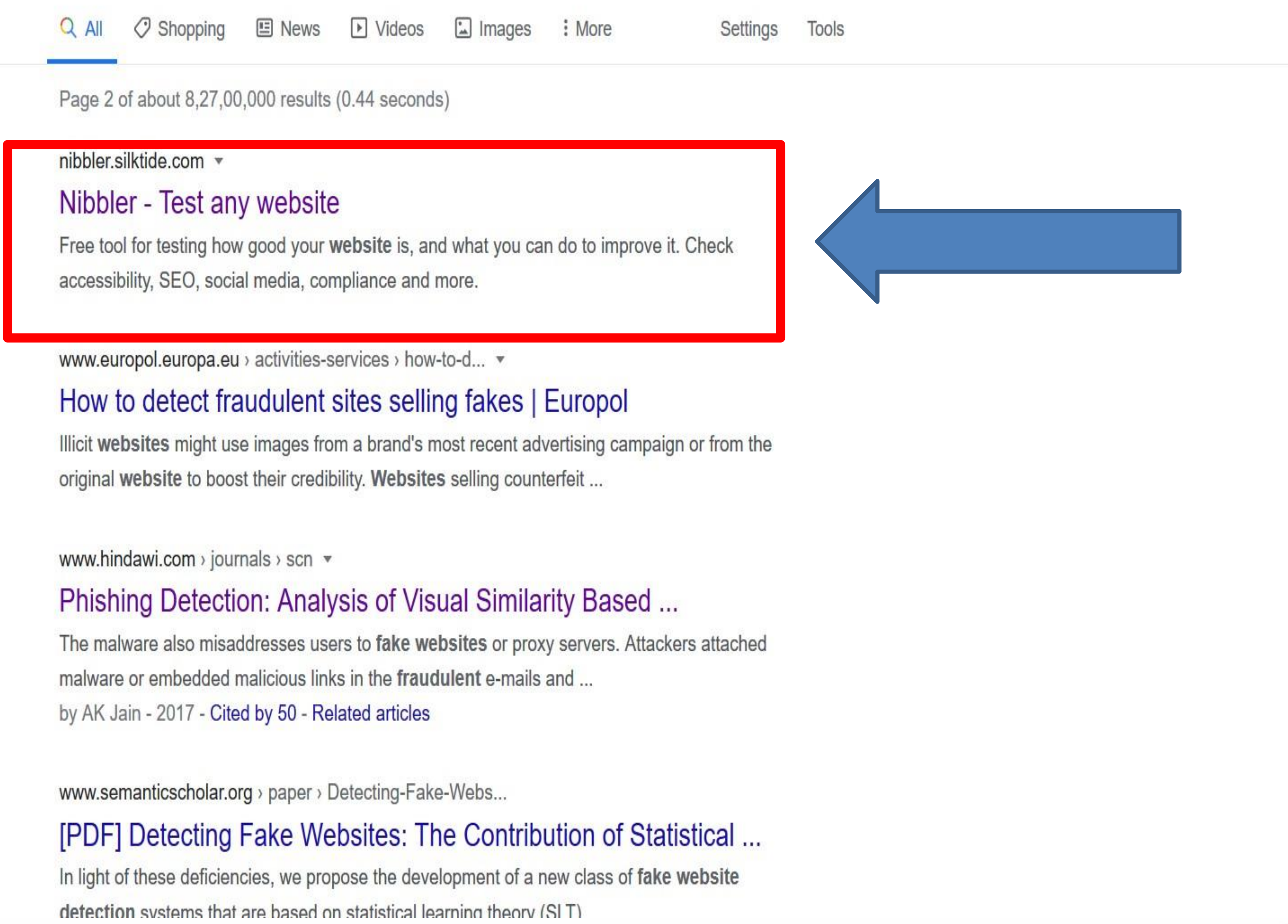
HOW TO CHECK A WEBSITE IS GENUINE OR NOT?

Nibbler

Nibbler is a free tool for testing websites.

https://nibbler.silktide.com/

SEARCH FOR NIBBLER



Page 2 of about 8,27,00,000 results (0.44 seconds)

nibbler.silktide.com

Nibbler - Test any website

Free tool for testing how good your **website** is, and what you can do to improve it. Check accessibility, SEO, social media, compliance and more.

www.europol.europa.eu › activities-services › how-to-d...

How to detect fraudulent sites selling fakes | Europol

Illicit **websites** might use images from a brand's most recent advertising campaign or from the original **website** to boost their credibility. **Websites** selling counterfeit ...

www.hindawi.com › journals › scn

Phishing Detection: Analysis of Visual Similarity Based ...

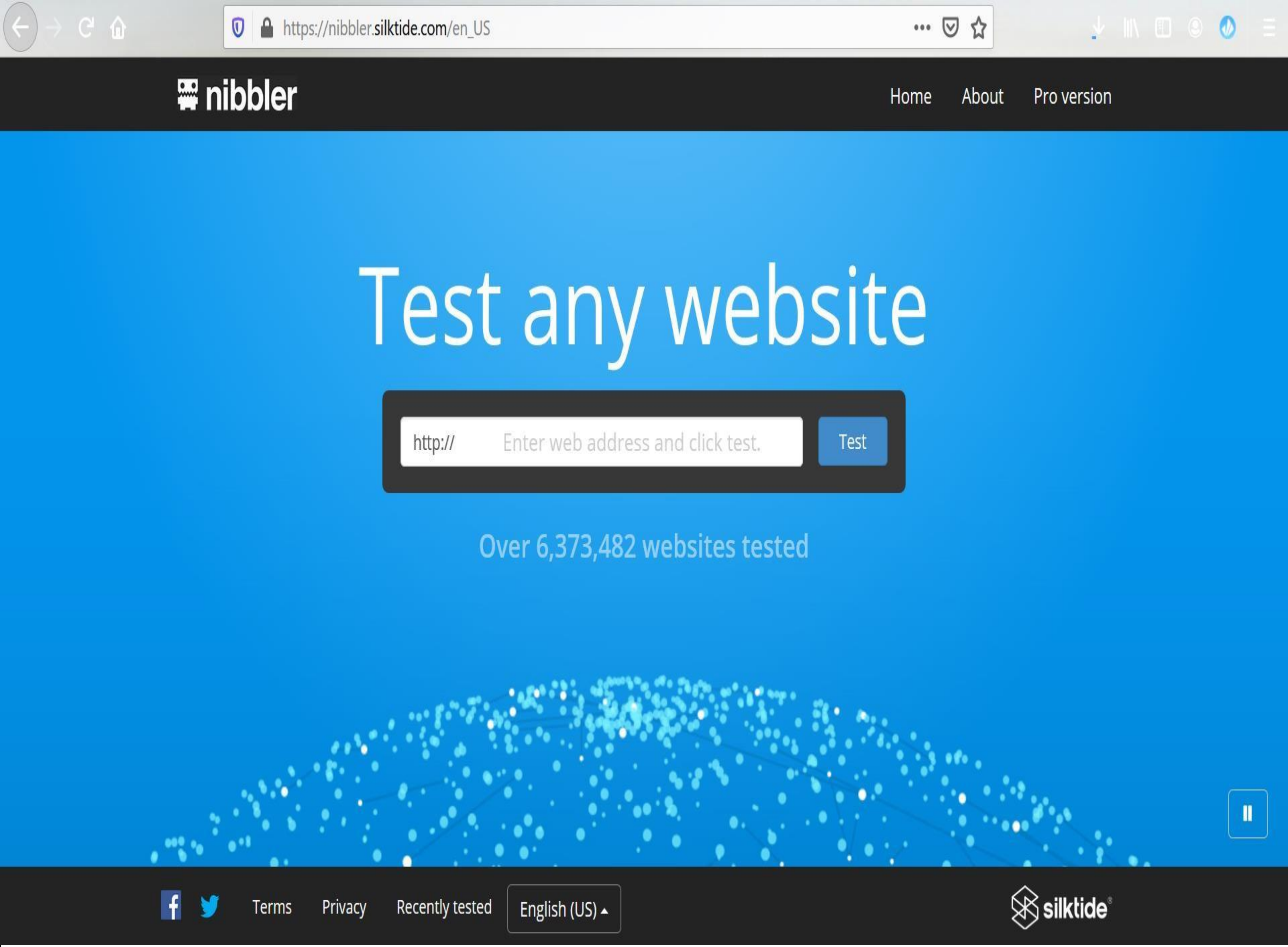
The malware also misaddresses users to **fake websites** or proxy servers. Attackers attached malware or embedded malicious links in the **fraudulent** e-mails and ...

by AK Jain - 2017 - Cited by 50 - Related articles

www.semanticscholar.org › paper › Detecting-Fake-Webs...

[PDF] Detecting Fake Websites: The Contribution of Statistical ...

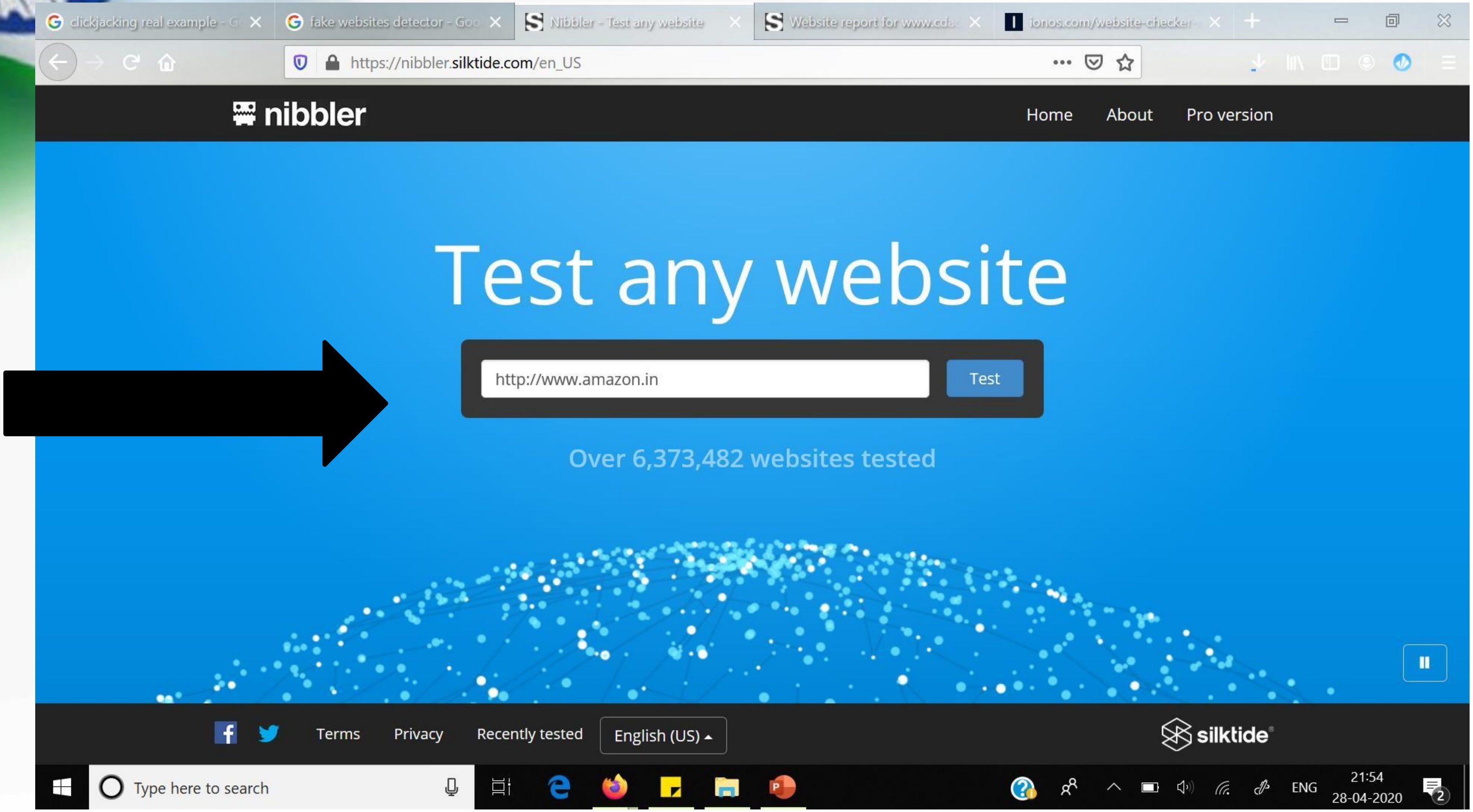
In light of these deficiencies, we propose the development of a new class of **fake website** **detection** systems that are based on statistical learning theory (SLT)



Test any website

Over 6,373,482 websites tested

ENTER URL


clickjacking real example - G
fake websites detector - Goo
Nibbler - Test any website
Website report for www.cdac
ionos.com/website-checker
https://nibbler.silktide.com/en_US
nibbler
Home
About
Pro version

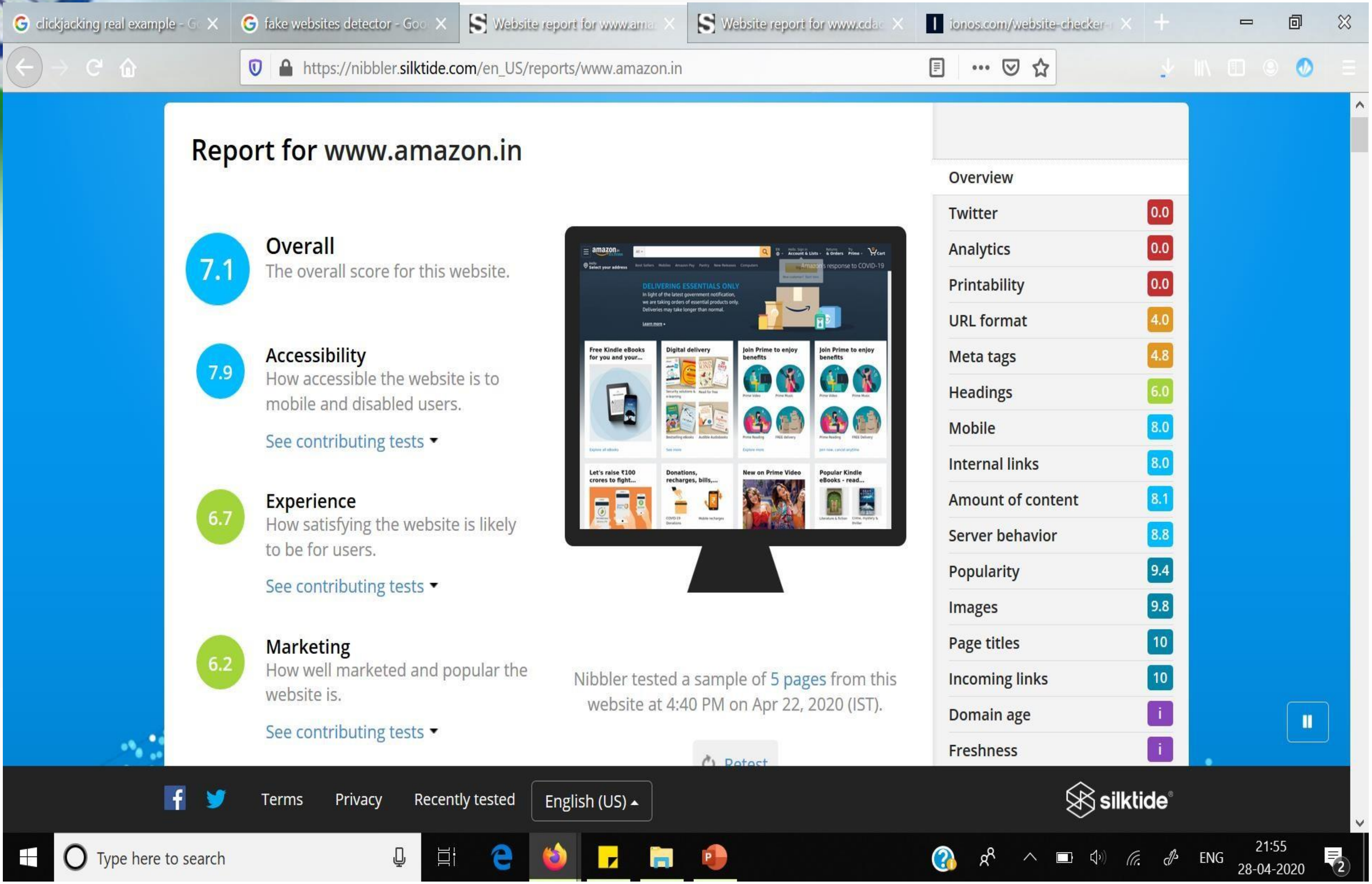
Test any website

http://www.amazon.in

Over 6,373,482 websites tested

Terms
Privacy
Recently tested
English (US)
silktide
Type here to search
ENG
21:54
28-04-2020

REPORT FOR THE SCANNED WEBSITE



clickjacking real example - Go
fake websites detector - Goo
Website report for www.ama
Website report for www.cdac
ionos.com/website-checker
https://nibbler.silktide.com/en_US/reports/www.amazon.in

Report for www.amazon.in

7.1 **Overall**
The overall score for this website.

7.9 **Accessibility**
How accessible the website is to mobile and disabled users.
See contributing tests ▾

6.7 **Experience**
How satisfying the website is likely to be for users.
See contributing tests ▾

6.2 **Marketing**
How well marketed and popular the website is.
See contributing tests ▾

Nibbler tested a sample of 5 pages from this website at 4:40 PM on Apr 22, 2020 (IST).

Retest

Overview	
Twitter	0.0
Analytics	0.0
Printability	0.0
URL format	4.0
Meta tags	4.8
Headings	6.0
Mobile	8.0
Internal links	8.0
Amount of content	8.1
Server behavior	8.8
Popularity	9.4
Images	9.8
Page titles	10
Incoming links	10
Domain age	i
Freshness	i

Browser Extensions

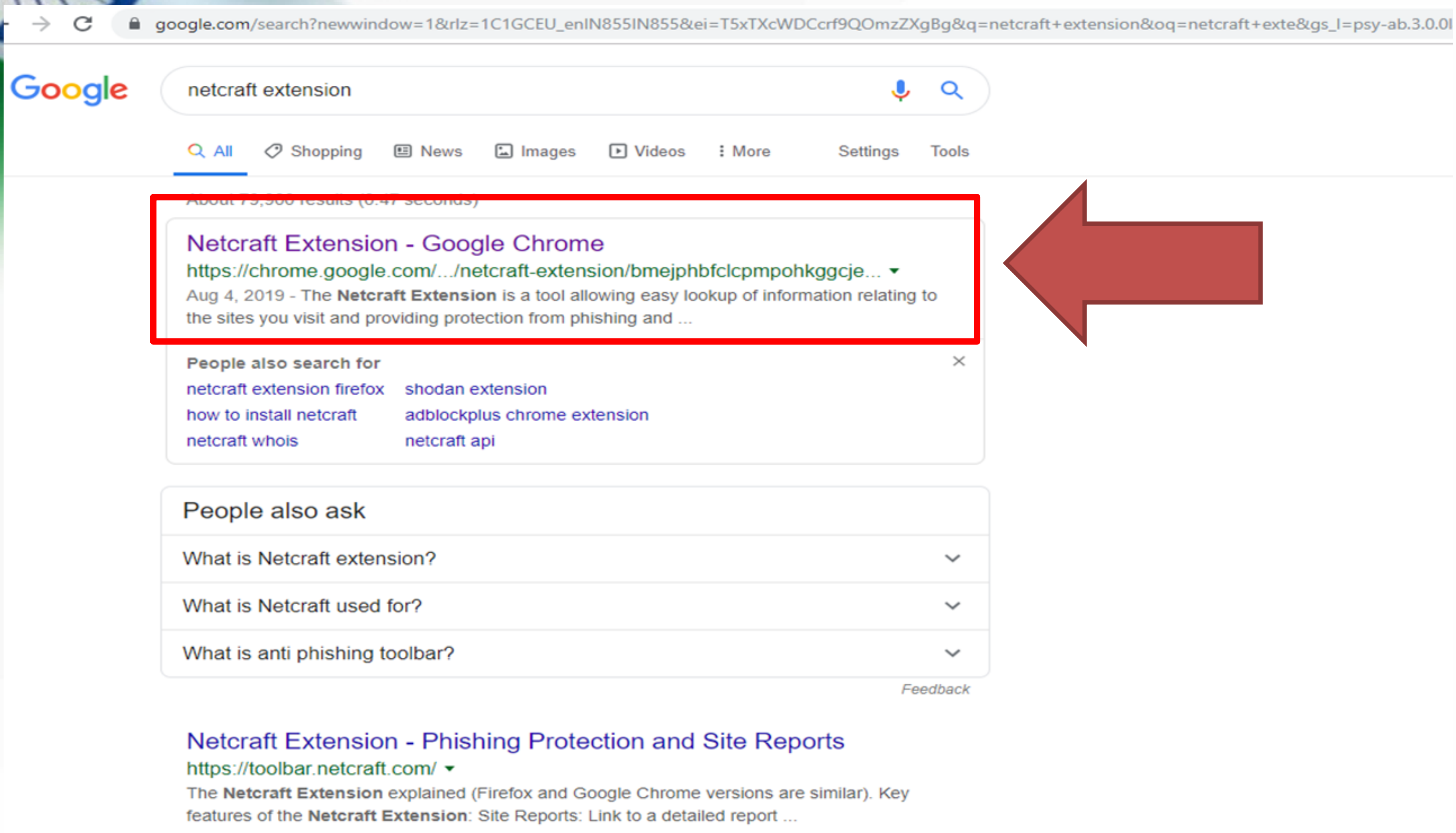
Netcraft

- The Netcraft Extension is a tool allowing easy lookup of information relating to the sites you visit and providing protection from phishing and malicious JavaScript.

Features

- Detailed site reports
- Risk Ratings
- Conveniently report suspected phishing & fraudulent sites
- Protection against Cross Site Scripting (XSS)
- Protection against Phishing sites
- Protection against malicious JavaScript

HOW TO INSTALL NETCRAFT



google.com/search?newwindow=1&rlz=1C1GCEU_enIN855IN855&ei=T5xTXcWDCcrf9QOmzZXgBg&q=netcraft+extension&oq=netcraft+exte&gs_l=psy-ab.3.0.0l

About 79,900 results (0.47 seconds)

Netcraft Extension - Google Chrome
https://chrome.google.com/.../netcraft-extension/bmejphbfclcpmpohkggcje...
Aug 4, 2019 - The **Netcraft Extension** is a tool allowing easy lookup of information relating to the sites you visit and providing protection from phishing and ...

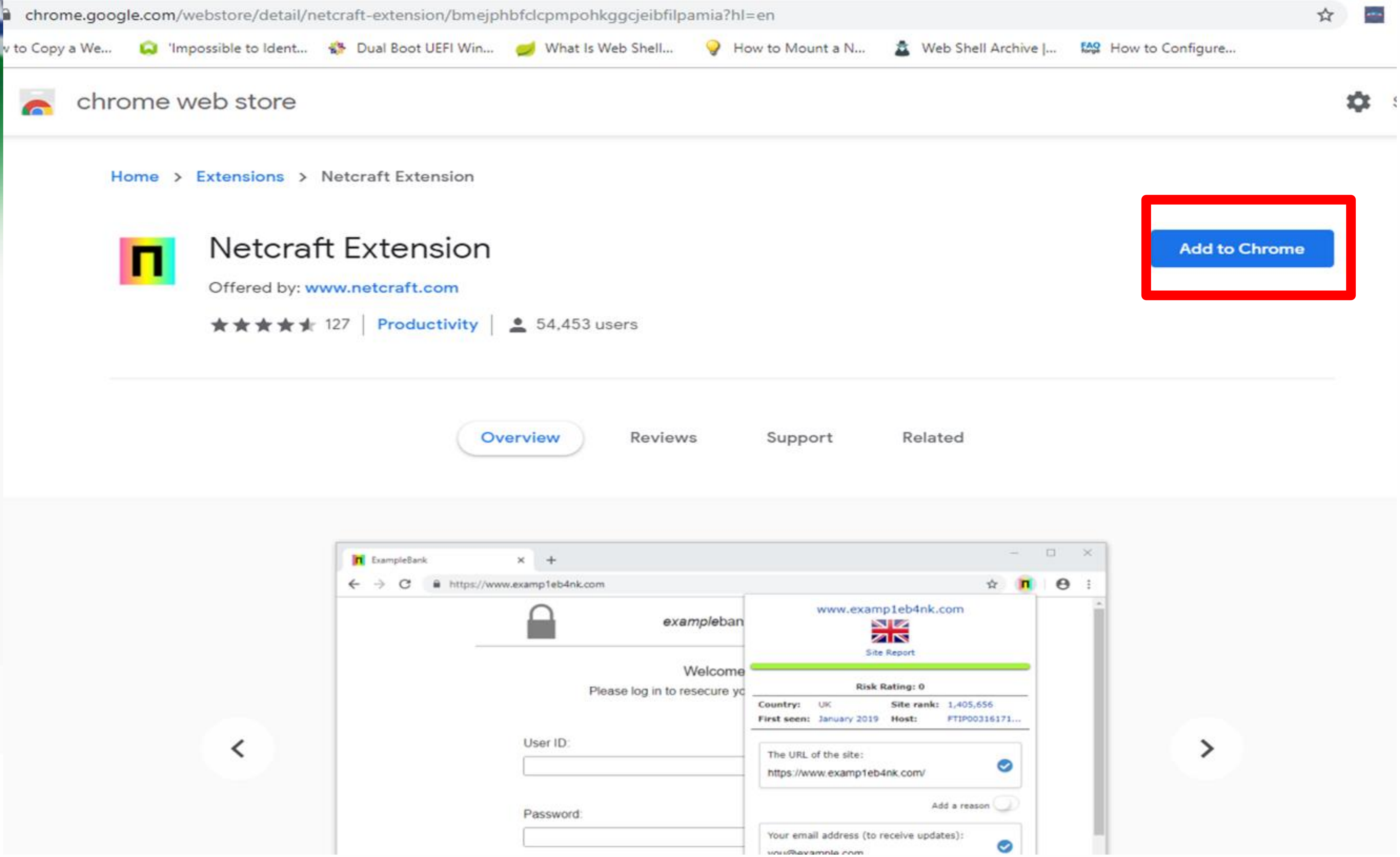
People also search for

netcraft extension firefox	shodan extension
how to install netcraft	adblockplus chrome extension
netcraft whois	netcraft api

People also ask

- What is Netcraft extension?
- What is Netcraft used for?
- What is anti phishing toolbar?

Netcraft Extension - Phishing Protection and Site Reports
https://toolbar.netcraft.com/
The **Netcraft Extension** explained (Firefox and Google Chrome versions are similar). Key features of the **Netcraft Extension**: Site Reports: Link to a detailed report ...



chrome.google.com/webstore/detail/netcraft-extension/bmejphbfclcpmpohkggcjeibfilpamia?hl=en

Home > Extensions > Netcraft Extension

Netcraft Extension

Offered by: www.netcraft.com

★★★★½ 127 | Productivity | 54,453 users

Please log in to resecure yo

User ID:

Password:

www.examp1eb4nk.com

Site Report

Risk Rating: 0

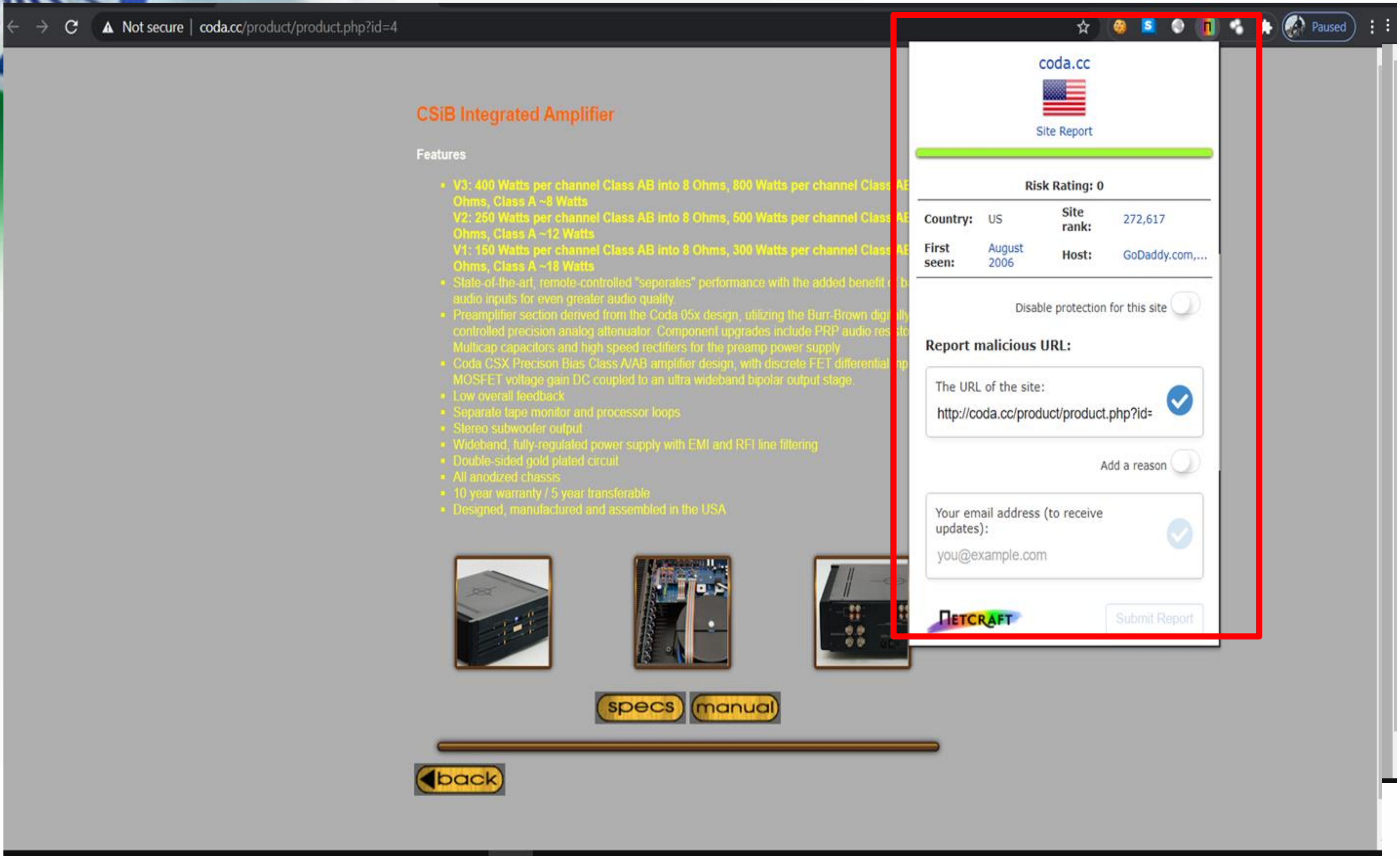
Country: UK Site rank: 1,405,656
First seen: January 2019 Host: FTIP00316171...

The URL of the site:
https://www.examp1eb4nk.com/

Add a reason

Your email address (to receive updates):
you@example.com

SCANNING RESULT OF WEBSITE



Not secure | coda.cc/product/product.php?id=4

Paused

CSiB Integrated Amplifier

Features

- **V3: 400 Watts per channel Class AB into 8 Ohms, 800 Watts per channel Class AE Ohms, Class A ~8 Watts**
  V2: 250 Watts per channel Class AB into 8 Ohms, 500 Watts per channel Class AE Ohms, Class A ~12 Watts
  V1: 150 Watts per channel Class AB into 8 Ohms, 300 Watts per channel Class AE Ohms, Class A ~18 Watts
- State-of-the-art, remote-controlled "seperates" performance with the added benefit b audio inputs for even greater audio quality.
- Preamplifier section derived from the Coda 05x design, utilizing the Burr-Brown digi lly controlled precision analog attenuator. Component upgrades include PRP audio res sto Multicap capacitors and high speed rectifiers for the preamp power supply
- Coda CSX Precison Bias Class A/AB amplifier design, with discrete FET differential np MOSFET voltage gain DC coupled to an ultra wideband bipolar output stage.
- Low overall feedback
- Separate tape monitor and processor loops
- Stereo subwoofer output
- Wideband, fully-regulated power supply with EMI and RFI line filtering
- Double-sided gold plated circuit
- All anodized chassis
- 10 year warranty / 5 year transferable
- Designed, manufactured and assembled in the USA

coda.cc

Site Report

Risk Rating: 0

Country:	US	**Site rank:**	272,617
First seen:	August 2006	**Host:**	GoDaddy.com,...

Disable protection for this site

Report malicious URL:

The URL of the site:
http://coda.cc/product/product.php?id=

Add a reason

Your email address (to receive updates):
you@example.com

NETCRAFT

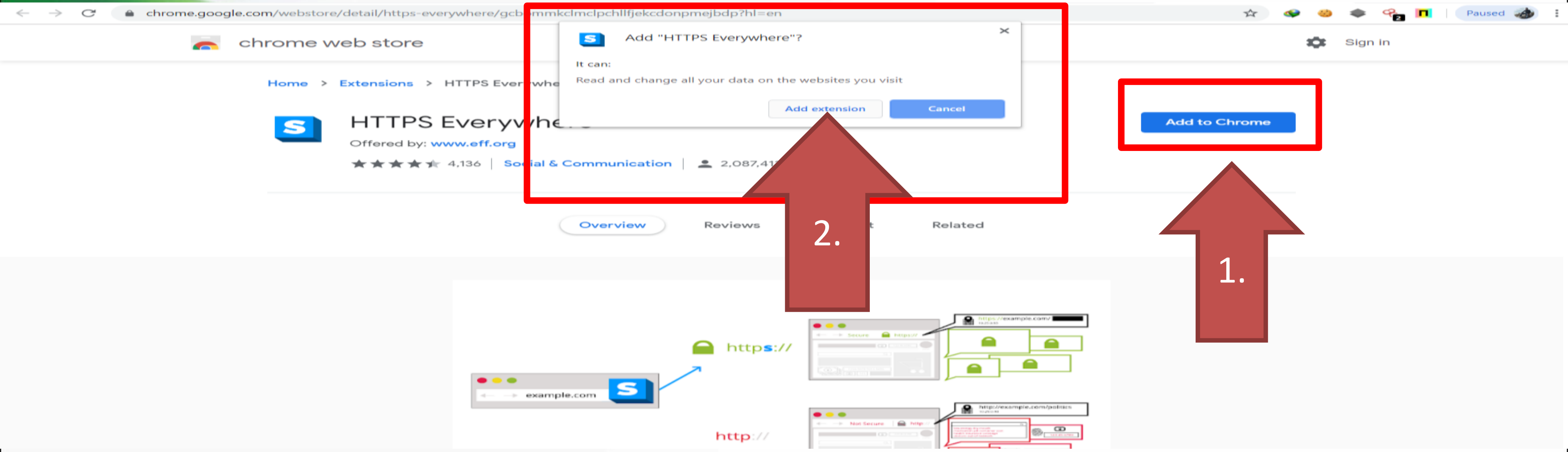
Submit Report

HTTPS Everywhere (Chrome Browser Extension)

- "HTTPS" is a website protocol that ensures a site is secure before you visit it.

- The Chrome extension, HTTPS Everywhere, rewrites the request you send to any website you want to visit in Chrome so you can be sure your browser produces the secure version of that site.

CLICK ON ADD TO CHROME



chrome.google.com/webstore/detail/https-everywhere/gcb mmkclmclpchllfjekcdonpmejbdp?hl=en

chrome web store

Home > Extensions > HTTPS Ever whe

HTTPS Everywhe

Offered by: www.eff.org

★★★★★ 4,136 | So ial & Communication | 2,087,41

Add "HTTPS Everywhere"?

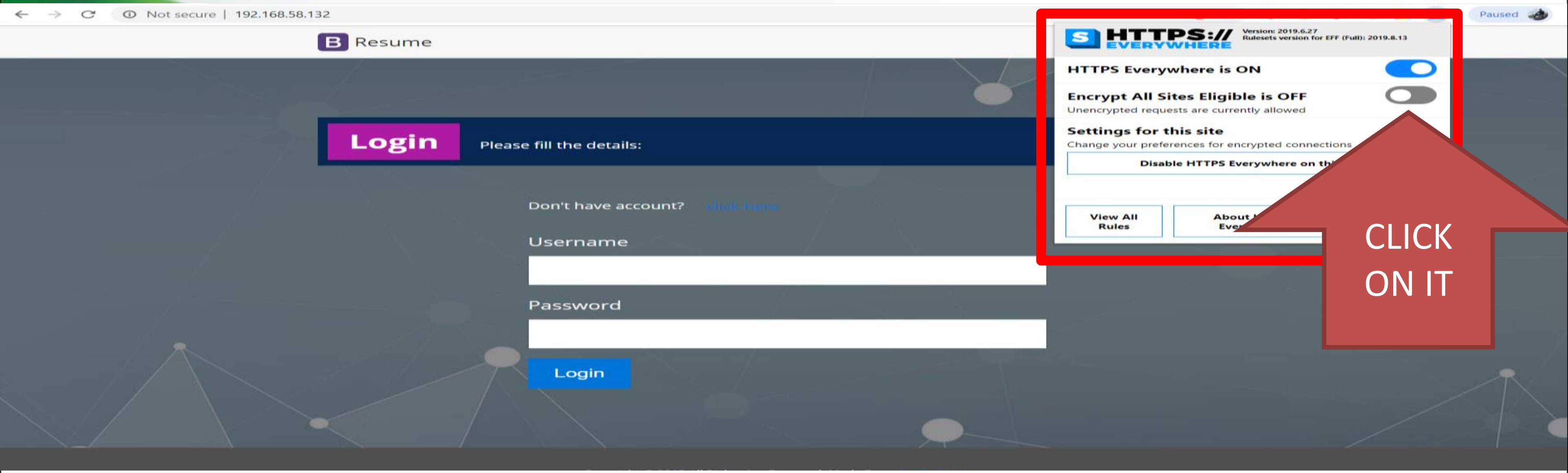
It can:

Read and change all your data on the websites you visit

Add extension   Cancel

Add to Chrome

CLICK ON ENCRYPT SITES



Version: 2019.6.27
Rulesets version for EFF (Full): 2019.8.13

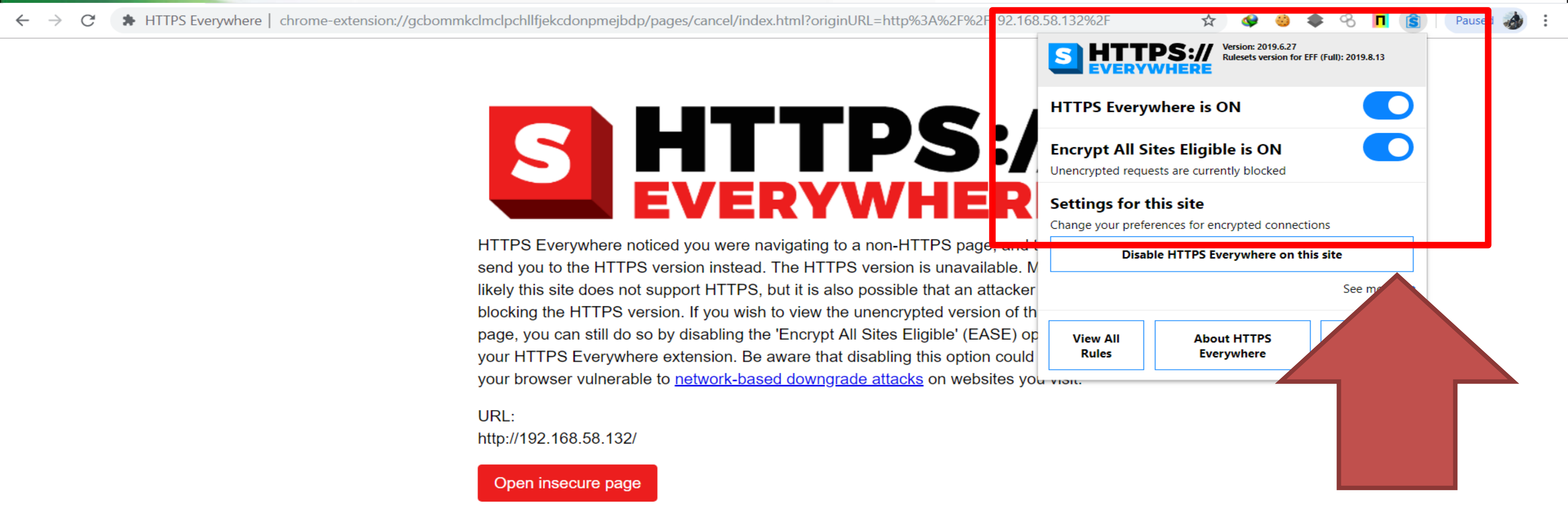
HTTPS Everywhere is ON

Encrypt All Sites Eligible is OFF
Unencrypted requests are currently allowed

Settings for this site
Change your preferences for encrypted connections

CLICK ON IT

CLICK ON ENCRYPT SITES



HTTPS Everywhere | chrome-extension://gcbommkclmclpchllfjekcdonpmejbdp/pages/cancel/index.html?originURL=http%3A%2F%2F192.168.58.132%2F
Paused
HTTPS:// EVERYWHERE

Version: 2019.6.27
Rulesets version for EFF (Full): 2019.8.13

HTTPS Everywhere is ON

Encrypt All Sites Eligible is ON
Unencrypted requests are currently blocked

Settings for this site
Change your preferences for encrypted connections

Disable HTTPS Everywhere on this site
See m
View All Rules
About HTTPS Everywhere
HTTPS:/ EVERYWHER

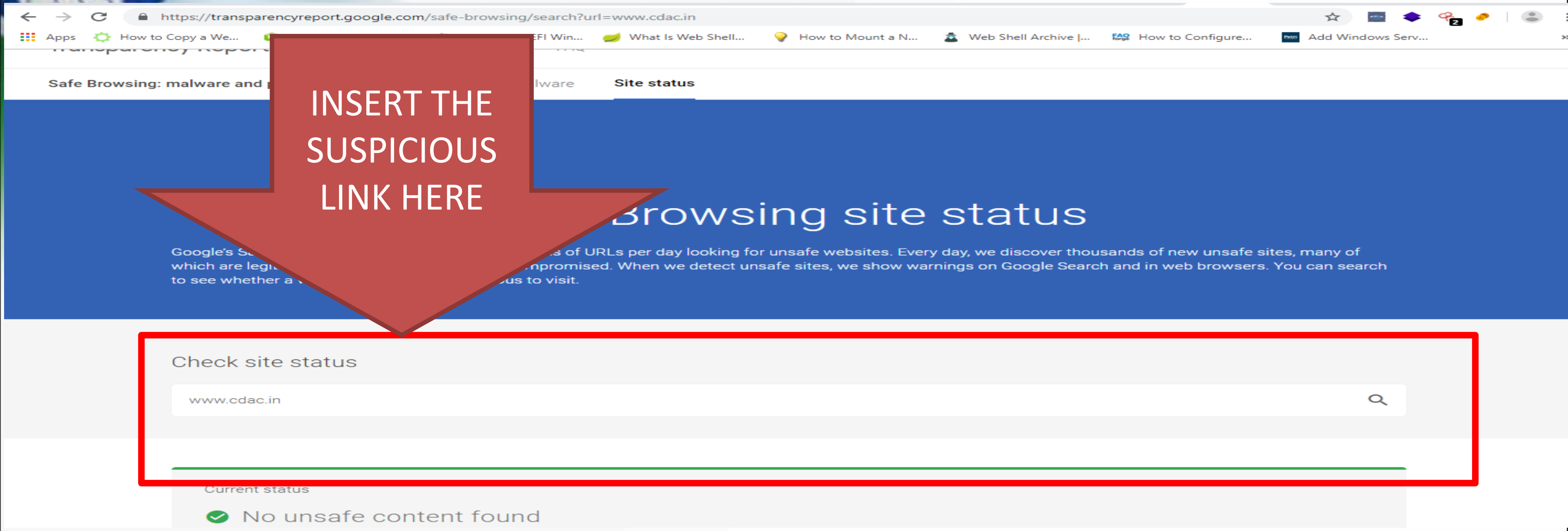
HTTPS Everywhere noticed you were navigating to a non-HTTPS page, and t
send you to the HTTPS version instead. The HTTPS version is unavailable. M
likely this site does not support HTTPS, but it is also possible that an attacker
blocking the HTTPS version. If you wish to view the unencrypted version of th
page, you can still do so by disabling the 'Encrypt All Sites Eligible' (EASE) op
your HTTPS Everywhere extension. Be aware that disabling this option could
your browser vulnerable to network-based downgrade attacks on websites you visit.

URL:
http://192.168.58.132/

Google Safe Browsing

- Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites.

- Every day, it discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised.



INSERT THE SUSPICIOUS LINK HERE

Browsing site status

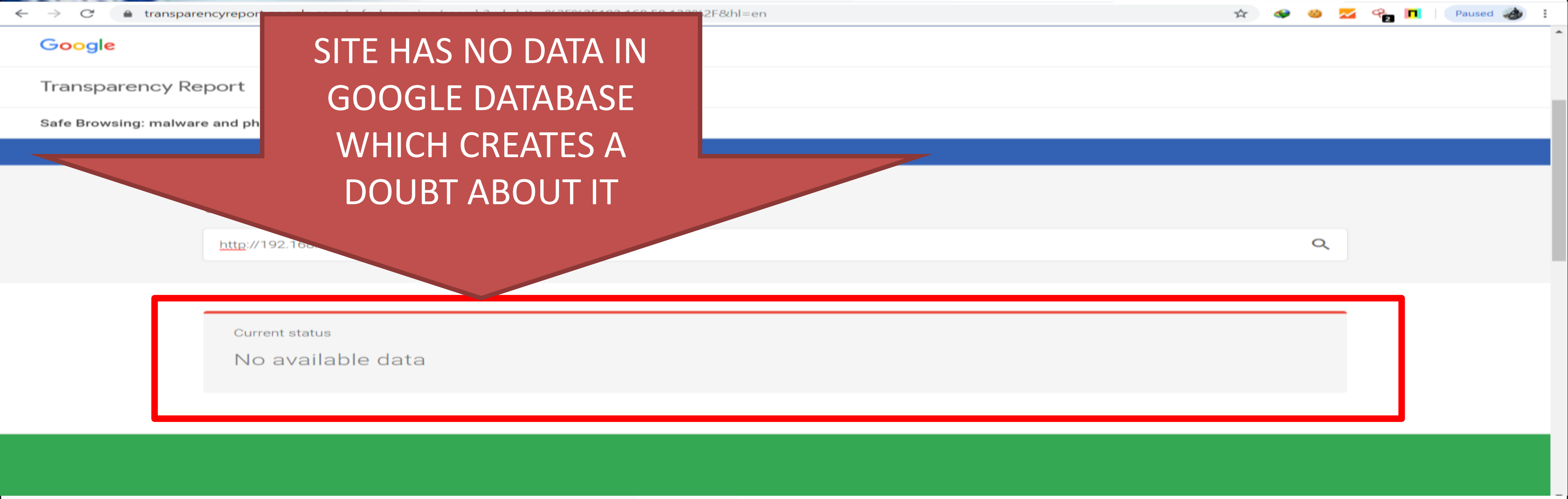
Google's S… …s of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legi… …npromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a … …us to visit.

Check site status

www.cdac.in

Current status

✓ No unsafe content found



transparencyrepor… 2F&hl=en

Google

Transparency Report

Safe Browsing: malware and ph

http://192.16…

Current status

No available data

SITE HAS NO DATA IN GOOGLE DATABASE WHICH CREATES A DOUBT ABOUT IT

PASSWORD SECURITY

VARIOUS TECHNIQUES USED BY HACKERS/CRACKERS TO RETRIEVE YOUR PASSWORDS

SHOULDER SURFING

BRUTE FORCE ATTACKS

DICTIONARY ATTACK

DON'T
Write passwords anywhere
Give passwords anyone over phone
Send passwords via email

SWITCH TO PASSPHRASE

MY PASSPHRASE

☞ **Never judge a book by its cover**

MY PASSWORD

☞ **nj@66!C**

☞ **N**ever **j**udge **@ 6**ook **6**y **!**ts **c**over

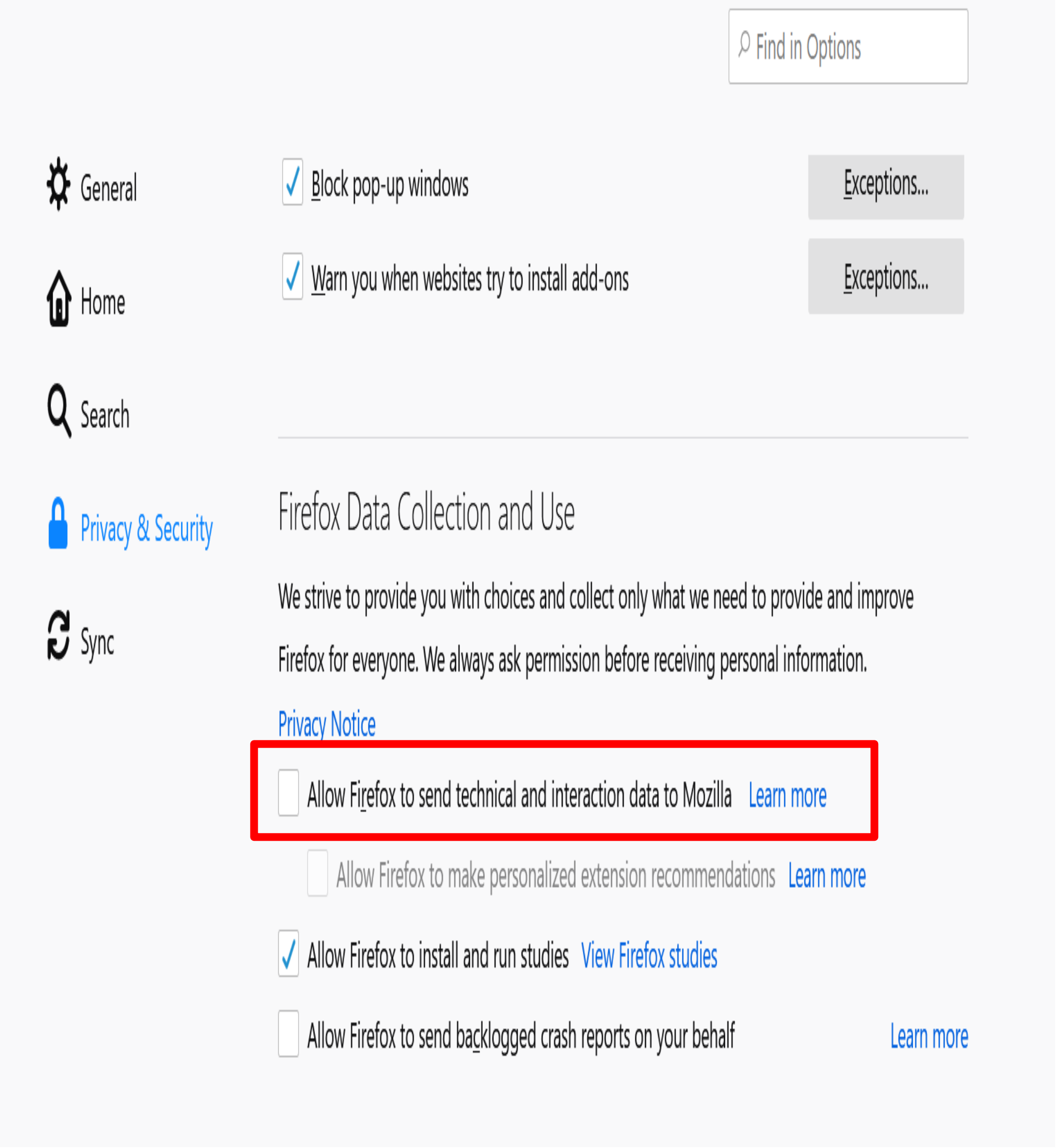
BEST PRACTICES TO KEEP PASSWORD SAFE

- Use a different Password for each Service
- Use a long and complex Password
- Change Password regularly
- Do not use your passwords on a shared computer
- Test your Password
- Use Passphrase

BROWSER SECURITY

DISABLE TELEMETRY

- To disable go to Open Menu (three bars at the top right corner of the browser) > **Options** > **Privacy & Security** > **Firefox Data Collection** and Use and then **uncheck the boxes** as you see below:
- **disable telemetry firefox**



☑ Block pop-up windows

☑ Warn you when websites try to install add-ons

Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.

Privacy Notice

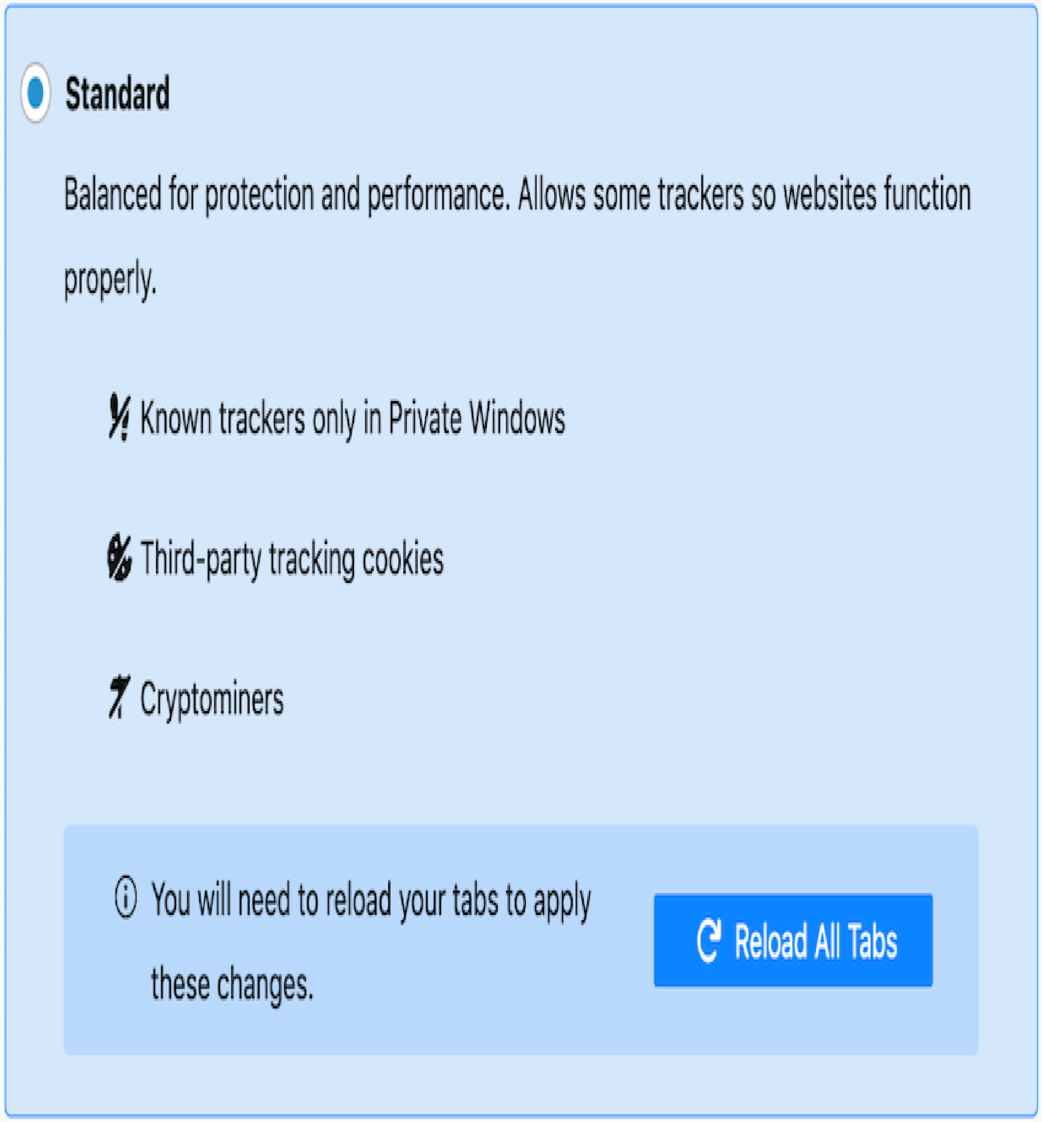
□ Allow Firefox to send technical and interaction data to Mozilla Learn more

□ Allow Firefox to make personalized extension recommendations Learn more

☑ Allow Firefox to install and run studies View Firefox studies

□ Allow Firefox to send backlogged crash reports on your behalf Learn more

- To adjust the Firefox Content Blocking settings, go to **Menu** > **Options** > **Privacy and Security** > **Content Blocking** and then select which mode you want to use.



● Standard

Balanced for protection and performance. Allows some trackers so websites function properly.

Known trackers only in Private Windows

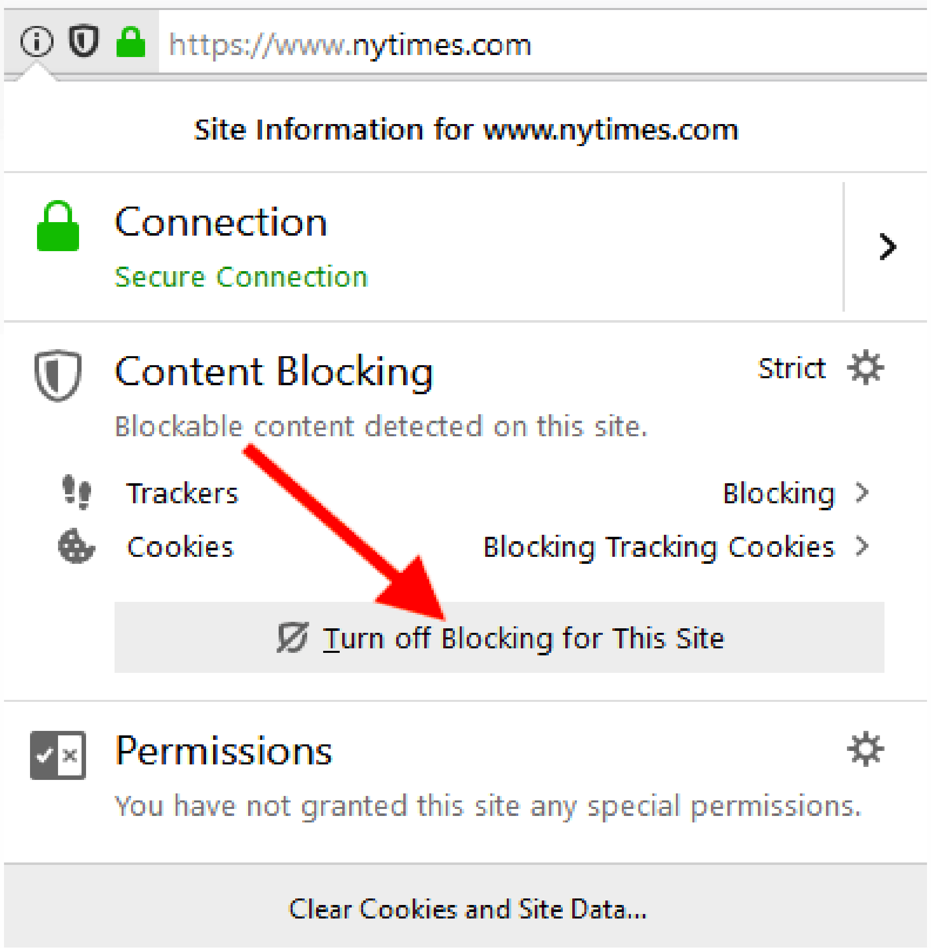
Third-party tracking cookies

Cryptominers

ⓘ You will need to reload your tabs to apply these changes.

DISABLE CONTENT BLOCKING FOR SPECIFIC SITES

- It’s easy to disable content blocking for certain trusted sites. Simply enter the website URL, then click the **“i”** icon to the left of the address bar, then click the grey button to **“Turn off Blocking for This Site.”**
- **turn off** content blocking firefox



https://www.nytimes.com

Site Information for www.nytimes.com

Connection

Secure Connection

Content Blocking — Strict

Blockable content detected on this site.

Trackers	Blocking ›
Cookies	Blocking Tracking Cookies ›

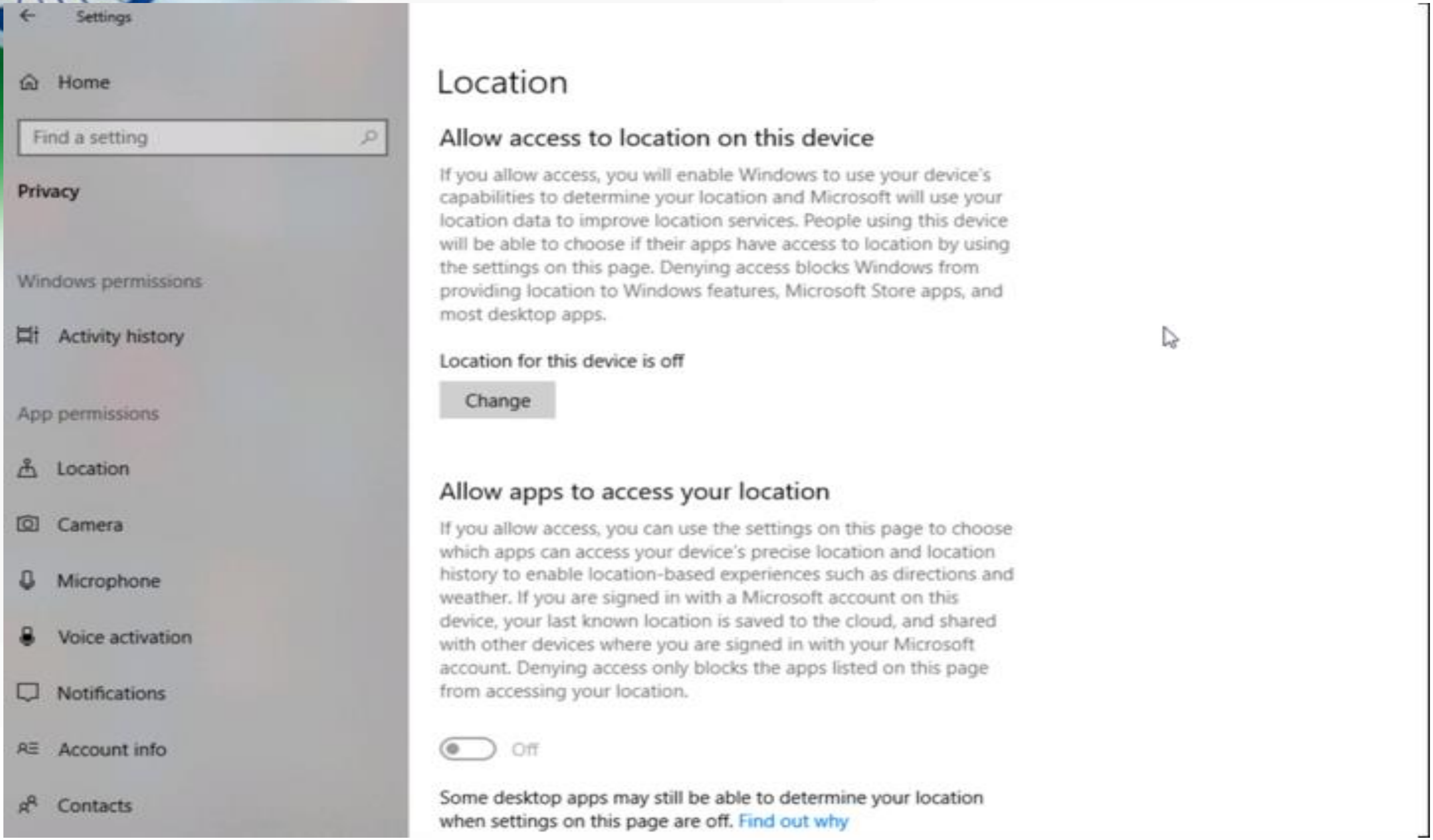
Turn off Blocking for This Site

Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data...

CHECK WHETHER YOU ARE SHARING THE LOCATION



Location

Allow access to location on this device

If you allow access, you will enable Windows to use your device's capabilities to determine your location and Microsoft will use your location data to improve location services. People using this device will be able to choose if their apps have access to location by using the settings on this page. Denying access blocks Windows from providing location to Windows features, Microsoft Store apps, and most desktop apps.

Location for this device is off

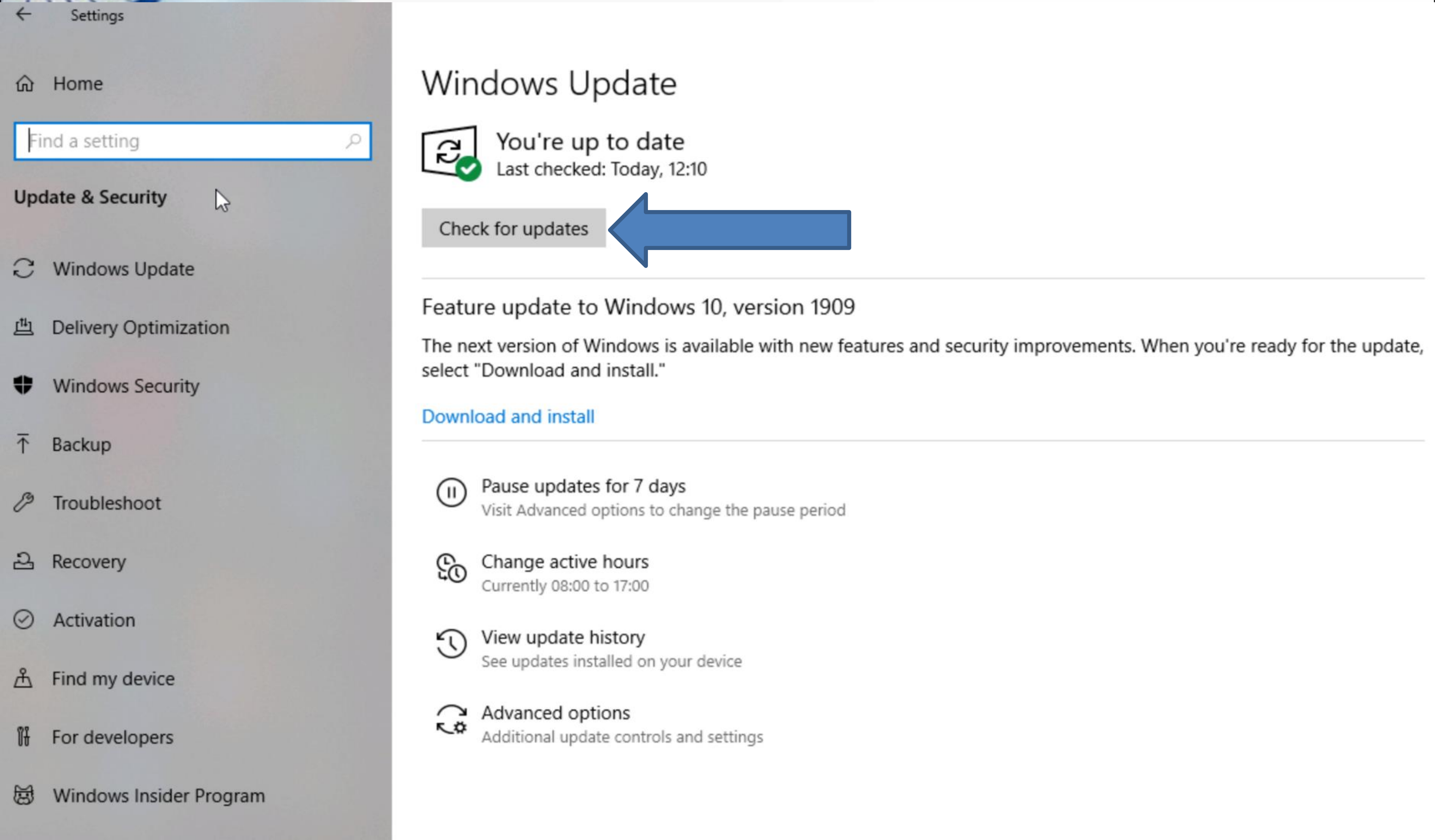
Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

○ Off

Some desktop apps may still be able to determine your location when settings on this page are off. Find out why

CHECK FOR THE UPDATES REGULARLY



Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Backup

Troubleshoot

Recovery

Activation

Find my device

For developers

Windows Insider Program

Windows Update

You're up to date
Last checked: Today, 12:10

Check for updates

Feature update to Windows 10, version 1909

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install."

Download and install

Pause updates for 7 days
Visit Advanced options to change the pause period

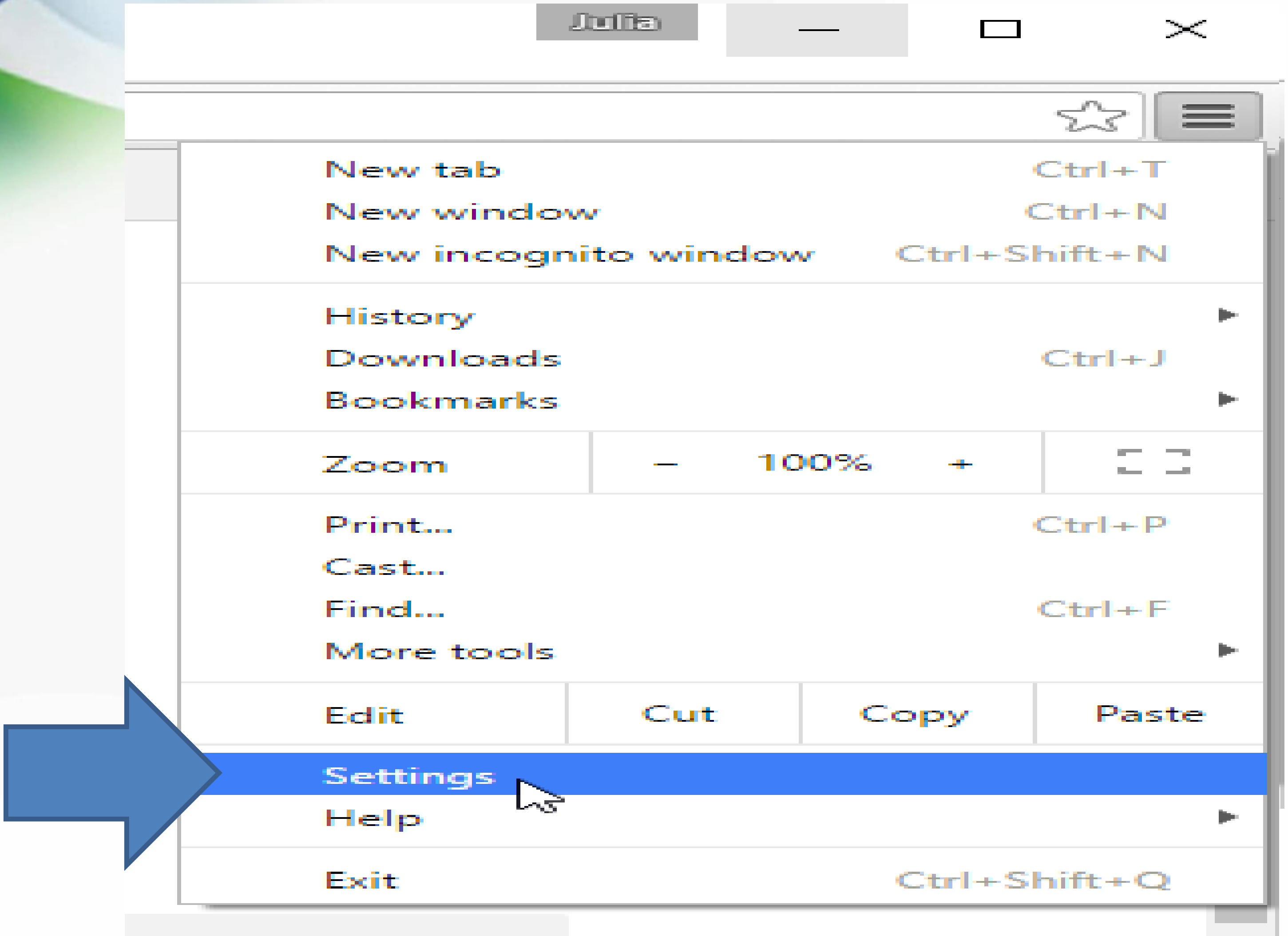
Change active hours
Currently 08:00 to 17:00

View update history
See updates installed on your device

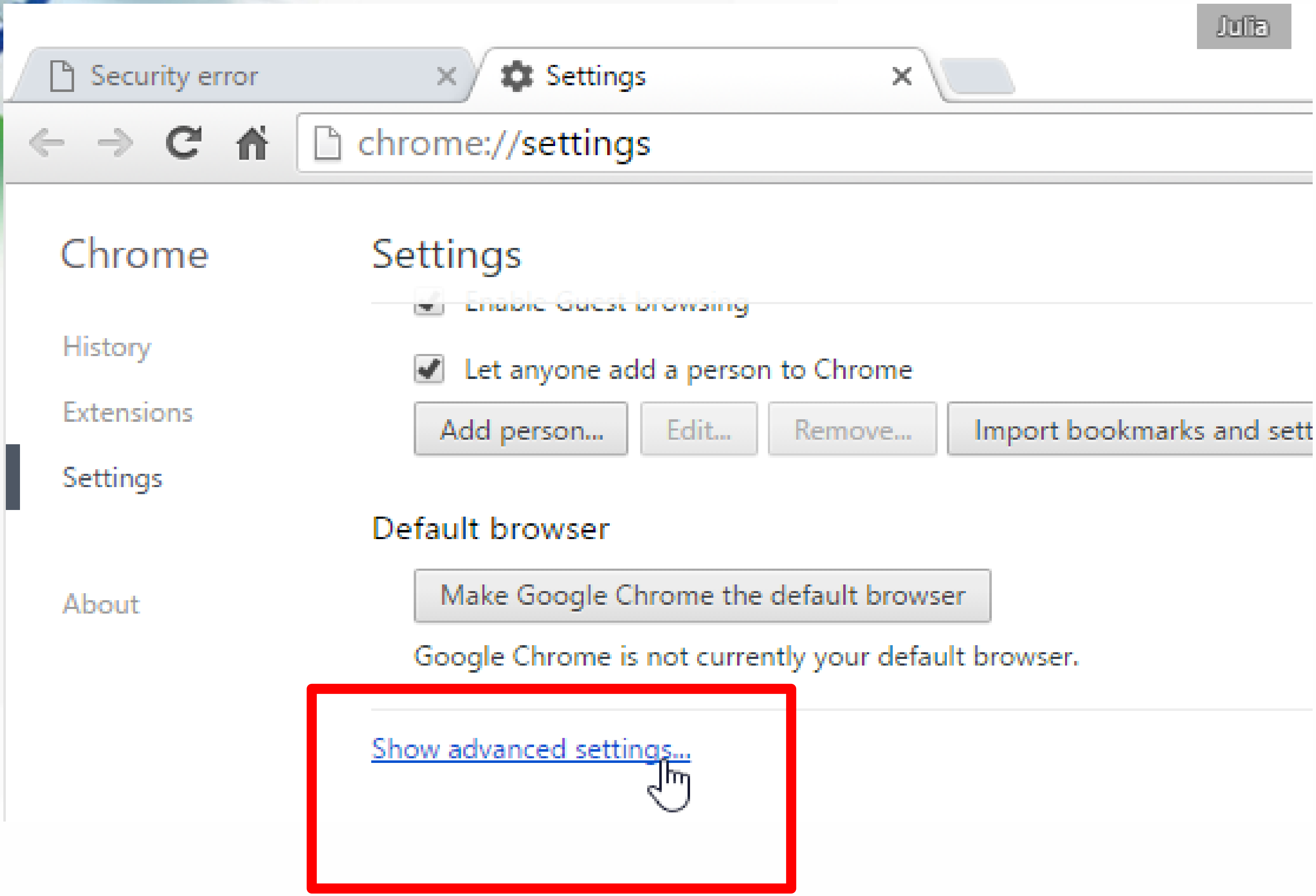
Advanced options
Additional update controls and settings

PRIVACY SETTINGS IN CHROME

Click the **Chrome menu** in the top-right corner of the browser, then select **Settings**.



The **Settings** tab will appear. Locate and select **Show advanced settings**.



Settings

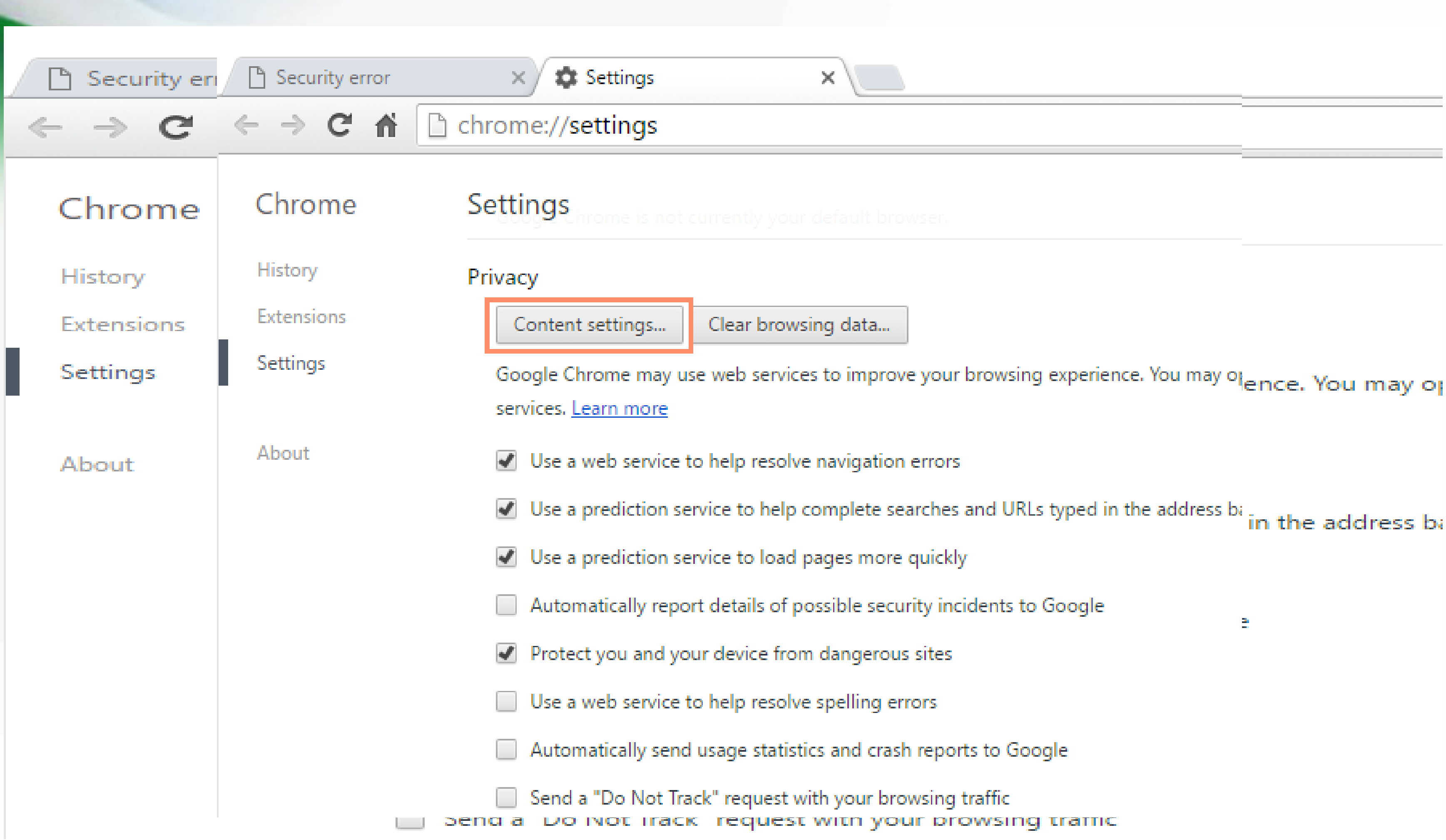
☑ Enable Guest browsing

☑ Let anyone add a person to Chrome

Default browser

Google Chrome is not currently your default browser.

The **privacy settings** will appear. To modify **basic privacy settings**, like enabling malware protection, check or uncheck the boxes next to each option.



Settings

Privacy

Google Chrome may use web services to improve your browsing experience. You may o services. Learn more

☑ Use a web service to help resolve navigation errors

☑ Use a prediction service to help complete searches and URLs typed in the address b

☑ Use a prediction service to load pages more quickly

□ Automatically report details of possible security incidents to Google

☑ Protect you and your device from dangerous sites

□ Use a web service to help resolve spelling errors

□ Automatically send usage statistics and crash reports to Google

□ Send a "Do Not Track" request with your browsing traffic

□ Send a "Do Not Track" request with your browsing traffic

FACEBOOK PRIVACY

FACEBOOK CLONING

What is Facebook Cloning?

Facebook cloning describes a technique in which scammers create a fake Facebook profile by using images and other information stolen from a targeted user’s real Facebook profile.

WHY WOULD SCAMMERS DO THIS?

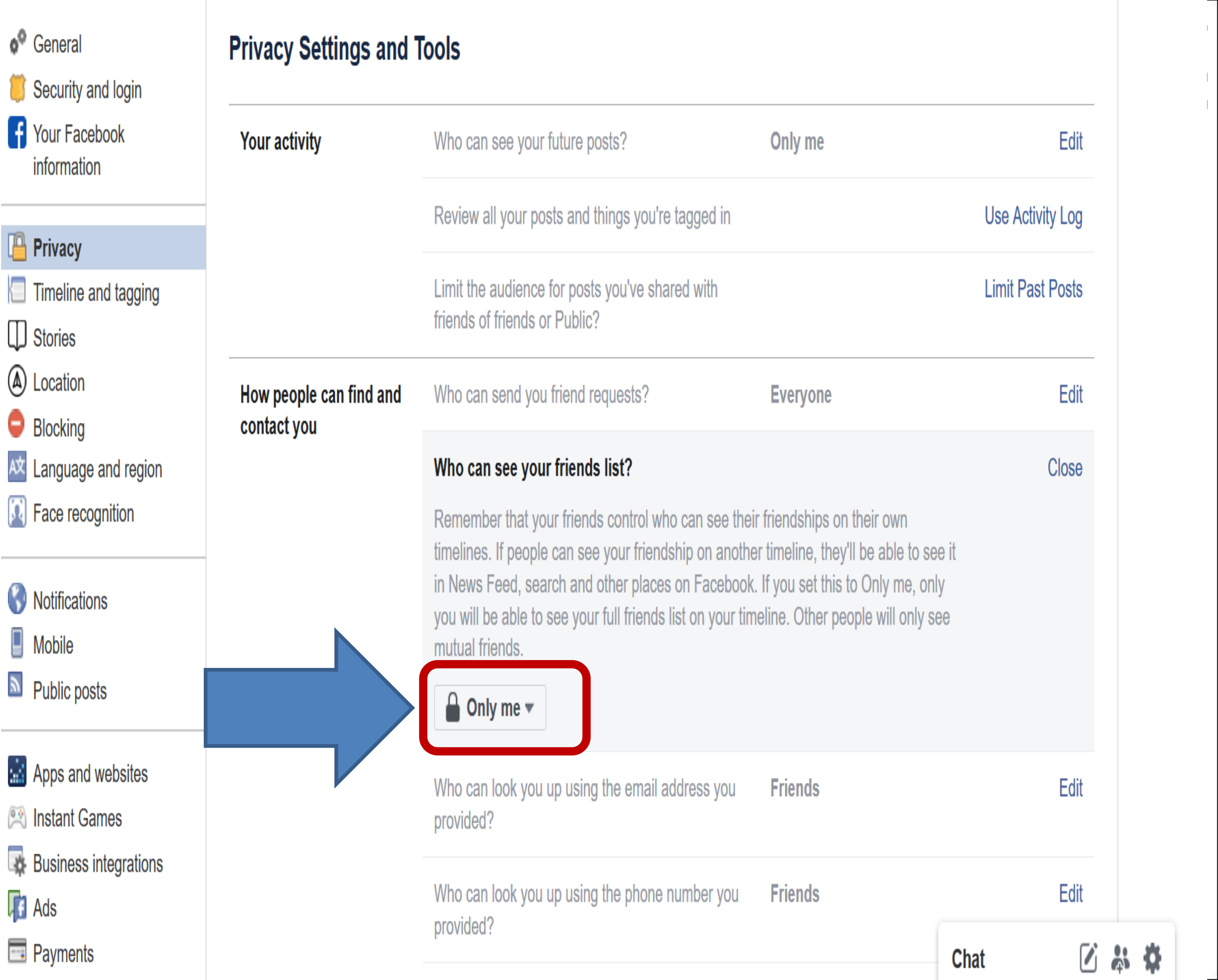
- Once the scammers have created a fake profile, they can send friend requests to people on the targeted person’s friends list.

- At least a few of the victim’s friends may accept this second friend request because they mistakenly believe that the victim has accidentally unfriended them.

HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

- **Hide Your Friends List**

To hide your friends list, open your profile and click on the "Friends" tab. Then, click the pencil icon on the right side and click "Edit Privacy"



Privacy Settings and Tools

Your activity

Who can see your future posts? — Only me — Edit

Review all your posts and things you're tagged in — Use Activity Log

Limit the audience for posts you've shared with friends of friends or Public? — Limit Past Posts

How people can find and contact you

Who can send you friend requests? — Everyone — Edit

Who can see your friends list? — Close

Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.

Only me ▾

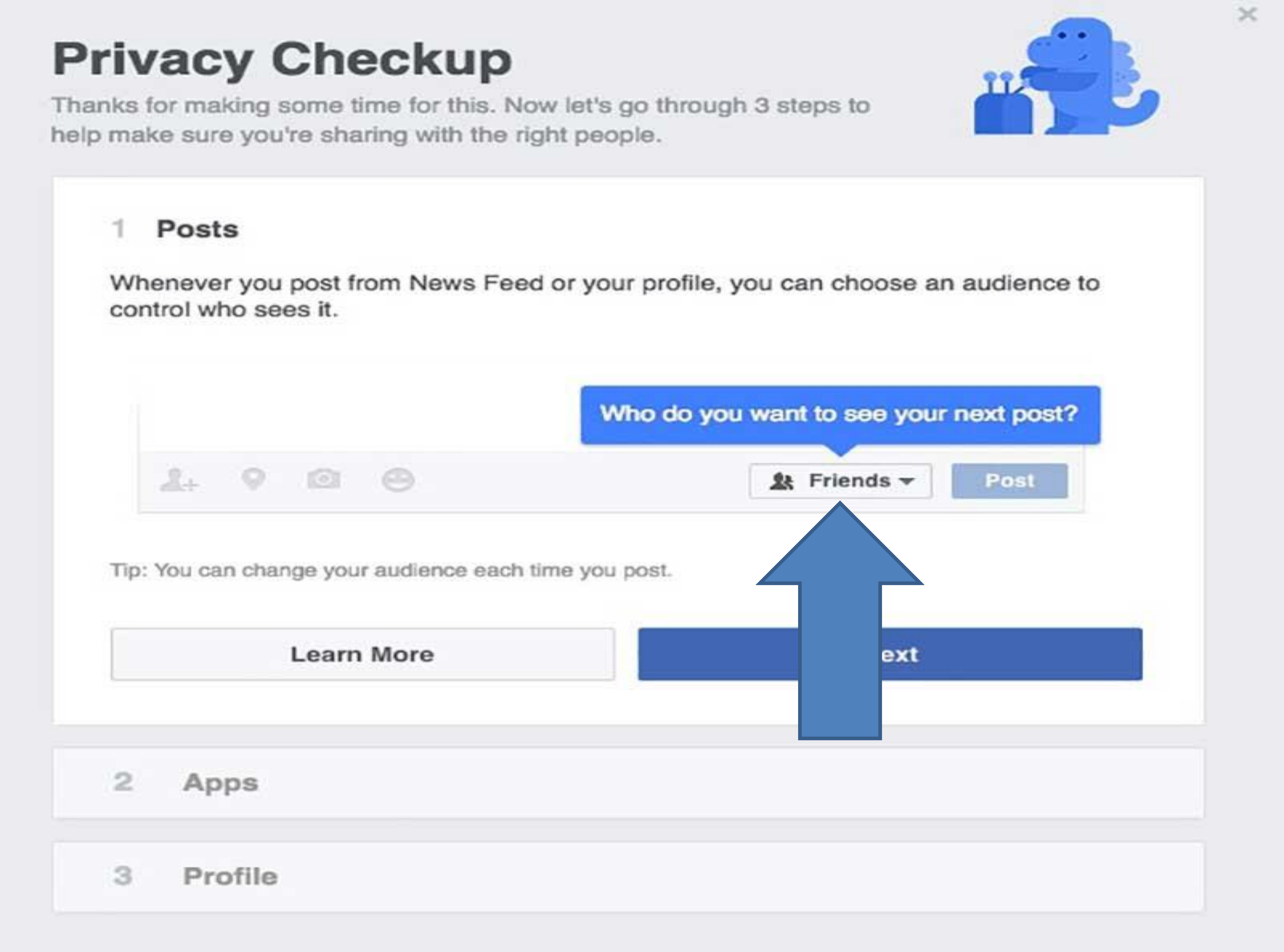
Who can look you up using the email address you provided? — Friends — Edit

Who can look you up using the phone number you provided? — Friends — Edit

HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

- **Run A “Privacy Checkup”**

If you click the “Lock” icon at the top right of your Facebook profile, you can perform a quick privacy checkup related to your posts, apps, and profile. Wherever possible, ensure that they are all set to “Friends” or “Only Me” rather than “Public”



Privacy Checkup

Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.

1 **Posts**

Whenever you post from News Feed or your profile, you can choose an audience to control who sees it.

Who do you want to see your next post?

Tip: You can change your audience each time you post.

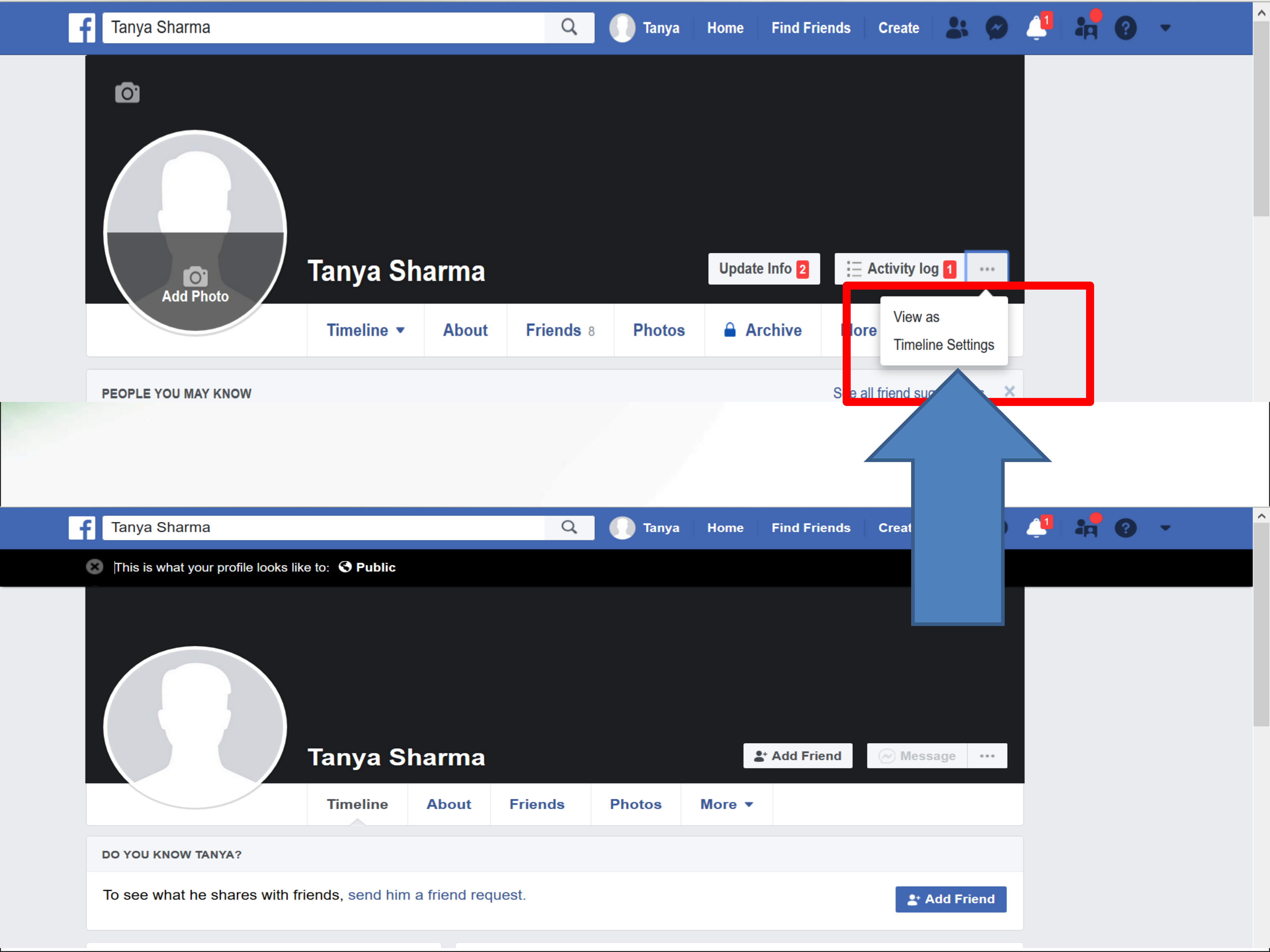
2 Apps

3 Profile

HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

- **View your profile as “Public”**

At this point, it’s probably a good idea to see what your Facebook actually looks like to somebody who is NOT your friend. To do this, click the “Lock” icon again then click “Who can see my stuff”. Now, click the “View As” link under “What do other people see on my timeline?”



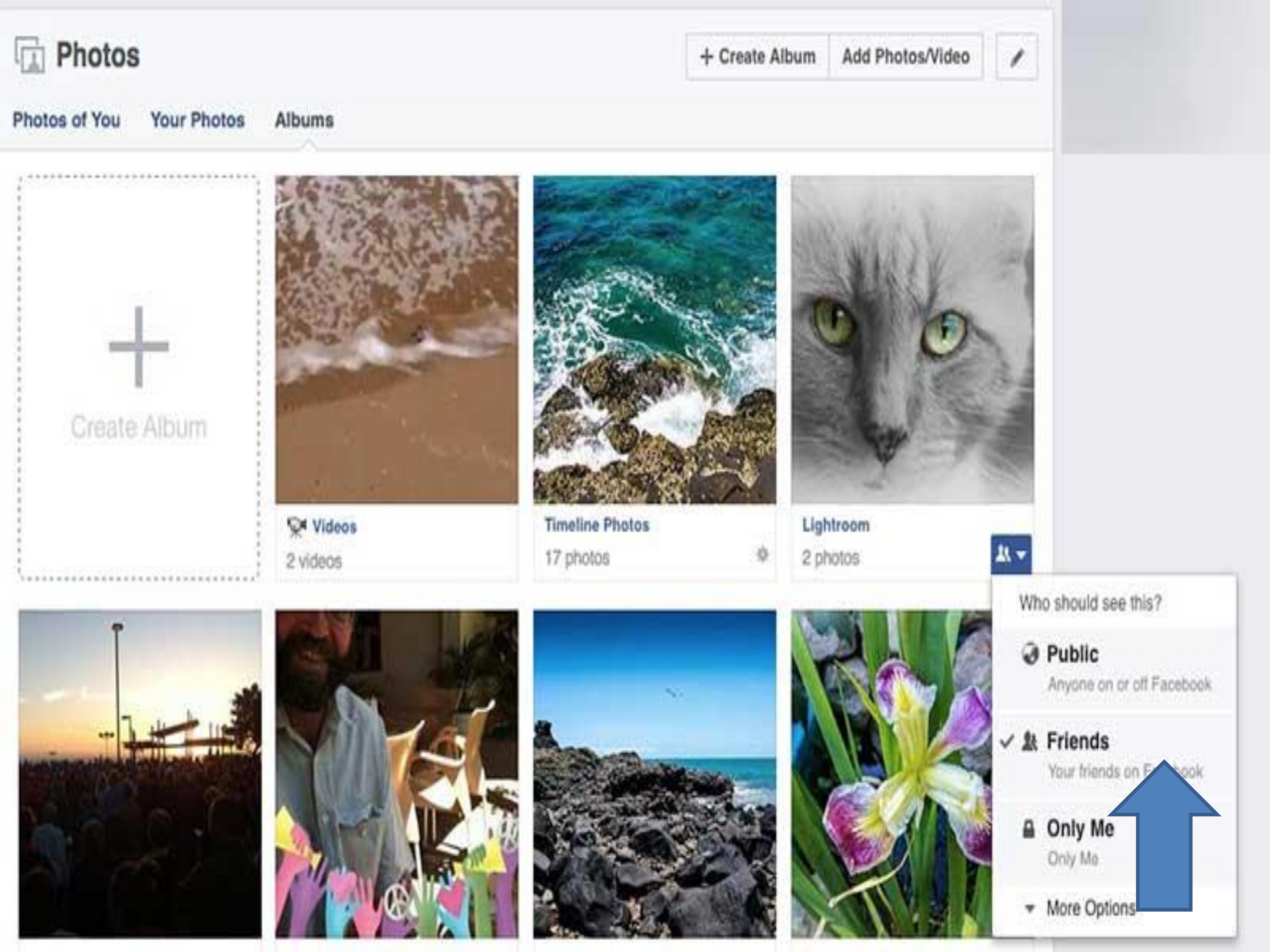
This is what your profile looks like to: Public

To see what he shares with friends, send him a friend request.

HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

- **Check Who Can See Your Photos**

Click the “Photos” tab and open “Albums”. Some types of album will have an audience selector that allows you to set all of the images in the album to “Friends” or “Only Me” in one click.



Photos

+ Create Album | Add Photos/Video

Photos of You | Your Photos | Albums

Create Album

Videos
2 videos

Timeline Photos
17 photos

Lightroom
2 photos

Who should see this?

Public
Anyone on or off Facebook

✓ Friends
Your friends on Facebook

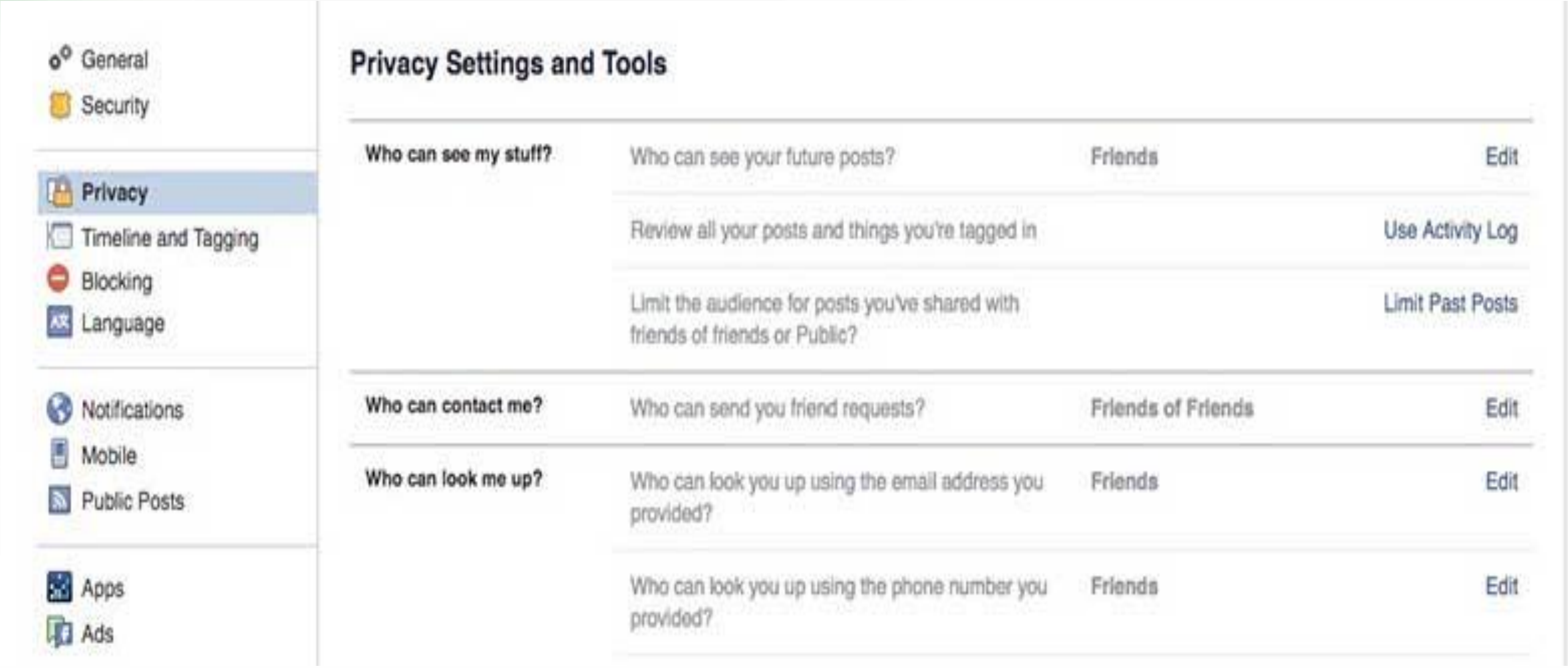
Only Me
Only Me

▾ More Options

HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

- **Dig into Your Privacy Settings**

You can also check and change privacy related settings via the “Privacy Settings and Tools” section.



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of Friends	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit

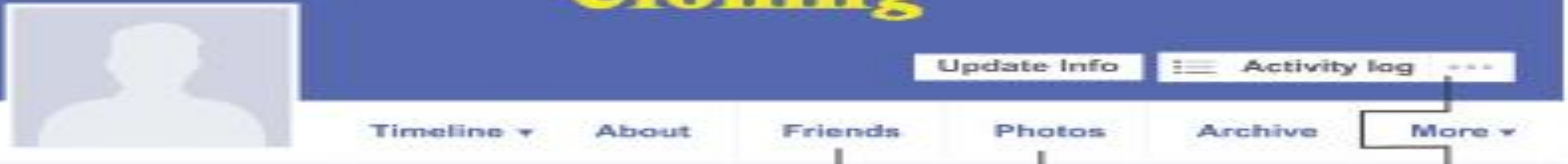
HOW TO PROTECT YOUR ACCOUNT FROM FACEBOOK CLONING

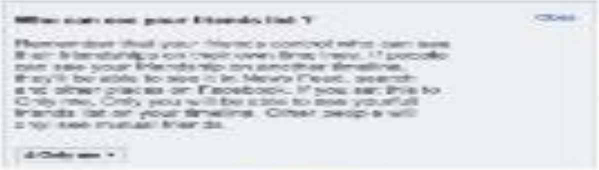
- Be wary of any friend requests from people that you are already friends with.
- If you receive one, check your own friends list to see if you are still friends with the person. If so, the friend request is likely to be from a cloned account.
- Alert your friend to the scam as soon as possible so that he or she can take steps to deal with the issue.

Information Security Education & Awareness
www.isea.gov.in

For more details visit
www.InfoSecawareness.in

How to protect your facebook account from Cloning





Who can see your friends list ?

Close

Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, Only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.

Only me

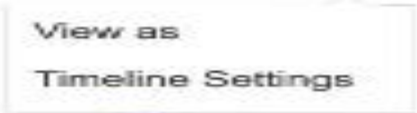
1

Hide your friends list from the public

(Settings ⟶ Privacy)

2

Limit the photos you post online

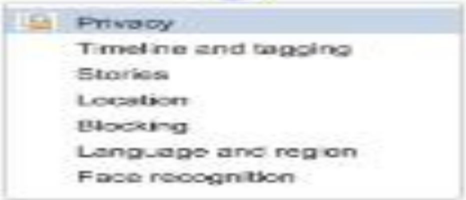


3

Check how your profile looks to the public

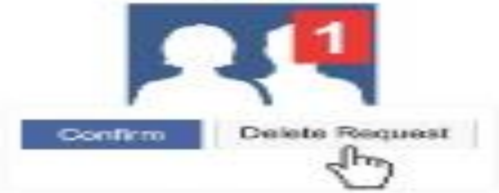
(Activy log ⟶ View as)

4



Utilize the privacy settings in the best way

5



Ignore / delete friends request from strangers

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

cert-in
http://cert-in.org.in
www.cyberswachhtakendra.gov.in

Cyber Safe Girl

END NOW

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी डैक
CDAC

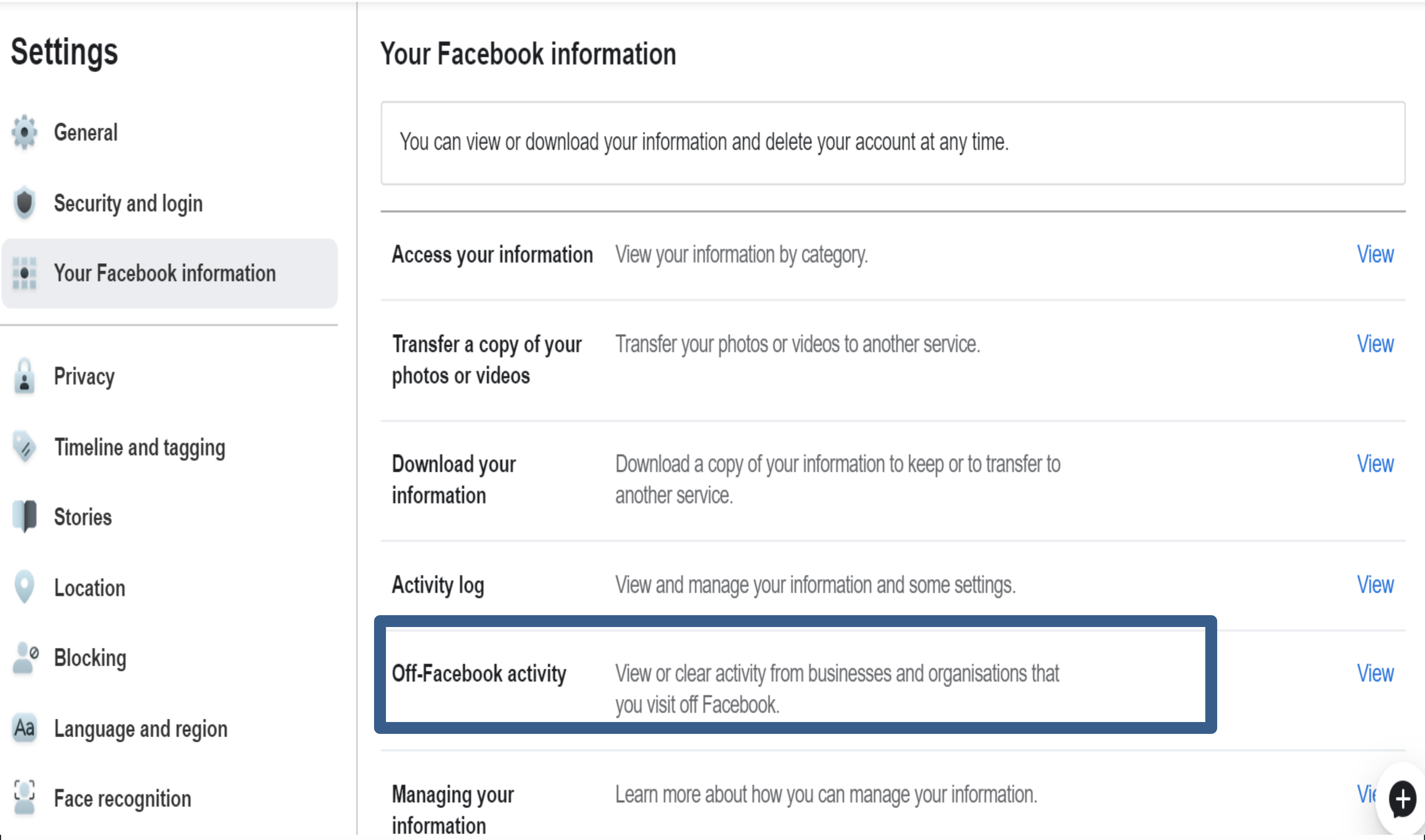
FACEBOOK OFF ACTIVITY

Facebook says turning off the ‘Off-Facebook activity’ result in the user no longer seeing personalized advertisements based on their daily online activity.

How to turn off ‘Off-Facebook’ activity sharing?

To check which apps and websites have been sharing your data with Facebook, head over to **Facebook Settings > Your Facebook Information > Off-Facebook Activity.**

CLICK ON OFF-FACEBOOK ACTIVITY



Settings

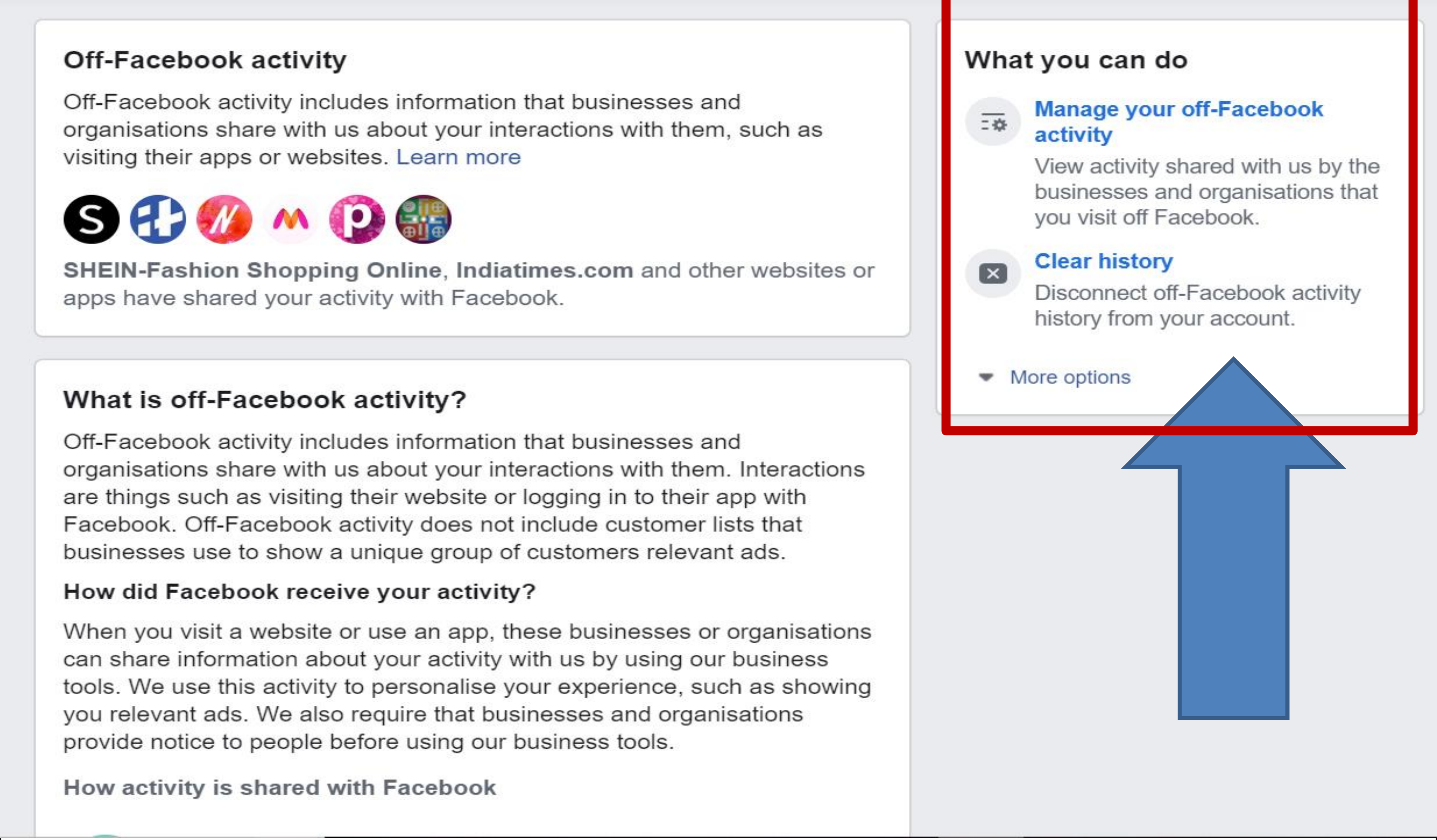
- General
- Security and login
- Your Facebook information
- Privacy
- Timeline and tagging
- Stories
- Location
- Blocking
- Language and region
- Face recognition

Your Facebook information

You can view or download your information and delete your account at any time.

Access your information	View your information by category.	View
Transfer a copy of your photos or videos	Transfer your photos or videos to another service.	View
Download your information	Download a copy of your information to keep or to transfer to another service.	View
Activity log	View and manage your information and some settings.	View
Off-Facebook activity	View or clear activity from businesses and organisations that you visit off Facebook.	View
Managing your information	Learn more about how you can manage your information.	Vi

YOU CAN MANAGE YOUR FACEBOOK ACTIVITY FROM HERE



Off-Facebook activity

Off-Facebook activity includes information that businesses and organisations share with us about your interactions with them, such as visiting their apps or websites. Learn more

SHEIN-Fashion Shopping Online, **Indiatimes.com** and other websites or apps have shared your activity with Facebook.

What is off-Facebook activity?

Off-Facebook activity includes information that businesses and organisations share with us about your interactions with them. Interactions are things such as visiting their website or logging in to their app with Facebook. Off-Facebook activity does not include customer lists that businesses use to show a unique group of customers relevant ads.

How did Facebook receive your activity?

When you visit a website or use an app, these businesses or organisations can share information about your activity with us by using our business tools. We use this activity to personalise your experience, such as showing you relevant ads. We also require that businesses and organisations provide notice to people before using our business tools.

How activity is shared with Facebook

What you can do

Manage your off-Facebook activity

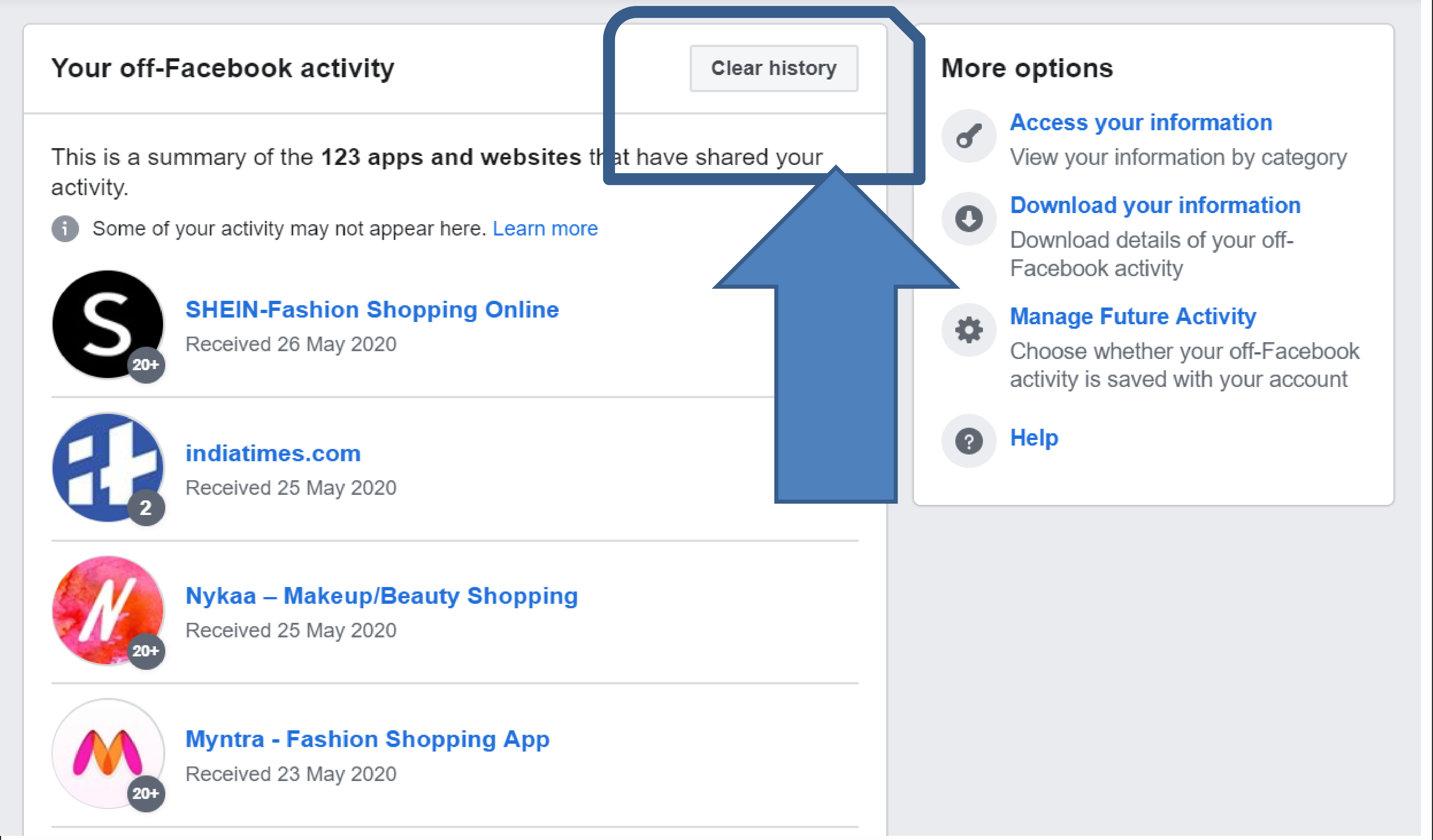
View activity shared with us by the businesses and organisations that you visit off Facebook.

Clear history

Disconnect off-Facebook activity history from your account.

▾ More options

TO TURN OFF-FACEBOOK ACTIVITY CLICK ON CLEAR HISTORY



Your off-Facebook activity

Clear history

This is a summary of the **123 apps and websites** that have shared your activity.

Some of your activity may not appear here. Learn more

SHEIN-Fashion Shopping Online
Received 26 May 2020

indiatimes.com
Received 25 May 2020

Nykaa – Makeup/Beauty Shopping
Received 25 May 2020

Myntra - Fashion Shopping App
Received 23 May 2020

More options

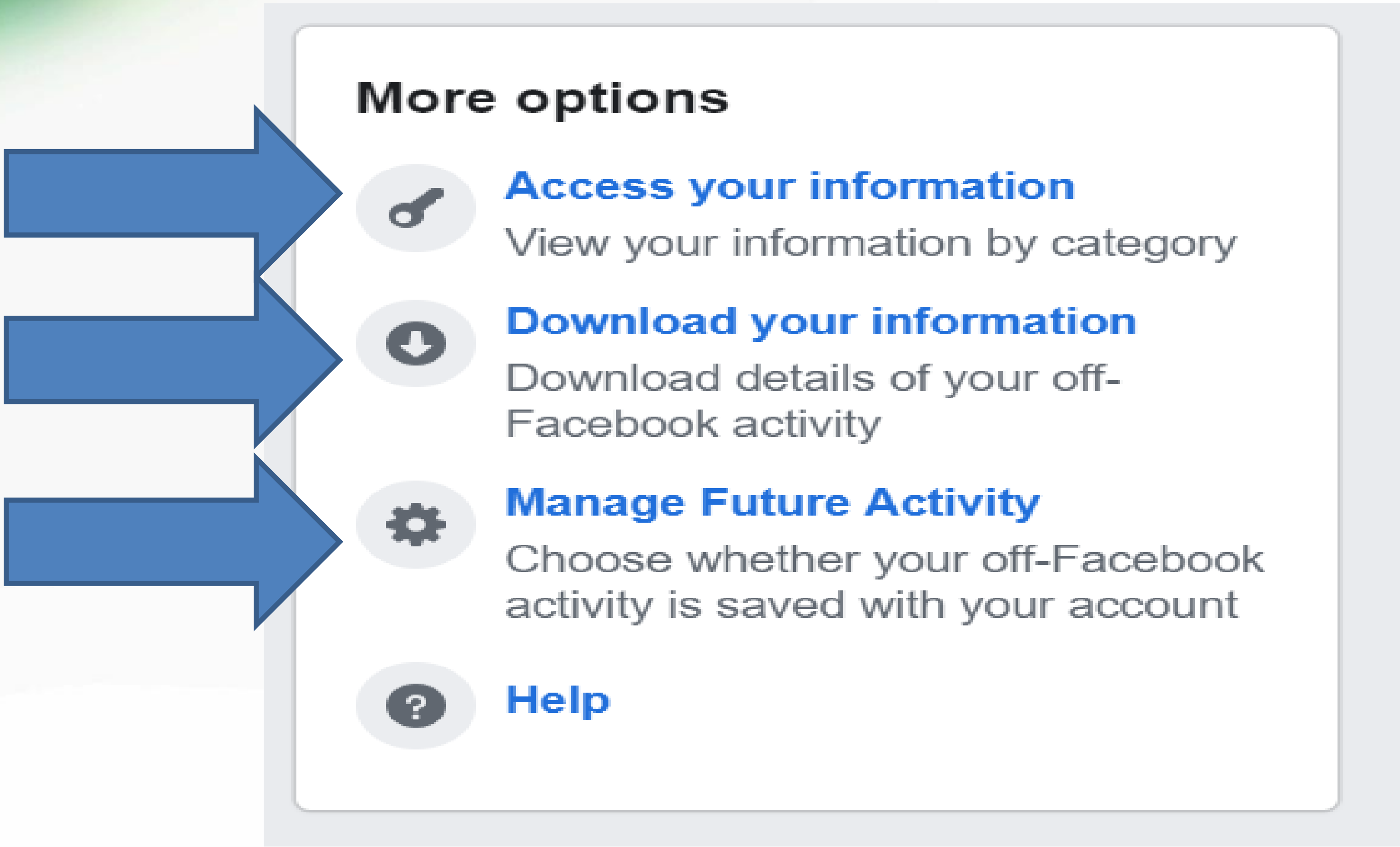
Access your information
View your information by category

Download your information
Download details of your off-Facebook activity

Manage Future Activity
Choose whether your off-Facebook activity is saved with your account

Help

CLICK ON THESE OPTIONS TO CHECK ALL THE INFORMATION WHICH YOU HAVE SHARED ON FACEBOOK TILL NOW. YOU CAN DOWNLOAD THE INFORMATION AS WELL



More options

Access your information
View your information by category

Download your information
Download details of your off-Facebook activity

Manage Future Activity
Choose whether your off-Facebook activity is saved with your account

Help

police personnel accused in the case.

InfoSec NEWS ALERTS

Prevent your Facebook Account from being Hacked

Turn on Login Alerts 1

When you turn on login alerts, you will be notified any time someone logs in to your account from a new computer or phone.

Enable Login Approvals 2

When you turn on login approvals, you'll be asked to enter a login approval code each time you access your Facebook account from a new phone or computer.

Add OpenPGP public key 3

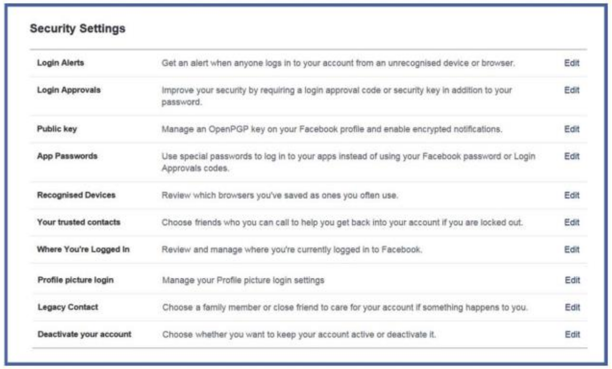
PGP stands for Pretty Good Privacy and is used to encrypt email communications and receive encrypted notification emails. It requires two keys -- one public, the other private -- to protect email. The sender needs to know the recipient's public key to encrypt the message, and then the recipient uses his or her private key to decrypt it

Enable app passwords 4

Go to App Passwords and have the tool generate unique passwords for your apps instead of using your Facebook password.

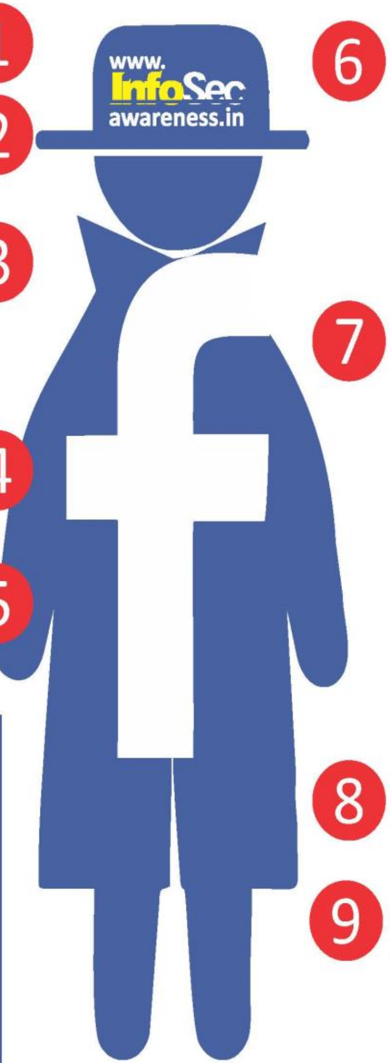
Create your trusted contact list 5

Trusted contacts are friends you can contact if you ever need help getting into your Facebook account



Security Settings

Login Alerts	Get an alert when anyone logs in to your account from an unrecognised device or browser.	Edit
Login Approvals	Improve your security by requiring a login approval code or security key in addition to your password.	Edit
Public key	Manage an OpenPGP key on your Facebook profile and enable encrypted notifications.	Edit
App Passwords	Use special passwords to log in to your apps instead of using your Facebook password or Login Approvals codes.	Edit
Recognised Devices	Review which browsers you've saved as ones you often use.	Edit
Your trusted contacts	Choose friends who you can call to help you get back into your account if you are locked out.	Edit
Where You're Logged In	Review and manage where you're currently logged in to Facebook.	Edit
Profile picture login	Manage your Profile picture login settings	Edit
Legacy Contact	Choose a family member or close friend to care for your account if something happens to you.	Edit
Deactivate your account	Choose whether you want to keep your account active or deactivate it.	Edit

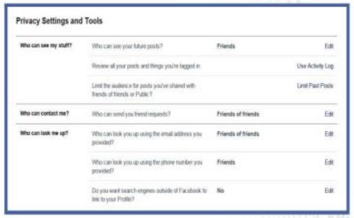


6 Limit the privacy of data you post

Take advantage of the privacy settings available in your account.

- Who can see my stuff?
- Who can contact me?
- Who can look me up?

Click edit button on the toip right corner and set your privacy

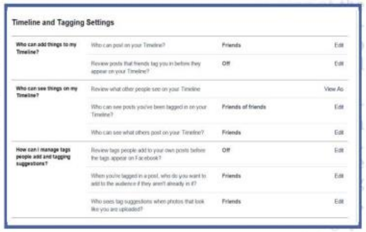


Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of friends	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends of friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit

7 Control the posts to be tagged in your timeline

You get to decide whether friends are allowed to post things on your Timeline or not and also decide whether you want to review posts that friends tag you in before they appear on your Timeline.



Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Friends	Edit
	Review posts that friends tag you in before they appear on your Timeline?	Off	Edit
Who can see things on my Timeline?	Review what other people see on your Timeline		View As
	Who can see posts you've been tagged in on your Timeline?	Friends of friends	Edit
	Who can see what others post on your Timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	Off	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	Friends	Edit

- Who can add things to my Timeline?
- Who can see things on my Timeline?
- How can I manage tags people add and tagging suggestions?

8 Manage Blocking

You can manage the pages, profiles etc., from viewing your profile through this setting.

9 Change your password regularly

Don't use same passwords for all your accounts. The harder you passwords the safer you are

HR man alleges FB account hacked

TIMES NEWS NETWORK

Gurgaon: An HR executive working for a private firm has filed a complaint against an unknown person who allegedly hacked her Facebook account and tried to extract her personal details like address and phone number from her friends.

Acting on her complaint, an FIR was filed at Sector 17/18 police station under sections 66C (punishment for identity theft) and 66D (punishment for cheating by personation by using computer resource) of the Information Technology Act.

Inspector Ram Kumar, SHO, Sector 17/18 police station, said the hacker interacted with her friends using her Facebook profile trying to extract a few details of the complainant from them. The complaint, which was filed in January, was sent to the cyber cell for verification.

"We have tracked down the accused's location with the IP address and will arrest him soon," said Kumar.

In a similar case, a woman from Nepal has accused one of her former neighbours, who is also from Nepal, of creating a fake Facebook account and uploading her pictures on it. The woman has also alleged that he posted images of her family members on the social media website.

The woman, who is living in Sirhaul in Sector 17, filed a complaint on Wednesday at the Sector 17/18 police station, on the basis of which an FIR was registered under section 354D (stalking), 66C and 66D of the Information Technology Act.

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

For Virus Alerts,Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents
http://cert-in.org.in/

www.
cyberswachhtakendra.
gov.in

For any queries on Cyber Security
Call us on Toll Free No.
1800 425 6235
between 10.00 AM to 6.00 PM or
give a missed call we will call back in 24hrs

सी डैक
CDAC

PREVENTION TIPS

Never Open E-Mail attachments With the file extensions Such as VBS,SHS,PIF etc

Never open Web-links in your e-mail. Always type links in Web browser

Always use e-mail transaction through secured mail sites

Never download anything from e-mail when the sender is unknown or the attachment has a doubtful name

New viruses creep upon a daily basis. It is important that we do back up our valuable data files regularly

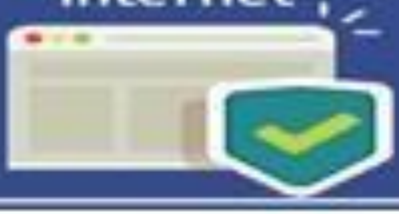
Check for spelling mistakes.
Fake job offer mails generally have spelling mistakes and grammatical errors

Never trust the icons in the e-mail attachment. The virus file may be shown as PDF file.

Never send your photograph through e-mail to unknown persons.

Don't respond to spam mails without verification of the e-mail origin

Always use secured web browsers which enables safe browsing over internet



Turn off all JavaScript or Active X support in your web browser before you visit unknown websites

Keep your OS and Browser software up to date with the latest versions and security patches.

Optimize your browser's settings to protect your device from malicious attacks

Block Pop-ups and scripts

Make sure the URL of the websites has "https://" or a padlock icon

Clear your browsing activity on regular basis to avoid threat to confidential information

THANK YOU!

STAY SAFE STAY SECURE

Dr. Neha Bajpai

nehakapoor@cdac.in

धन्यवाद आभार આભાર ਧਨਵਾਦ ধন্যবাদ நன்றி നന്ദി [illegible]