OSINT How-Tos

OPSEC

Basic Operational Security (OPSEC)

- Why OPSEC?
  - Avoid the investigation being discovered
  - Avoid providing your personal information to social media platforms or
  - Shield your activities from being linked to you personally by search engines,
  - Maintain your security and privacy

  - Depends upon threat profile to you, the analyst, and to the integrity of the investigation, depending upon the project

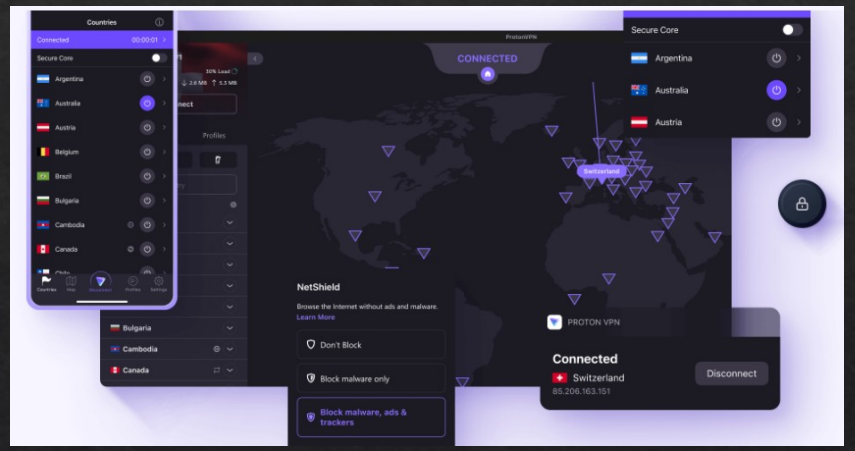
Using VPNs

Gives online privacy and anonymity by creating a private network from a public internet connection.

Use:

- When you need to change your “geographical” IP location
- When you need to be certain of a secure and encrypted connection
- When using Tor

We use ProtonVPN – may be issues w/the VM, but it works.



Research Accounts, aka “Sock Puppet”

- Used to access social media services to collect information and perform research
  - Accounts often needed to get deeper info
  - Anonymity
    - Do not use your personal social media accounts
    - Targets can determine if (and sometimes who) is investigating them
- Note: the object isn't to "hide" from platforms, but Subjects
  - It's ok to use Gmail
  - Remember: appear boring

Research Accounts, aka “Sock Puppet”

- Persona - Fake Name Generator
- Password Manager - Bitwarden

For deeper personas, a burner phone will be necessary.

- Burner Phone
- SIM Card
- Non-work non-home WIFI (coffee shop, library)
- Email Account
- Setup 2FA
- Switch contact info to Google Voice or MySudo VoIP

Alternative Email Providers

Do not use your regular work or personal email to sign up for accounts

- Use a service common in the jurisdiction you're going to be researching in.
- **It should look real and blend in.**

  - Gmail
  - Mail.com
  - Outlook.com
  - Aol.com
  - Hotmail.com

Accessing Pages

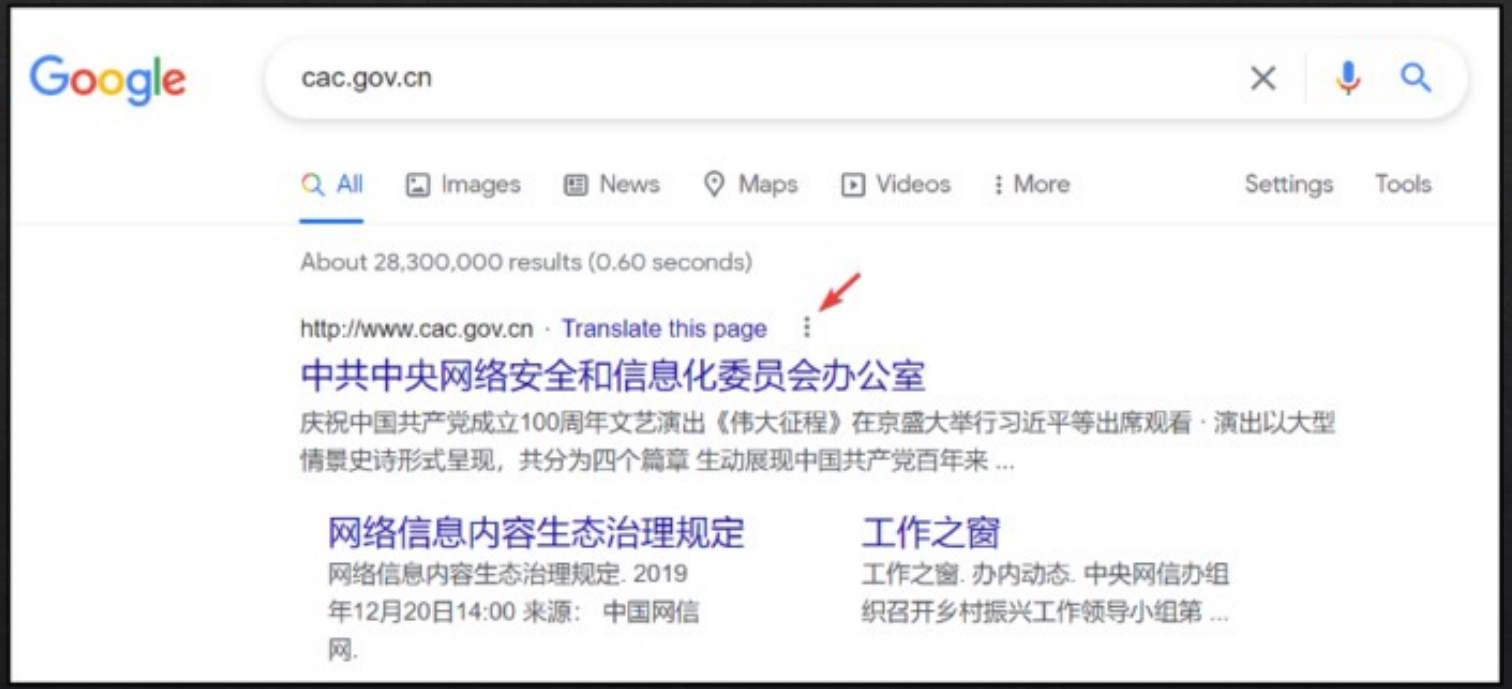
- Accessing pages
  - Cached or archived pages are previous versions of a page
  - Safer than accessing a page directly
    - May also contain missing or deleted info

- Method 1:
  - https://www.cachedpages.com

Cached Pages - Get the cached page of any URL

Accessing a Cached Page

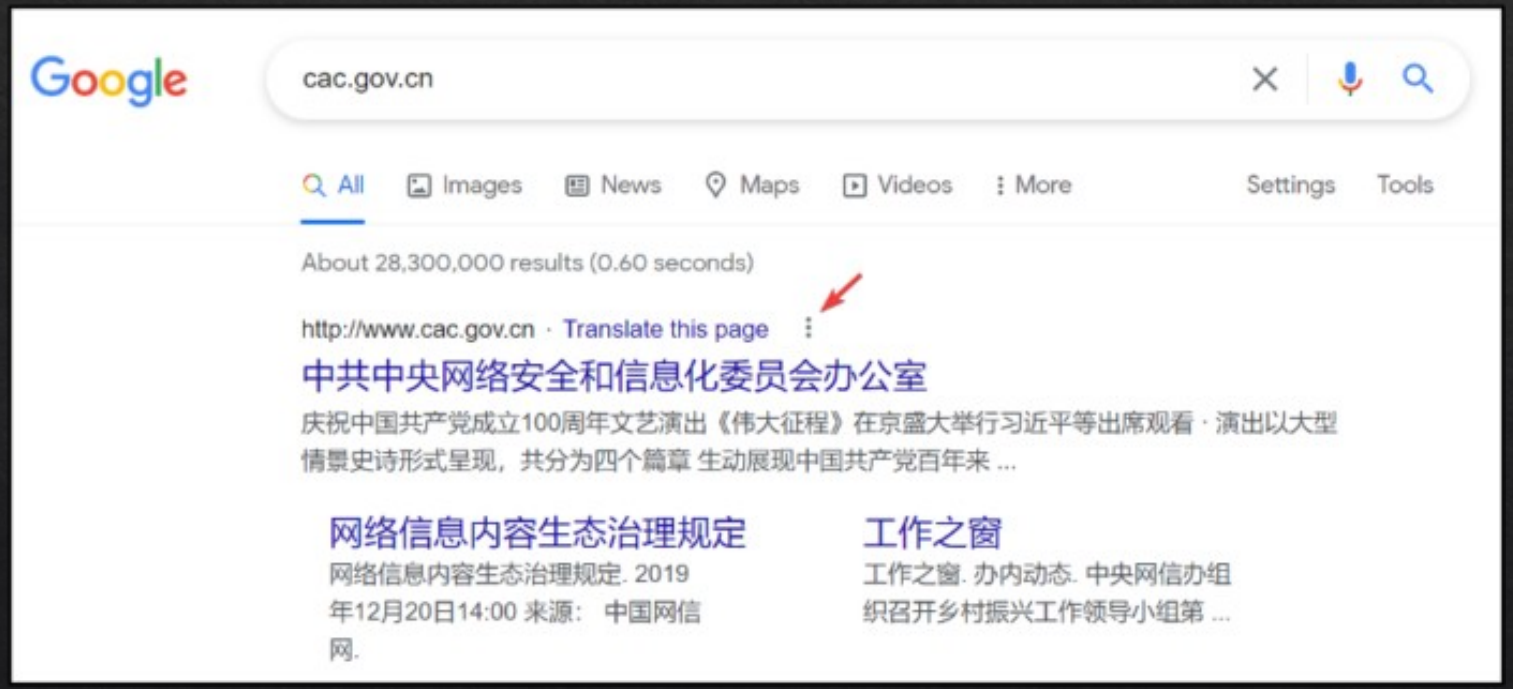
Method 2: “cache:[URL]” directly into search bar
Method 3: Click on 3 vertical dots nfiletype to Google search result



The bottom-right corner of the ensuing pop-up will include a button that says “Cached.”

Click on it to access the cached page.

Accessing a Cached Page



- Scan all files with a virus scanner and check for malware.
  - Keep definitions up to date

Use Cached Pages to look at files before downloading, like .xls, .doc, .pdf, or .xlsx.

Google's cache will transform it into a web page:

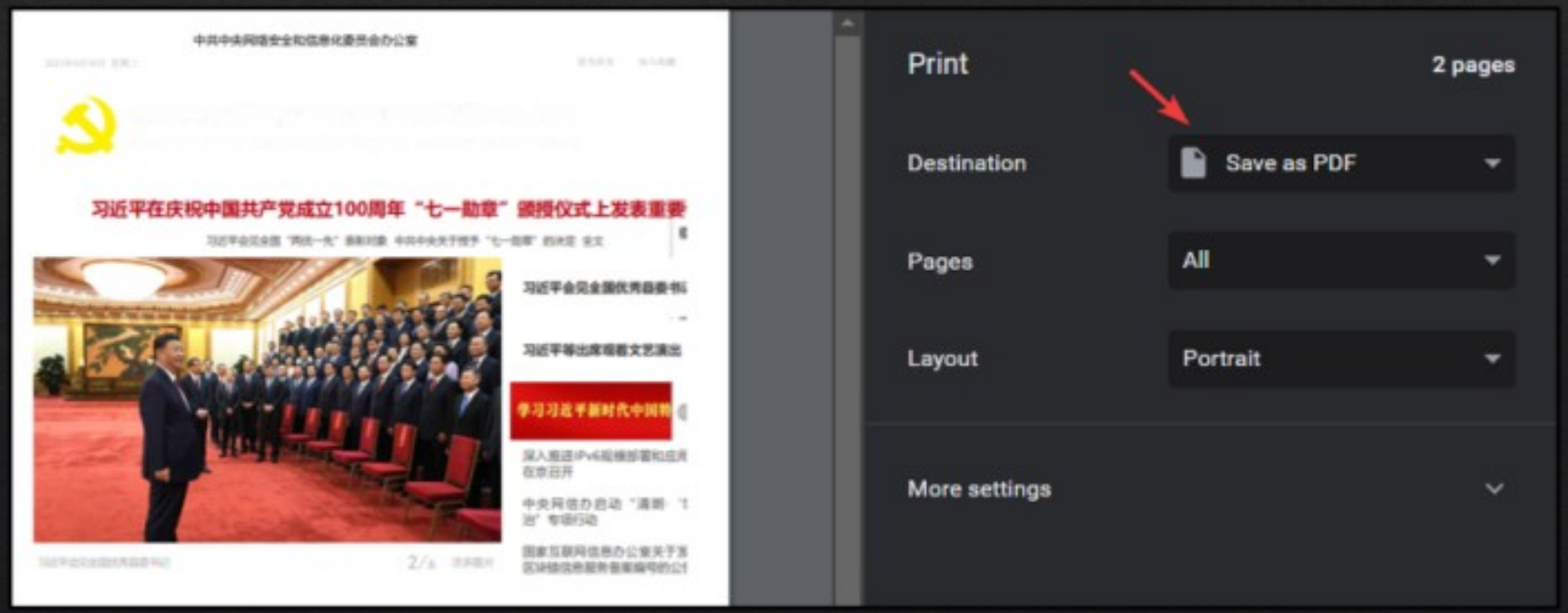
Note: Site owners can still track who's viewing their cached pages.

Accessing tfiletype-only versions of pages helps.

It also makes pages load faster.

Archive Services:

- Check if a page has been saved already:
  - The Internet Archive (Wayback Machine) or Archive Today
  - Can also request that they save the page
  - Drawback: most archive services "ping" the target website with your IP – alerts the site that they're under investigation.
- Workaround? Yes: "Print to .pdf"



Light Side of OPSEC Failure:

- https://twitter.com/RALee85/status/1610018005462749190?cxt=HHwWjMC4mZC299csAAAA

Research Categories

OSINT Research Categories

- Why do Clients care about these areas?
  - They highlight the kinds of risk that a Subject could bring to the Client, or (if the Client is also the Subject) that the Subject could experience
    - Reputation, Legal, Financial, Social, potential for blackmail, physical risk, contfiletype (supply chain, theft, IP, etc.)
- Misinformation could damage a VIP's reputation, their ability to conduct business, or the value of the organization they represent.
- If left unchecked, misinformation could represent a serious danger to your principal.
- Imagine false reports suggesting your company has planned a hostile takeover of a rival firm. Such rumors could incite anger, putting executives at higher risk of an attack.
- Keeping tabs on rumors or false reports allows corporate security teams to respond quickly.

What Can These Areas Tell Us About the Subject?

- Each interest area is queued to a particular kind of risk

- Non-exhaustive list of potential exposure types:

  - Media Searches - reputation, background information
  - Litigation - criminal or civil legal involvement
  - Regulatory Checks - legal
  - Sanctions & PEP - legal
  - Leaked Docs - reputation, criminal, or civil legal
  - Political Donations - conflict of interest
  - Directorship/Shareholdings - conflict of interest
  - UBO - legal, criminal, conflict of interest
  - Source of Wealth - legal, criminal, conflict of interest

- Analysis enables the Client to determine how they would like to proceed with the Subject given the findings

OSINT Fail

Doxxed CEO wrongly identified as 'sovereign' woman thanks supporters

MAY 6, 2020

https://www.straitstimes.com/singapore/doxxed-ceo-wrongly-identified-as-sovereign-woman-thanks-supporters

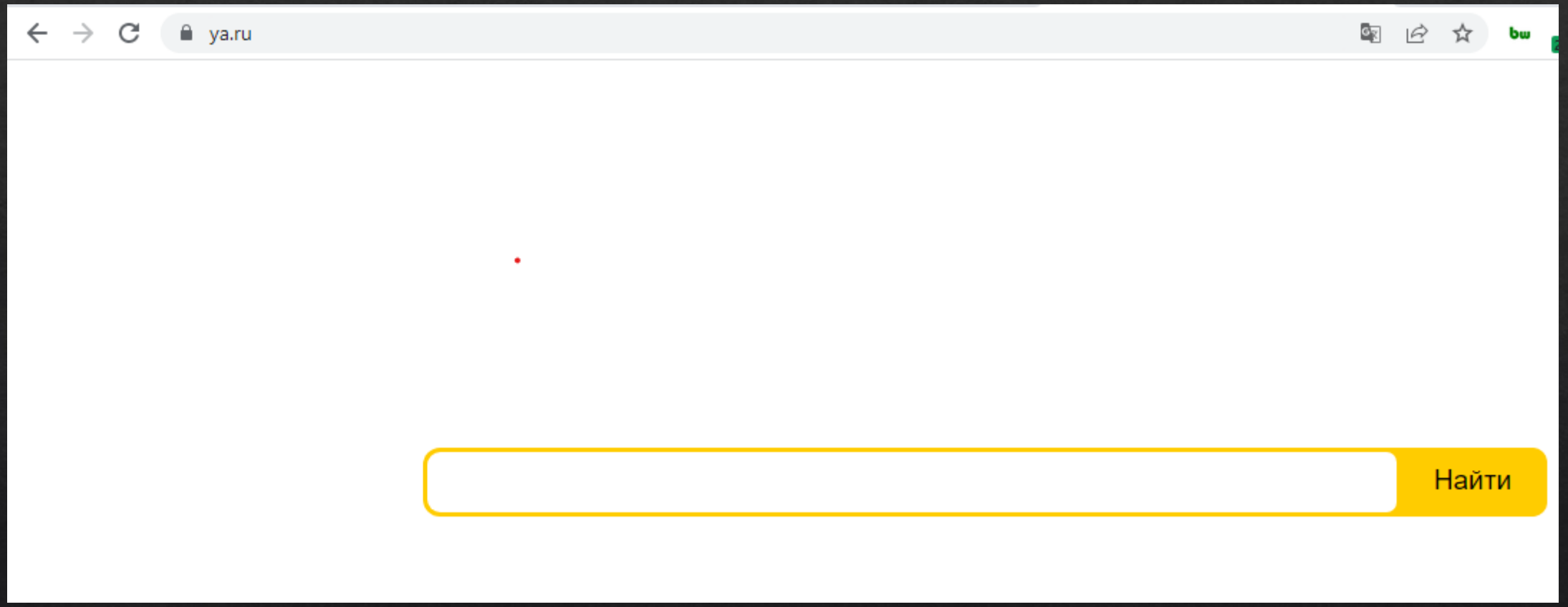
Examples of World-wide search engines

- Google
- Bing
- DuckDuckGo
- Yahoo
- Baidu (China)
- Yandex (Russia)
- YouTube

Baidu

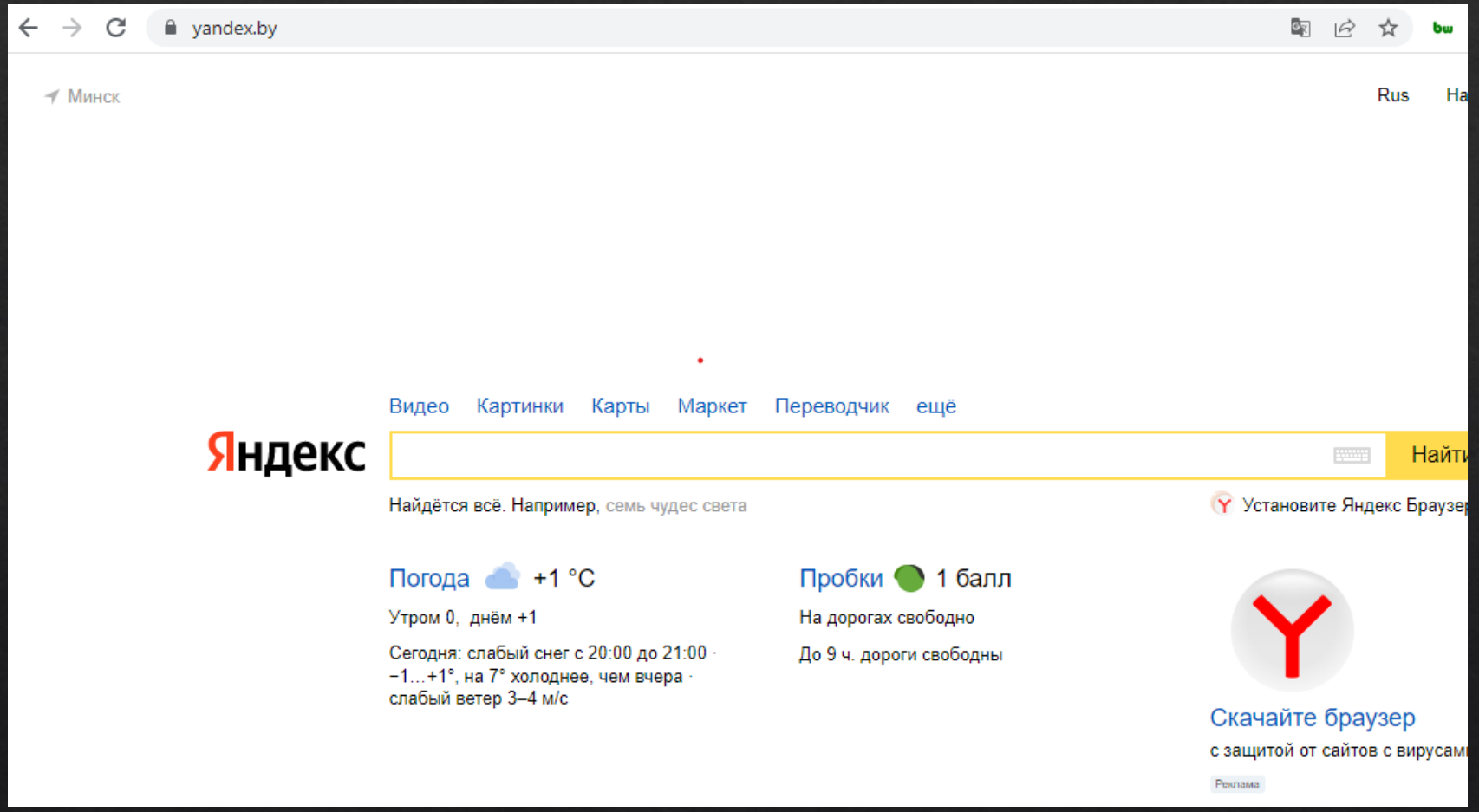

Not secure | baidu.com
新闻 hao123 地图 贴吧 视频 图片 网盘 更多
Bai du 百度
百度一下
百度热搜
换一换
2023，过好每一天
1 韩国对中国游客设限2天后系统崩溃 热
2 感染XBB1.5会大便失禁？专家回应 热
3 XBB的致病力增加了？五问五答
4 发朋友圈致蒙脱石散脱销 当事人... 热
5 韩国发布全球前十最强国家名单！

Yandex – in Russian



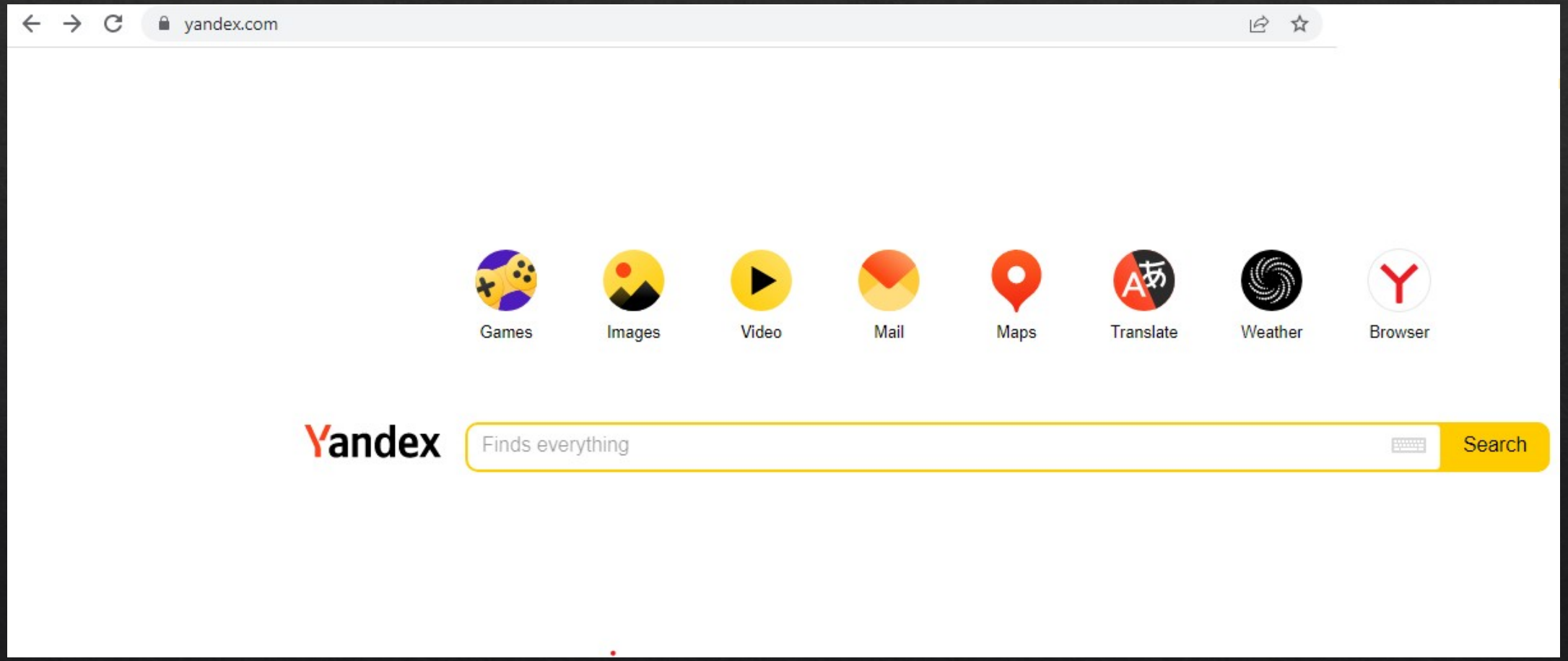
https://ya.ru/

Yandex – in Belorusian



It's good to use a VPN, or to change to the native version of a site.

Yandex – in English

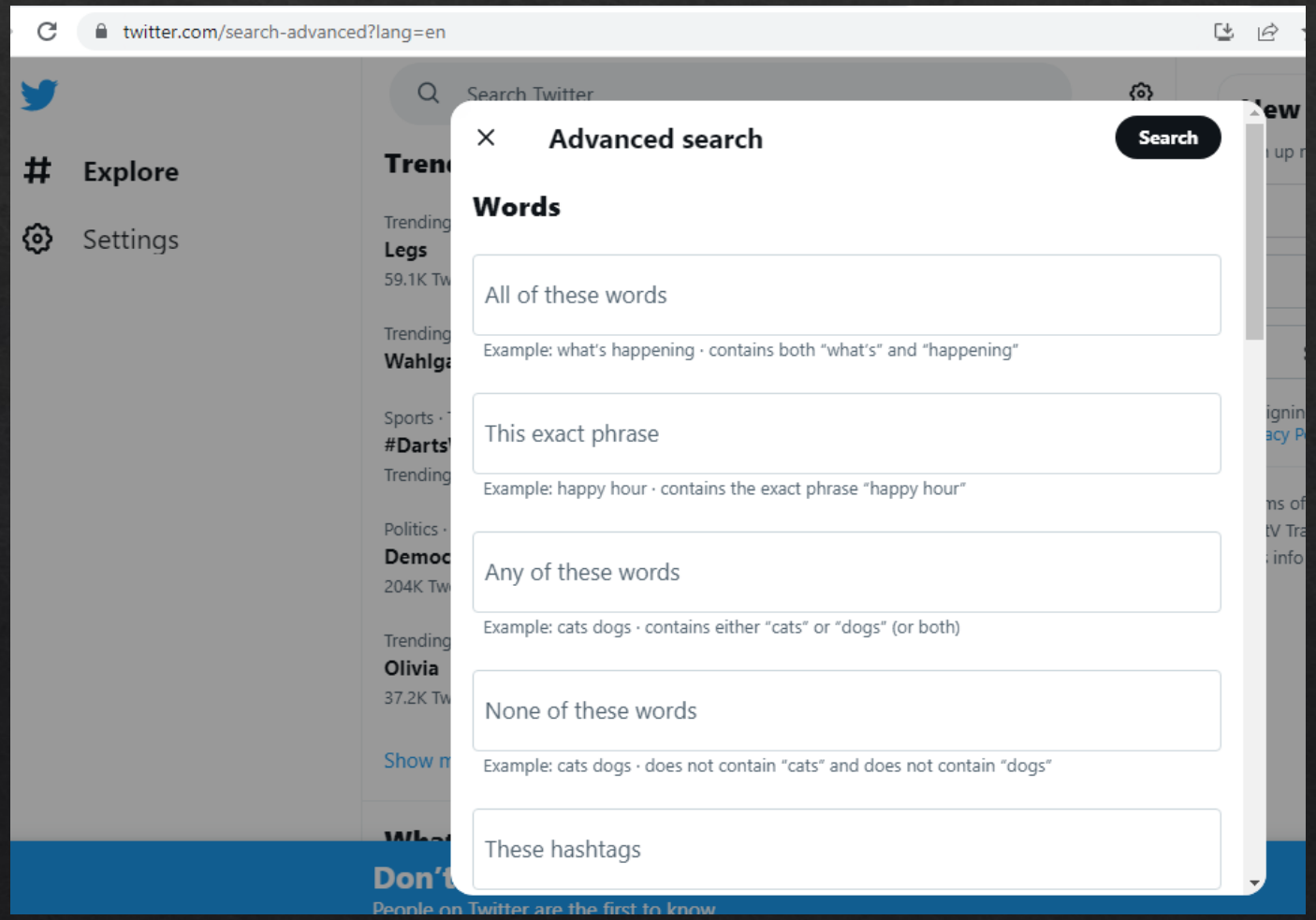


https://yandex.com

Social Media Searches

- Twitter
- Facebook Search
- OK.ru (Russia)
- Vkontakte (Russia)
- Naver (South Korea)
- LinkedIn

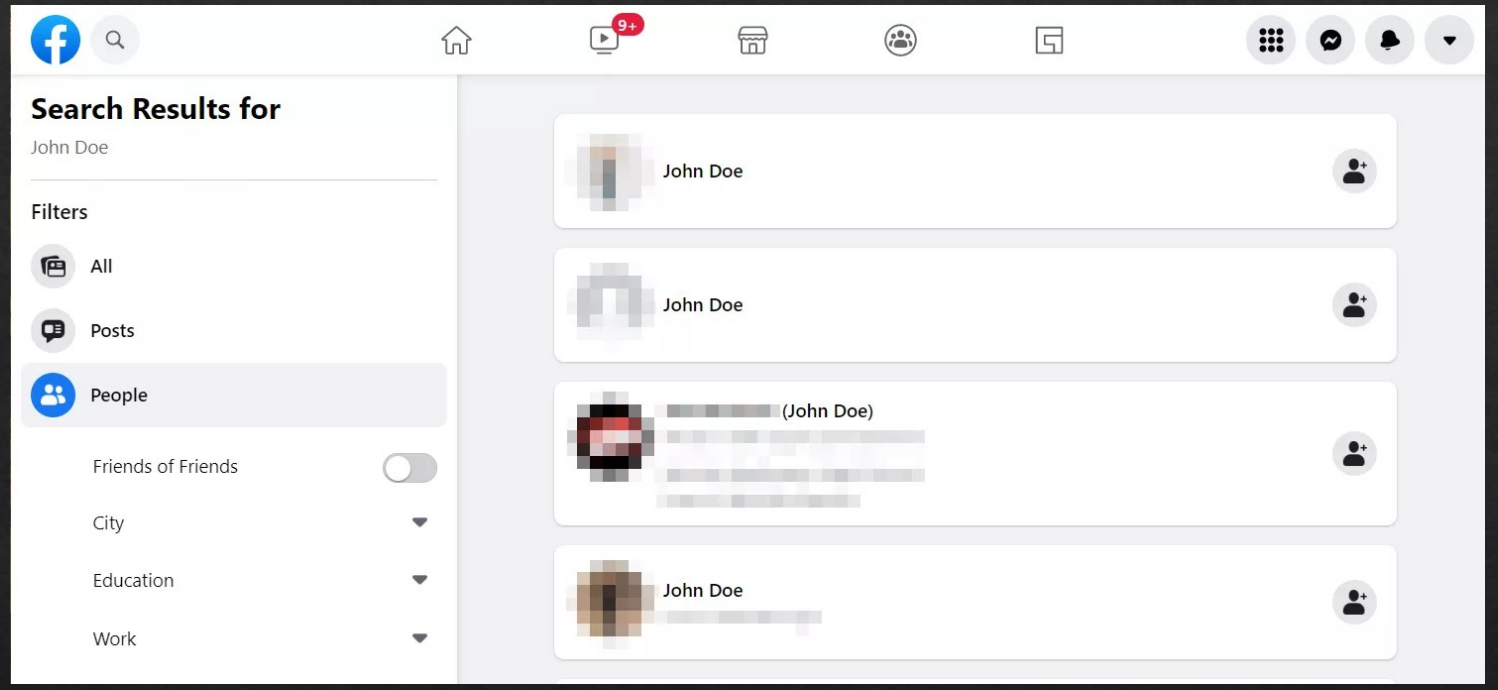
Twitter Advanced Search



- Twitter has an advanced search at
- https://twitter.com/search-advanced?lang=fr
  - Can swap the language!

- Once logged in to Twitter, do use Tweetdeck at
- https://tweetdeck.twitter.com/

Facebook People Search



- Use filters to make searches more relevant
- Select “People” to zero in
- Order of searches can save time:
  - Search for business or city
  - Then choose “People”
- Look at the Subject’s friends to see if the Subject appears in their pages, photos, comments

Special Searches (a Deep Web Selection)

- Internet Archive
- Have I Been Pwned
- Dilisense

External paid resources

- Fast Turnaround Reports (Basem)
- Sayari
- LexisNexis

Questions?