

4-3-2 Safer Browsing

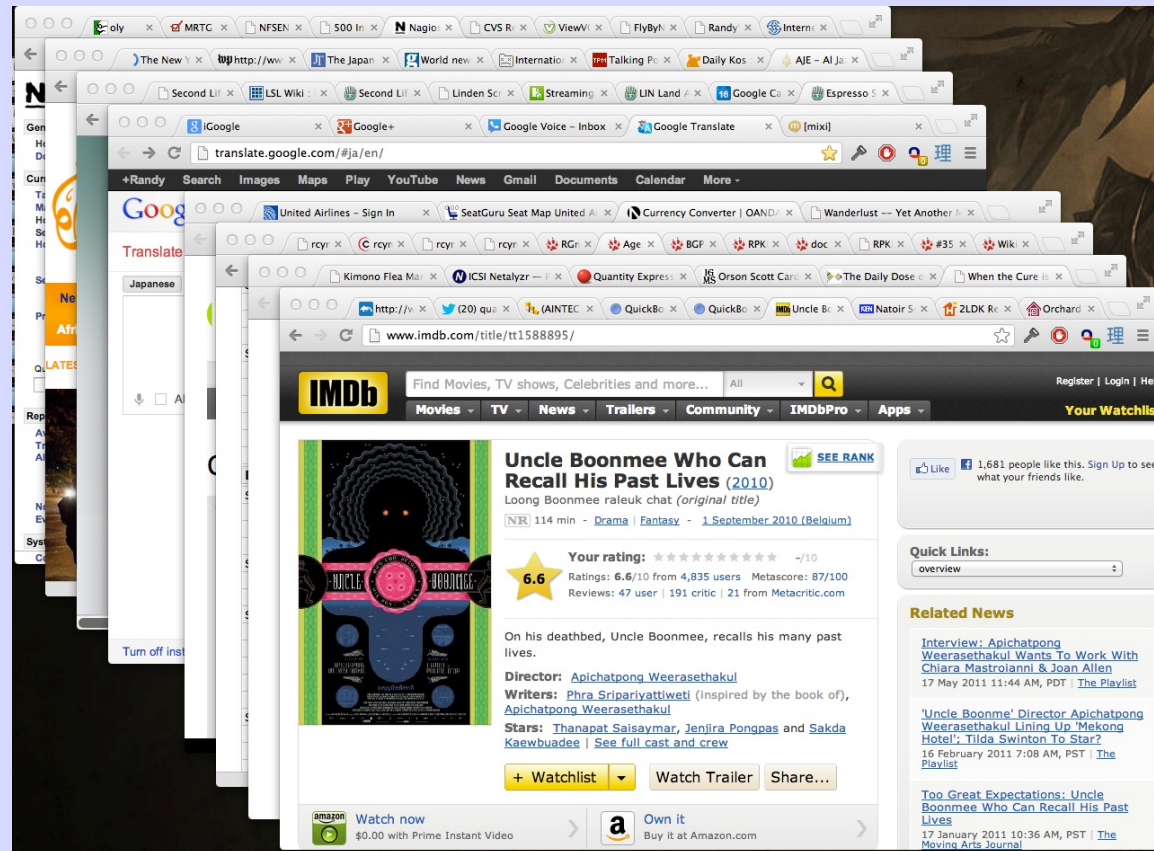
Internet Explorer

- Long History of Vulnerabilities
- First Target because of Popularity
- Microsoft is Not Always Concerned with Your Privacy
- Closed Source, No One Inspects it
- Does SandBoxing, so Reasonably Safe

Sometimes I Use Chrome

- Process Isolation per Tab, so scales well

And
I
Care!



- But I Worry About Leaking Data to Google

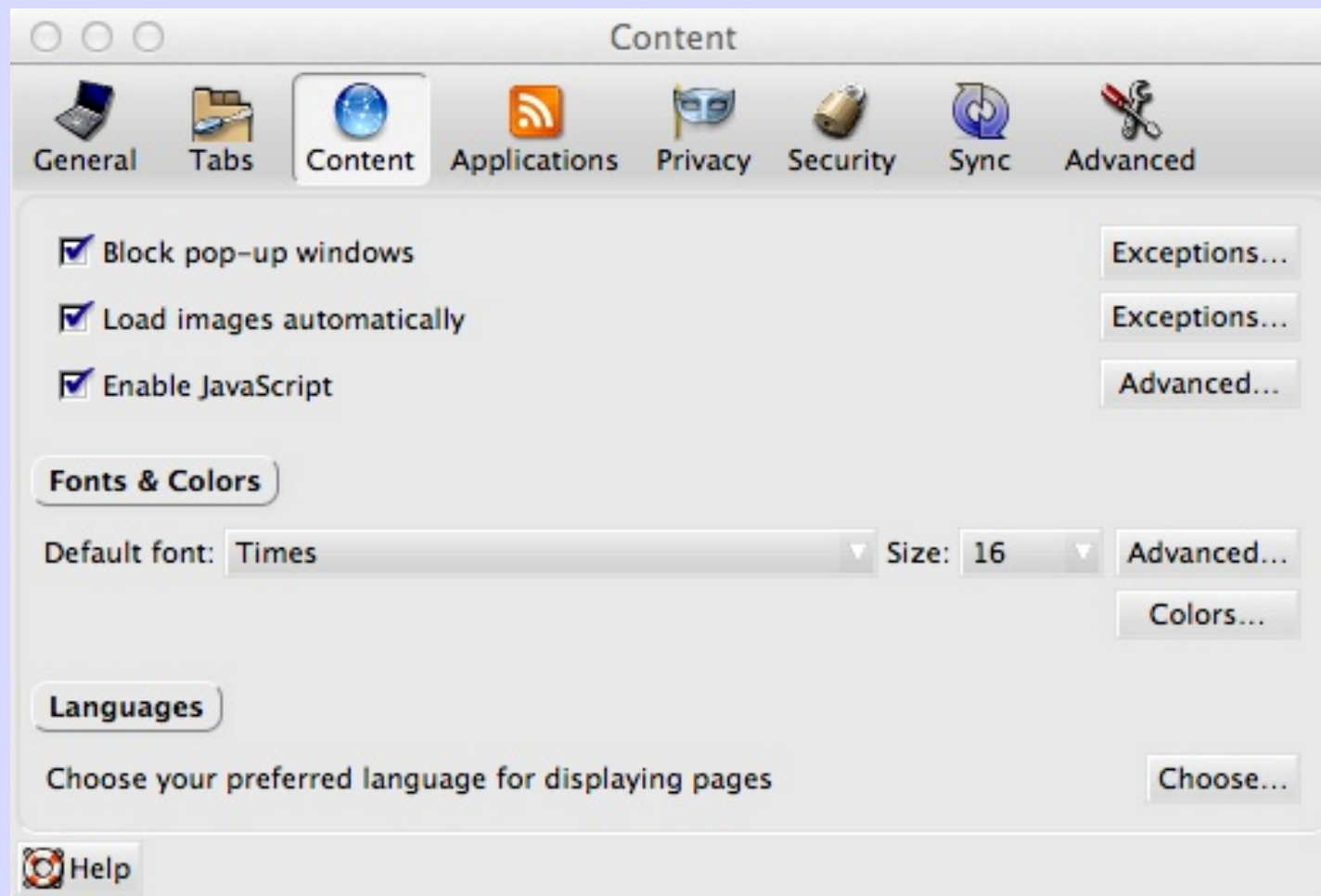
I Recommend FireFox

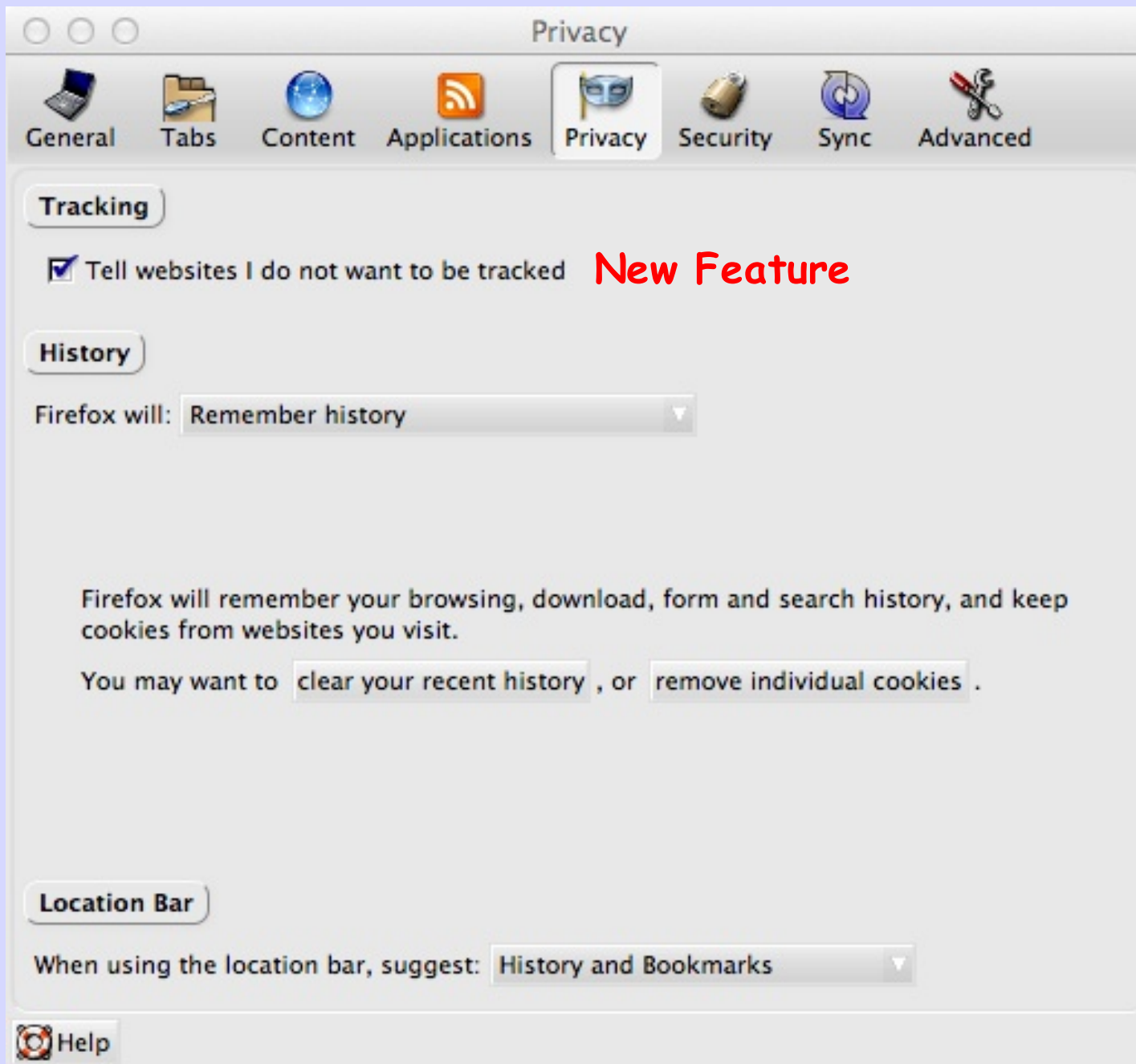
- Free and Open Source (i.e. inspected)
- Standards Compliant, no Proprietary Tricks to Lock You In
- Popular, so has Rich Extension Catalog
- Runs on All Significant Platforms

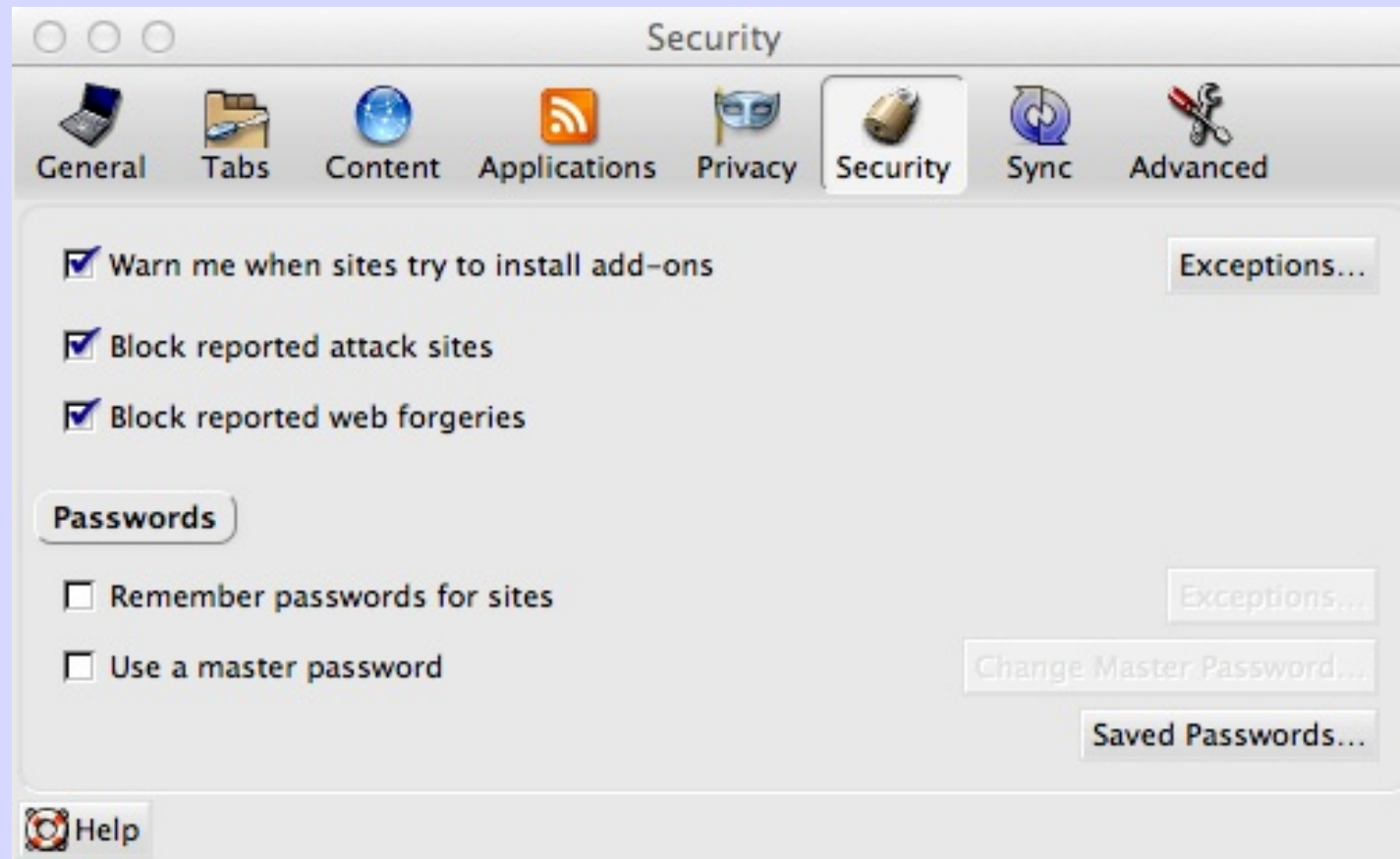
Let Browser Remember Passwords

- Only if you use Full Disk Encryption
- Only if your Laptop Locks Quickly
- Lose Laptop and Lose your Bank Account
- Use 1Password or LastPass managers


Prefs - Content











Plug-Ins

 Get Add-ons

 Extensions


 Appearance

 Plugins


 Services

Some extensions could not be verified


Search all add-ons

**1Password**
Password and identity manager for Mac, Windows, iOS and Android. [More](#)


DisableRemove

**Privacy Badger**
Protects privacy by blocking spying ads and invisible trackers. [More](#)


PreferencesDisableRemove

**The Addon Bar (restored)**
Gives you a place to put all your addon buttons without over-cro... [More](#)

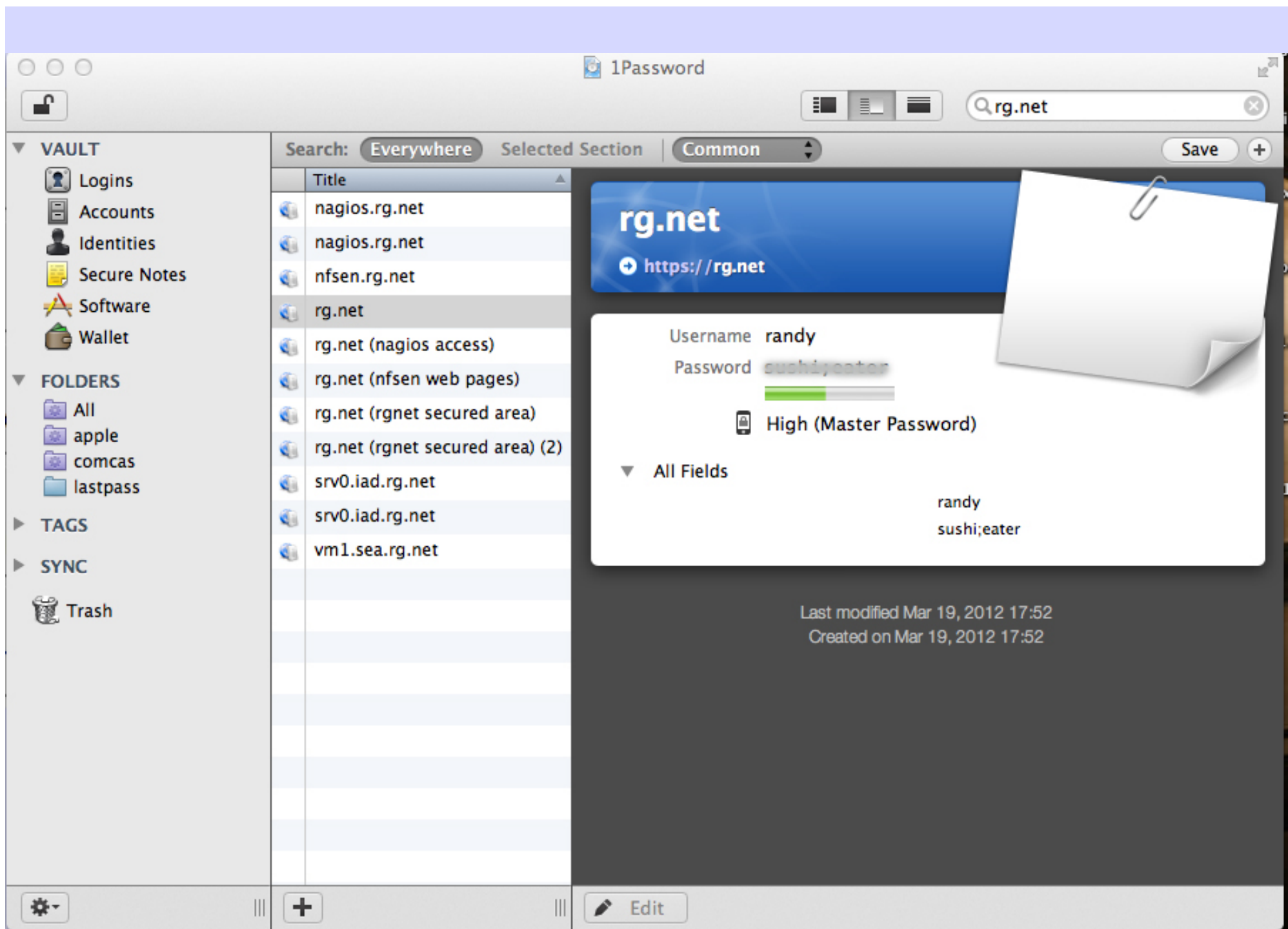
PreferencesDisableRemove

**uBlock**
A fast, potent, and lean blocker. Easy on CPU and memory. [More](#)

PreferencesDisableRemove

**Privacy Badger**
Protects privacy by blocking spying ads and invisible trackers. [More](#)

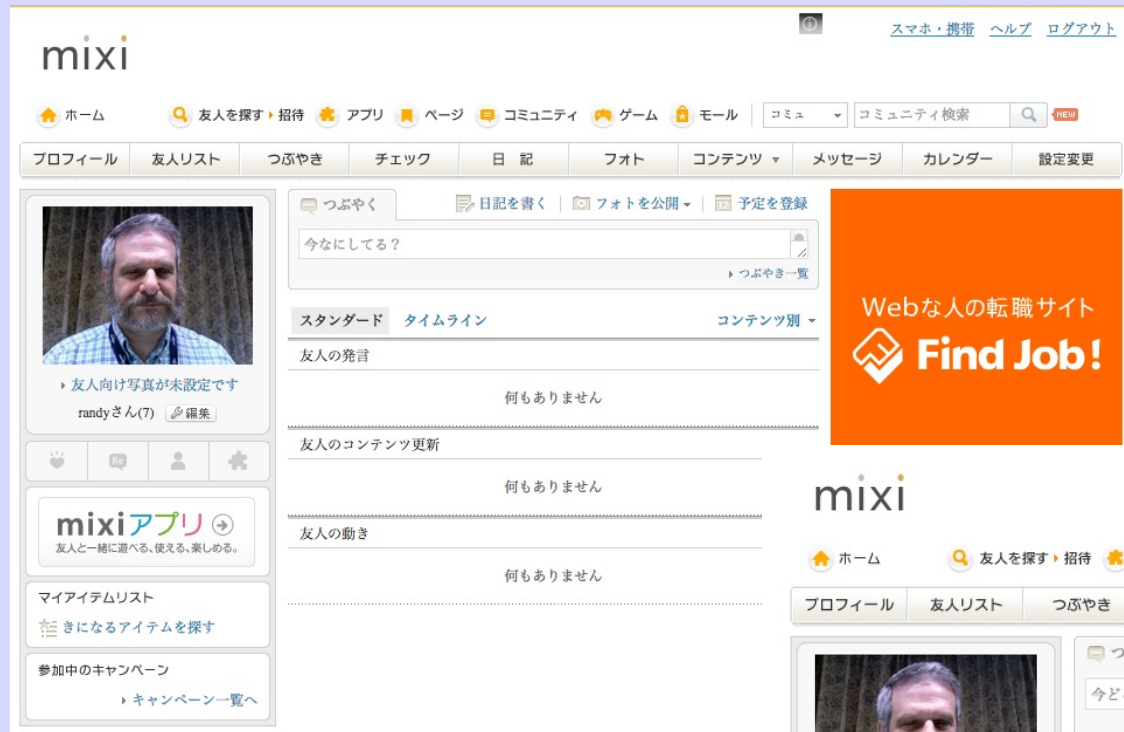
PreferencesDisableRemove



LastPass

- Runs on Most Platforms
- Plug-Ins for Most Browsers
- Passwords, Credit Cards, Addresses, ...
- Keep DataBase in DropBox and you
Have Data on Phone, Laptop, Tablet, ...

uBlock

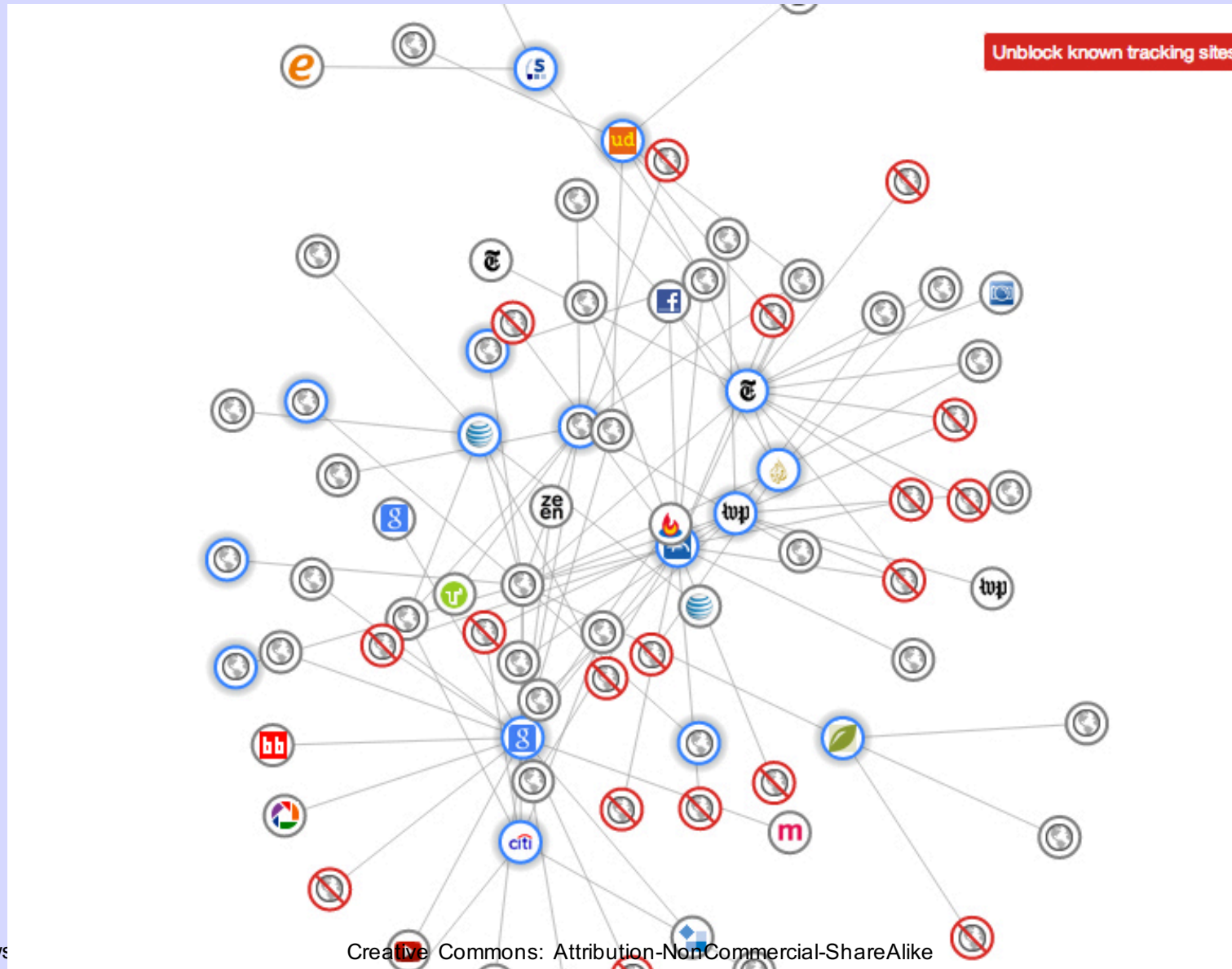


Without uBlock

With uBlock



Privacy Badger



Disconnect Blocks Too

The screenshot shows a web browser window with the address bar displaying 'Wikipedia (en)'. The main content area shows the New York Times website, dated Saturday, November 17, 2012. A large image of a grocery store aisle filled with boxes of Twinkies and other snacks is visible. Overlaid on the right side of the browser is a dark blue 'Do Not Track Plus' notification box. The box contains the following information:

- Blocking tracking @ nytimes.com** (with an 'Allow site' button)
- 1 social network tracking you: 1 blocked** (with a social media icon)
- 2 ad networks tracking you: 2 blocked** (with an 'AD' icon)
- 5 companies tracking you: 4 blocked** (with a building icon)
- In Control! Your all-time total is: 176 blocked**
- Abine.com | the online privacy company**
- How DNT+ works | Settings | Say hello**
- Special Offer For DNT+ Users** (button)
- Be Safe on Public WIFI** (button)
- Support DNT+: Review Us!** (button)

At the bottom of the browser window, the text 'COMMON SENSE' is visible.

NoScript - JavaScript



HTTPS Everywhere

- If a Site has HTTP and HTTPS, it Forces Use of HTTPS
- I.e. You get Authentication of Site
- Your Traffic is Encrypted
- Becoming Obsolete

DNSsec & DANE

- The green lock tells you that the site's TLS certificate is valid
 - You are talking to the right site
 - Your traffic is encrypted
- Want to know if the site you are visiting is DNSsec signed?
- Want to know if the cert is really valid?

There's an AddOn



1Password

Password and identity manager for Mac, Windows, iOS and Android. [More](#)

Disable

Remove



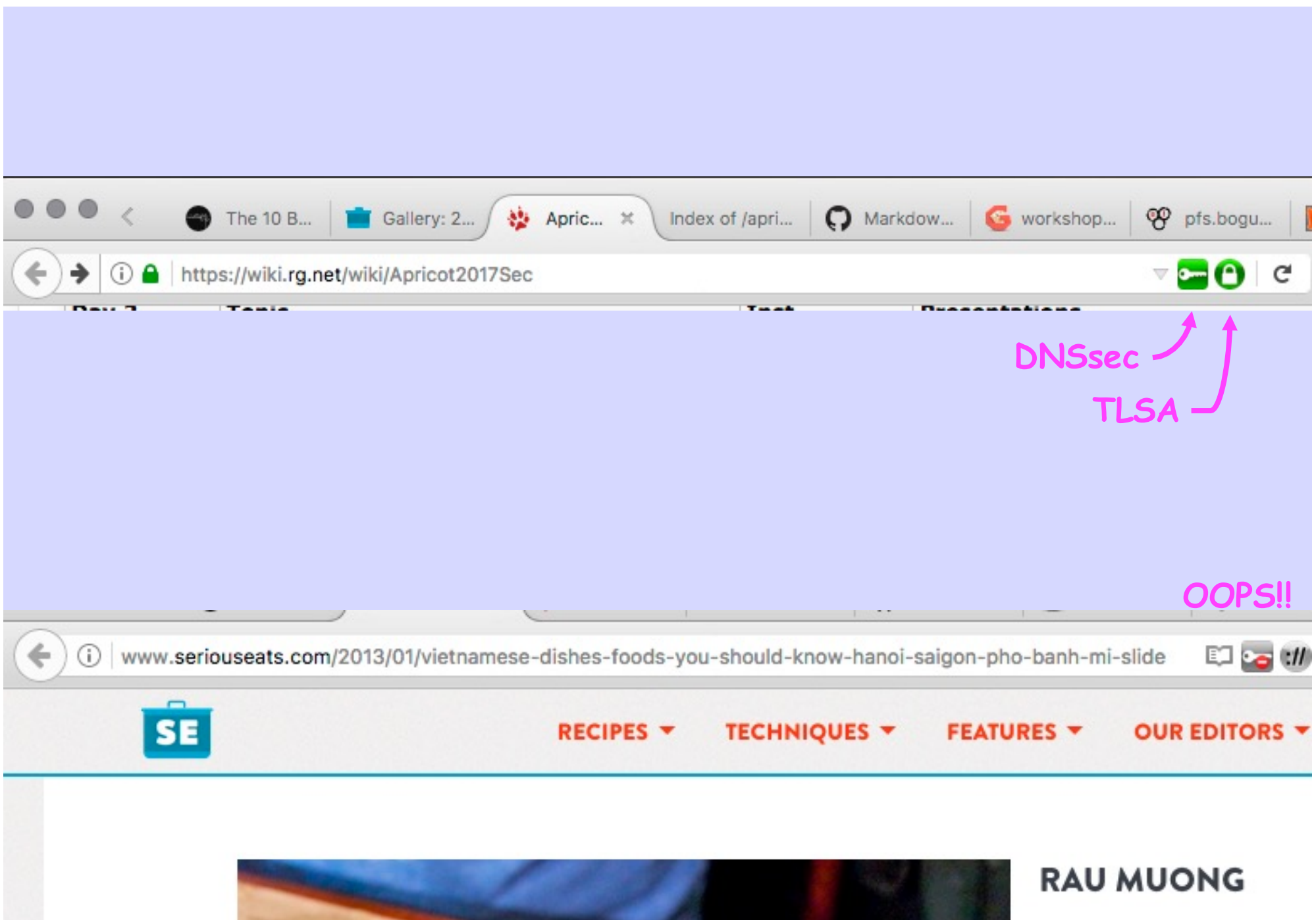
DNSSEC/TLSA Validator

Check DNSSEC security of domain names and chec... [More](#)

Preferences

Disable

Remove



Install & Configure

- <https://mozilla.org/firefox/>
or IE or Safari if you insist
- Configure for Privacy
- <https://www.eff.org/privacybadger>
- <https://www.ublock.org/>
- <https://addons.mozilla.org/en-US/firefox/addon/dnssec-validator/>
- <https://lastpass.com/>