ONLINE PRIVACY AND SECURITY

Digital Security for Journalists and Human Rights Defenders

By Ronalyn V. Olea | Bulatlat, NUJP

CHOOSING THE RIGHT BROWSER

Go to https://coveryourtracks.eff.org/
to check your browser

The company collects a lot of personal information about you.

If you want to maximize your privacy, install these add-ons:
Privacy Badger
Cookie Auto delete
Facebook Container
Firefox Multi-Account Containers

Private

Secure

Ads blocks

HTTPS upgrading

Private window with TOR

ACCESSING WEBS SECURELY

Minimize browser leakage

1. Use a “private browsing” mode. This option is available with Firefox, Safari, Chrome.

2. Change your default search engine to something like DuckDuckGo or StartPage. These privacy-protecting search engines are noncommercial—they don’t track you or collect personal information or search history.

ACCESSING WEBS SECURELY

3. Clear your browsing history regularly. If your browsing history is stored in your browser (which in most browsers is the default), it can be collected by a variety of companies as you browse the web.

4. Opt out of Google and Apple showing you “personalized ads”: On Android you can find the opt-out in the Ads Settings; on iPhone, scroll down to the bottom of your Privacy settings to Advertising > Limit Ad Tracking.

https://slate.com/technology/2017/02/cybersecurity-self-defense-how-to-increase-security-on-your-smartphone.html

ACCESSING WEBS SECURELY

Consider using VPN

- Disguises your actual network IP address and encrypts internet traffic between a computer (or phone or any networked “smart” device) and a VPN’s server.
- Acts as a sort of tunnel for your internet traffic, preventing outsiders from monitoring or modifying your traffic. Traffic in the tunnel is encrypted and sent to your VPN, which makes it much harder for third parties like internet service providers (ISPs) or hackers on public Wi-Fi to snoop on a VPN users’ traffic or execute man-in-the-middle attacks.

ACCESSING WEBS SECURELY

Consider using VPN

- - Offers more privacy and security, but does not make you completely anonymous online: your traffic can still be visible to the operator of the VPN.
- - not the same thing as an ad blocker, does not, by default, disrupt other sorts of online tracking.
- Free VPN apps: Psiphon and Tunnelbear

ACCESSING WEBS SECURELY

TOR and VPN

- Tor is a free browser that provides maximum anonymity through a decentralized server network. It is best for transmitting highly-sensitive information, but it’s extremely slow.
- There's the probability that exit nodes could read unencrypted data, but not the source of such data.

GOOGLE AND PRIVACY

GOOGLE AND PRIVACY

1. Find out what Google thinks about you
http://www.google.com/settings/ads/

2. Find out your location history
https://maps.google.com/locationhistory

3. Find out your entire Google Search history
https://www.google.com/history/

GOOGLE AND PRIVACY

4. Find out all the apps and extensions that are accessing your Google data https://security.google.com/settings/security/permissions

5. Google also keeps a history of your YouTube searches https://www.youtube.com/feed/history/search_history

GOOGLE AND PRIVACY

6. Export all of your data out of Google

Google lets you export all your data: bookmarks, emails, contacts, drive files, profile info, your youtube videos, photos and more here:
https://www.google.com/takeout

Source: http://www.google.com/goodtoknow/online-safety/security-tools/

SECURING YOUR GOOGLE

A walk-through on Google Privacy and Security Settings

https://www.google.com/settings/dashboard

SECURING YOUR GOOGLE

On Android, you can open up Settings then pick Google to tweak some data-tracking options. Tap Google Account; tap Ads to opt out of personalized ads specifically on your phone.

Tap Location from the menu to turn off location tracking completely for the Android device you're using.

If you'd rather restrict this on an app-by-app basis, go to Apps & notifications, then Advanced, then App permissions instead.

SECURING YOUR GOOGLE

On iOS, open up the Google app for iOS, tap the three dots lower right, and then choose Privacy and Security, you can stop Google from tracking your location on this particular device.

To do it on an app-by-app level, head to the main iOS Settings screen, then choose Privacy and Location Services, and find the app you're looking for. Each app can be granted permission to view your location all the time, only when the app is being used, or never.

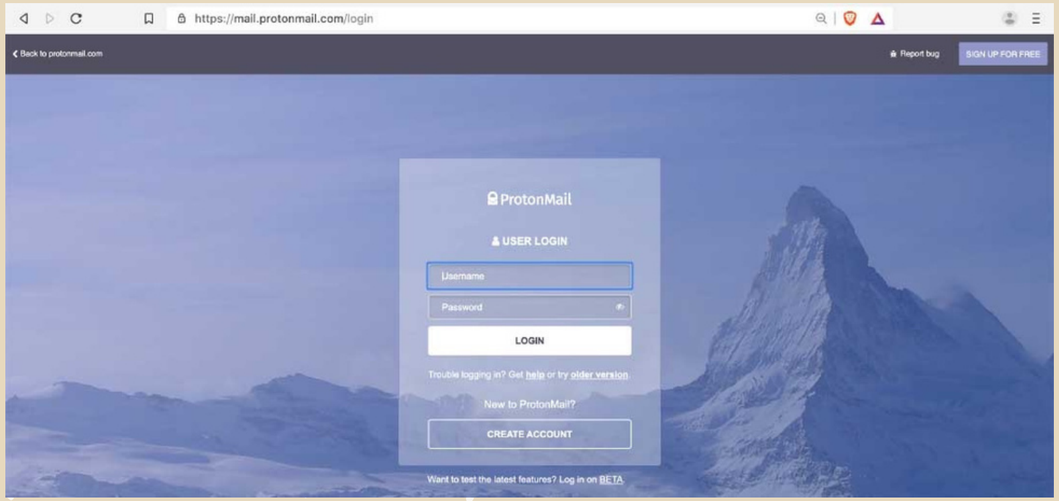
ONLINE SECURITY- EMAIL

- All of the information contained in your inbox, your sent folder and your address book are only as secure as your digital security practices.

EMAIL

Google collects a lot of information about its Gmail users that can put you at risk. If you must use Gmail, read its privacy policy and understand the risks.

EMAIL



ProtonMail offers end-to-end encryption if you are sending an email to another ProtonMail account. Emails sent to recipients who do not have a ProtonMail account can also be encrypted with an added password that the recipient must know.

EMAIL

- Consider setting up multiple email accounts and using one or more as a decoy. Setting up new email accounts will make it more difficult to identify and monitor you.
- Make it difficult to link your identity to your email account(s).

EMAIL

- Don’t open emails with suspicious subject lines; they may contain viruses or malware.
- Don’t open attachments from email addresses that you don't recognize; they may contain viruses or malware.

PHISHING

Electronic equivalent of fraud

Take the quiz:
https://phishingquiz.withgoogle.com/

PROTECTION VS PHISHING

- Keep all your software updated (OS, apps, AV
- Examine messages and emails and their content
- Look for spelling mistakes, errors and check facts
- Verify emails with senders

PROTECTION VS PHISHING

- Test URL and files in virustotal.com
- Open suspicious files in Google Drive
- Use 2FA to protect your online accounts

MALWARE

Malware is what infects your PC. The word is a combination of “malicious” and “software,” and it refers to viruses of all kinds.

- From infected hardware (such as USB sticks)
- From unlicensed or cracked software (e.g., fake download sites)

MALWARE

- By clicking malicious links to download viruses (e.g., fake advertisements)
- By downloading them through malicious email attachments
- Through social engineering attacks (i.e., impersonation)
- By downloading them through scams on social networking sites.

PROTECTION VS MALWARE

- Keep your software and OS up to date
- Install and keep up to date an anti virus software
- Use password manager
- Do not use pirated software
- Install a Firewall that helps protect your device!