



Enhancing Online Anonymity Smart Card

Why is striving for online anonymity important?

- Everything you do on the Internet involves sharing your identity information
- Identity information can be compared across services by advertisers and data brokers to build consumer profiles
- This data can also be compiled by identity thieves and malicious actors to gain access to bank accounts and other sensitive information

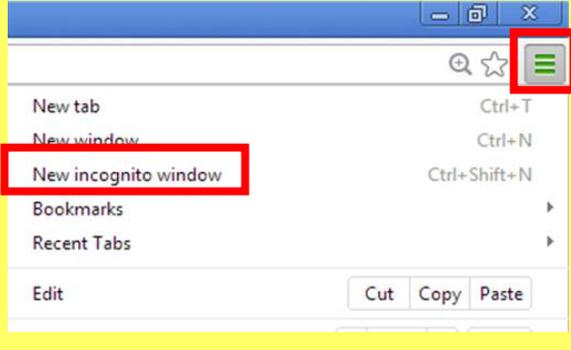
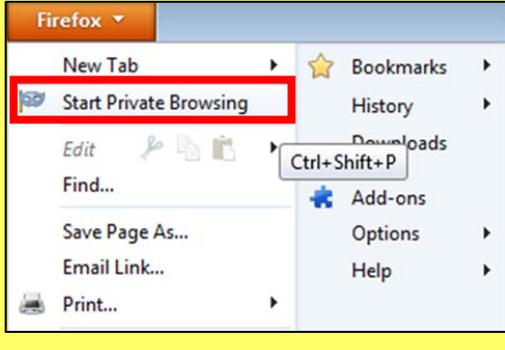
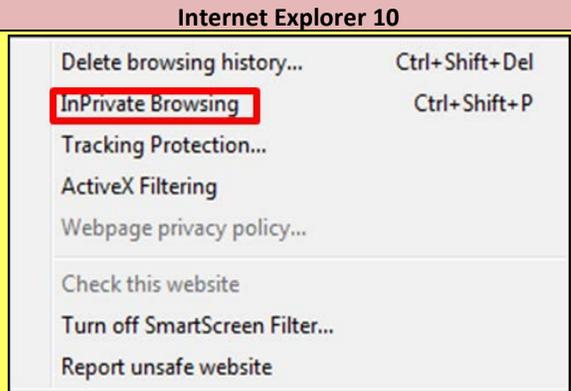
There's no such thing as total anonymity online. Generally, though, how can I make my online activity more anonymous?

- Use different email accounts, user names, and passwords for different kinds of activity (e.g., banking, instant messaging, social media). For more information on creating emails, see the *Anonymous Email Services* smart card
- Use a pseudonym whenever possible; don't volunteer information to websites unless they require it
- For more enhanced anonymity, consider using TOR, a free browser that anonymizes your IP address. To install TOR, see the *Anonymous Email Services* smart card

Browsing

VULNERABILITY: browsers allow websites to install cookies to track your online activity

Recommendation: private browsers do not store most cookies

Google Chrome	Mozilla Firefox	Caveats
		<p>Secure browsing still relays your IP addresses to the websites you visit.</p> <p>You must close the browser for activity to be deleted.</p>
		<p>Your Internet Service Provider (ISP) can still see your browsing activity.</p>

Internet Searches

VULNERABILITY: searches may be recorded and associated with IP address, user agent, or identifiers stored in cookies

Recommendation: Search Obfuscation

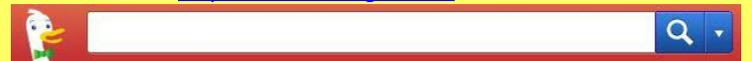
- Use general search terms
- Identify a topic of interest from linked sites
- DO NOT search using location or individual name, or specific topics



The image shows two Google search boxes. The first has the search term 'news' and a green checkmark next to it, indicating it is a good search term. The second has the search term 'traffic in clarendon va' and a red X next to it, indicating it is a bad search term because it is too specific and includes a location.

DuckDuckGo

- Uses an encrypted connection by default
- Only retains cookies related to users' settings preferences
- Does not store users' IP addresses, search queries, or personal information.
- Browser extensions for Firefox, Chrome, Internet Explorer, Safari, and Opera
- Available at: <https://duckduckgo.com/>





Enhancing Online Anonymity Smart Card

Enhancing Online Anonymity Smart Card HK 100813_1145

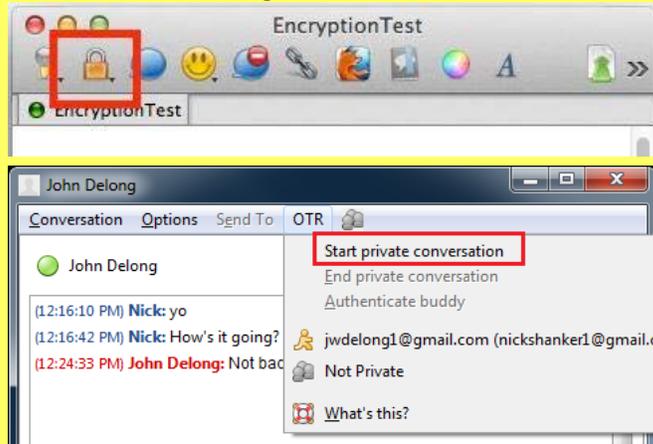
Instant Messaging

- Performed on services such as Adium, Pidgin, Google Chat
- Allows users to send instant messages from desktop and mobile devices that may contain images, audio clips, and videos
- Accessed through either explicit registration or implicit registration through an email service

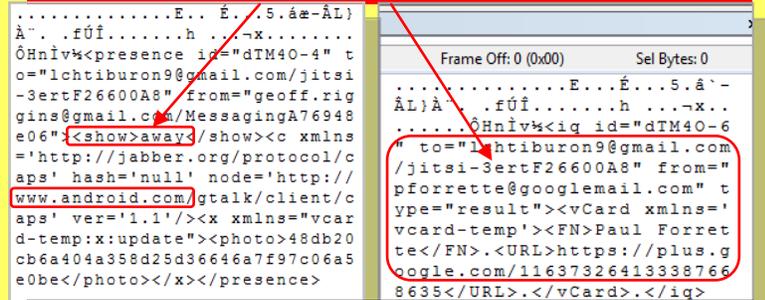
VULNERABILITY: message histories can be intercepted; packet contents of chats can be intercepted; usernames can link to email addresses

Recommendation: Off The Record (OTR) Messaging

- Encrypts instant messages
- Does not save chat logs



Chat clients may store users' passwords in a local text file on users' PCs (Pidgin); they may also share information such as status, device, contact list, and email address in packet



Best practices include: 1) using separate emails for chatting and emailing 2) registering for chat clients with a pseudonym used only with that chat client

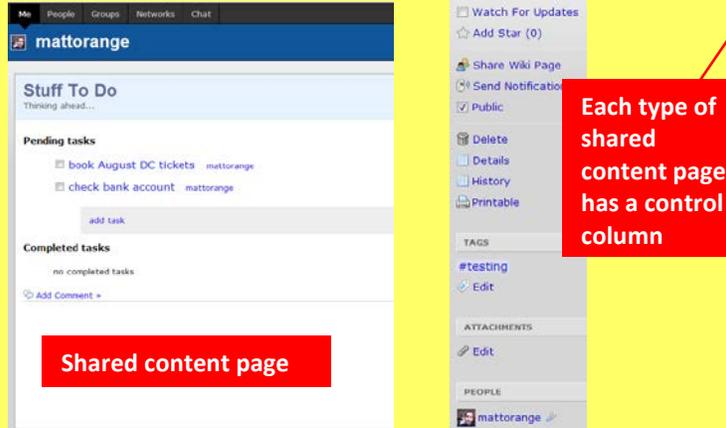
File Sharing

- Allows users to store, share, and create files such as Office Docs, image, video, and audio files
- Include services such as DropBox, Google Drive, Evernote
- Cloud or web based

VULNERABILITY: sharing private information on SNS; users sharing documents; weak password protection

Recommendation: Crabgrass <https://we.riseup.net/crabgrass>

- Allows users to register with only an email address
- Supports file sharing, collaborative wikis, group pages



When sharing files online, be sure to 1) verify sharing permissions are set to ONLY users you wish to share with 2) verify that, if possible, links to shared files can be set to expire 3) ensure that both the sender and receiver have non-identifying user names

Recommendations: File Tea <https://filetea.me/default/>

- Does not require registration
- File contents are not cached or stored server side
- Server never analyzes or processes the files being transferred
- No cache or log entry of a file transfers are kept
- IP addresses of users are never stored

Once the file is uploaded, a link can be copied and pasted to emails or chats; once the browser window is closed, the link expires

