if you
SEE SAY
SOMETHING SOMETHING®
CYBER

NEW YORK STATE | Counter Terrorism | Cyber Incident Response Team

Andrew M. Cuomo
Governor

Web Browser Security

Web browsers are the most common way that users interact with the Internet, making them a primary target for cybercriminals. A few simple steps can reduce browser-based risks to your privacy and the security of your computer.

Here are some tips to help you secure your web browser:

Keep browsers up-to-date

- Keeping your browser updated to the latest version is one of the best ways to stay secure

Minimize the usage of browser plugins (sometimes called "add-ons")

- Plugins provide useful features but may also collect information about you or weaken your computer's security
- Browser-based attacks often target plugins instead of the browser because they're more likely to be out of date

Verify the URL you are visiting

- Use caution when following links forwarded to you via email or other means (think about who sent the link and why)
- Hover over the link to see if it's directing you to the same site that's displayed on the page
- If you're still uncertain about a link, contact your help desk or technical support team for guidance

Ensure you are using Hypertext Transfer Protocol Secure (HTTPS)

- HTTPS secures your connection to the site you're visiting and makes it harder for someone to intercept your data
- Most reputable websites are HTTPS-enabled and display a padlock in the address bar to let you know

Pay careful attention to warnings and pop-ups like browser requests

- Don't grant permissions or ignore warnings unless you're sure those actions are necessary and appropriate
- When in doubt, contact your help desk or technical support team for guidance

If you suspect a cyber incident, immediately contact:

CIRT is an initiative of the New York State Division of Homeland Security and Emergency Services.
For additional information, visit dhses.ny.gov/oct/cirt