



NATIONAL CYBER SECURITY AWARENESS MONTH



National Cyber Security Awareness Month Our Shared Responsibility What the Federal Government Can Do

1. Participate in National Cyber Security Awareness Month
2. Customize and print National Cyber Security Awareness Month posters for placement in government offices
3. Encourage employees to practice cybersecurity and protect their identity at home and in the workplace
4. Review cybersecurity top tips (available at www.staysafeonline.org) at departmental meetings
5. Add cybersecurity top tips (available at www.staysafeonline.org) to departmental websites
6. Review and update network and computer acceptable use policies
7. Remind all computer users to change their passwords on a regular basis. Use long, complex passwords (letters, numbers, and symbols) to help thwart hackers
8. Conduct annual cybersecurity training for federal employees
9. Encourage citizens to report cyber crimes to the FBI's Internet Crime Complaint Center (www.ic3.gov) and the FTC (spam@uce.gov)
10. Provide cybersecurity resources on federal websites. Link to: www.us-cert.gov/cas/tips/, www.onguardonline.gov and www.staysafeonline.org.
11. Offer cybersecurity education webinars for federal employees, contractors and other stakeholders. Contact NCSA for more information. info@staysafeonline.org (subject line: education webinars)
12. Provide employees with information about NCSA's C-SAVE Program (Cyber Security Awareness Volunteer Education): A program to engage IT and cybersecurity professionals to volunteer to teach basic cybersecurity awareness in local K-12 schools and encourage their participation.

Our Shared Responsibility

 **STAYSAFEONLINE.org**
National Cyber Security Alliance

OCTOBER 2009