

Spread the word with daily online safety and preparedness tips on Google+, Facebook and Twitter. Use the following blog, or create your own, and post all throughout the month. Remember to include the hashtags **#COReady #NCSAM #CyberAware**

### Simple Steps to Online Safety

October is [National Cyber Security Awareness Month](https://www.dhs.gov/national-cyber-security-awareness-month) (NCSAM), the annual campaign to raise awareness about the importance of cybersecurity. The internet touches almost all aspects of everyone’s daily life, whether we realize it or not. [NCSAM](https://www.dhs.gov/national-cyber-security-awareness-month) is designed to engage and educate public and private sector partners through events and initiatives to raise awareness about the importance of cybersecurity, provide them with tools and resources needed to stay safe online, and increase the resiliency of the nation in the event of a cyber incident.

All members of the public can take some simple actions to protect themselves online and to recover in the event a cyber incident occurs.  Week one addresses the top consumer cybersecurity concerns, provide simple steps to protect against these concerns, and help the public understand what to do if they fall victim to cybercrime.

Unlike preparing for physical threats such as fires or natural disasters, the best preparedness for and defense against cyber threats is practicing safe online behaviors every day. When you are smart about your online behaviors, you not only protect yourself but also your family, community and workplace. Be cyber prepared by practicing these simple online safety habits every day:

* **Be wary of free Wi-Fi networks.** Never bank or shop over free Wi-Fi networks. Free Wi-Fi is often not secure. You risk cyber criminals gaining access to your accounts and stealing your personal information.
* **Think before you click.** Do not click on links or open email attachments you do not trust. Look closely at the link or the sender of the message to make sure it is legitimate. When in doubt, throw it out – ignore the link or delete the email.
* **Protect your privacy.** Review the privacy settings on your social media accounts to limit who can see your information. Never post sensitive information – such as your address, birthday or phone number – publicly.
* **Back up your data.** With threats like ransomware on the rise, it is more important than ever to protect your valuable work, music, pictures and other digital information by keeping back-up copies.
* **Set strong passwords:** Do not use the same password twice, and choose passwords that are hard to guess and contain a combination of letters and numbers.

Cybercrime impacts all of us, not just large corporations, and cyber criminals are only getting more sophisticated. According to the Pew Research Center, nearly [two-thirds of Americans](https://www.dhs.gov/redirect?url=http%3A%2F%2Fwww.pewinternet.org%2F2017%2F01%2F26%2Famericans-and-cybersecurity%2F) have beenpersonally affected by a cybercrime like hijacked email accounts, fraudulent credit card charges, identity theft, and stolen sensitive information such as Social Security or financial account numbers.

If you become the victim of a malware attack, phishing scheme, or other cybercrime, contact your local law enforcement or the United States Computer Emergency Readiness Team (US-CERT) at [www.us-cert.gov/forms/report](http://www.us-cert.gov/forms/report).

### Resources

* [Department of Homeland Security](https://www.dhs.gov/national-cyber-security-awareness-month)
* [Stop.Think.Connect](https://www.stopthinkconnect.org/)

For more tips and preparedness information, follow us:
On Twitter: [@READYColorado](http://www.twitter.com/readycolorado)
Facebook: [www.Facebook.com/READYColorado](http://www.Facebook.com/READYColorado)
Google +: [READYColorado](https://plus.google.com/100167075139424077484)
YouTube: [www.youtube.com/READYColorado](file:///C%3A%5CUsers%5Cmtrost.DPS%5CDocuments%5CMicki%5CPrepareColorado%5CMay2015%5Cwww.youtube.com%5CREADYColorado)