

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**

### Cybersecurity in the Workplace is Everyone’s Business

Creating a culture of cybersecurity is critical for all organizations ‒ large and small businesses, academic institutions, non-profits, and government agencies – and must be a shared responsibility among all employees. As part of [National Cybersecurity Awareness Month](https://www.dhs.gov/national-cyber-security-awareness-month), this week highlights how organizations can protect against the most common cyber threats. The week also looks at resources to help organizations strengthen their cyber resilience, including the use of the [National Institute of Standards and Technology Cybersecurity Framework](https://www.nist.gov/topics/cybersecurity).

Businesses face significant financial loss when a cyberattack occurs. Cybercriminals often rely on human error – from employees failing to install software patches to clicking on malicious links – to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of every employee to keep data, customers, and capital safe and secure.

Follow these simple tips from the [Stop.Think.Connect.™ Campaign](https://www.stopthinkconnect.org/about) to help foster a culture of cybersecurity in your organization.

1. **When in doubt, throw it out**. Stop and think before you open attachments or click links in emails. Links in email, instant message, and online posts are often the way cybercriminals compromise your computer. If it looks suspicious, it is best to delete it.
2. **Back it up**. Make electronic and physical back-ups or copies of all your important work. Data can be lost in many ways including computer malfunctions, malware, theft, viruses and accidental deletion.
3. **Guard your devices**. In order to prevent theft and unauthorized access, never leave your laptop or mobile device unattended in a public place and lock your devices when they are not in use.
4. **Secure your accounts**. Use passwords that are at least eight characters long and a mix of letters, numbers and characters. Do not share any of your usernames or passwords with anyone. When available, turn on stronger authentication for an added layer of security, beyond the password.
5. **Report anything suspicious**. If you experience any unusual problems with your computer or device, report it to your IT Department.
6. **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.

Small businesses may not consider themselves targets for cyberattacks due to their small size or the perception that they do not have anything worth stealing. However, small businesses have valuable information cyber criminals seek, such as employee and customer records, bank account information and access to the business's finances and access to larger networks. In some ways, small businesses are at a higher risk of cyberattacks than larger businesses because they often have fewer resources dedicated to cybersecurity.

The [National Institute of Standards and Technology Cybersecurity Framework](https://www.nist.gov/topics/cybersecurity) (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities. The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation. NIST’s cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country’s ability to address current and future computer and information security challenges.  For more on NIST you can visit their website at [www.nist.gov](file:///C%3A%5CUsers%5Cmtrost%5CDocuments%5CMicki%5CPrepareColorado%5C2017%5Coctober%202017%5Cwww.nist.gov).

### Resources

* [National Institute of Standards and Technology Cybersecurity Framework](https://www.nist.gov/topics/cybersecurity)
* [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)