



CyberSecurity4biz.com

can your business survive without its data?

New Year, New Digital You

When Americans reflect back on the previous year and think about their aspirations for 2021, [common goals range from getting more exercise to learning a new skill to traveling or reading more.](#)

At the beginning of a new year in today's hyper-connected and often remote world, it's prime time to think about a new, improved digital you. By taking some smart, simple steps, you can greatly impact the safety and security of your online identity.

“Year round, the National Cyber Security Alliance encourages everyone to be safe and secure online,” said Kelvin Coleman, NCSA's executive director. “However, during times of national hardship, such as the coronavirus outbreak, bad actors increase their fraudulent activities. As such, we urge everyone to be extra vigilant against online scams, including phishing and malware, that are more prevalent in times like these.”

NCSA's Top Recommendations for a New Digital You

- **Think Before You Click.** Cyber criminals are distributing malware campaigns that impersonate reputable sources by asking you to click on links. Slow down. Don't click. Go directly to a reputable website to access the content. As more employees work and learn from home, basic security measures need to be taken to protect the individual and enterprise from cyber criminals who are taking advantage of lax security practices. Review more [NCSA tips for remote workers.](#)
- **Connect to a secure network and use a company-issued Virtual Private Network to access any work accounts.** Home routers should be updated to the most current software and secured with a lengthy, unique passphrase. Employees should not be connecting to public WiFi to access work accounts unless using a VPN. Separate your network so your company devices are on their own WiFi network, and your personal devices are on their own.
- **Share with care.** Be aware that when you post a picture or message, you may also be inadvertently sharing personal details and sensitive data with strangers about yourself, family and friends. It is OK to limit who can see what you share. Learn about privacy and security settings on your favorite websites. NCSA has an excellent and recently updated resource that includes direct links to [update your privacy settings](#) on popular devices and online services.
- **Lock Down Your Login.** Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. A strong passphrase is a sentence that is at least 12 characters long. Focus on sentences or phrases that are easy to remember. On many sites, you can even use spaces. MFA will fortify your accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device. This additional layer of security makes it harder for cybercriminals to log in as if they were you.



Get Started Now

There are some low-lifts that can help jumpstart your New Year, New Digital You at home and/or in the workplace.

- Have a family meeting to discuss the importance of protecting privacy and take action by configuring privacy settings.
- Volunteer at your local senior center to help this vulnerable audience learn basics like creating secure passphrases.
- Post this tip sheet up in the breakroom or distribute it through email.
- Talk to a local school group about configuring privacy settings. Help students of all ages understand how to put this information into play in their local communities to “spread cyber cheer, not fear”.
- Host a virtual “lunch and learn” for your staff. Train your employees to practice safe online behaviors.



[Learn More About Data Privacy Day.](#)
[Become a Data Privacy Day Champion](#)



CyberSecurity4biz.com

can your business survive without its data?