# TALKING TO YOUR CHILD ABOUT CYBER SECURITY

**Resources for Families**

Technology has become fully integrated into young people's lives, and it is nearly impossible for parents or guardians to know everything their teens are doing online. The goal should not be for parents to monitor everything, but instead to teach teens how to be responsible digital citizens. NCSA recommends parents and guardians take time to discuss cybersecurity best practices with their teens.

## We recommend a few critical points to stress:

PRIVACY AND SECURITY SETTINGS EXIST FOR A REASON Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.

ONCE POSTED, ALWAYS POSTED Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70 percent of job recruiters rejected candidates based on information they found online.

KEEP PERSONAL INFO PERSONAL Limit how much you reveal about your daily routines, habits or travels. The more information you post, the easier it may be for a hacker or someone else to steal your identity, access your data or commit other crimes such as stalking or cyberbullying.  If you ever feel uncomfortable or threatened by someone online, immediately stop communicating with that person and alert a responsible adult.

## Cell Phone Security

Be careful when downloading apps. Hackers will create apps that look a lot like a genuine popular app but are actually malware. Check the permissions on all the apps you install.

Disable Bluetooth on your devices unless you're actively using it. It opens your phone up to being hijacked and having your data stolen. Similarly, public wifi networks can be penetrated by hackers – or even be set up and operated by data thieves – who can watch the traffic and see what you do online.

## Gaming Safety

Don't share personal information on gaming sites, or use gamertags or other profile information that could connect your gaming persona with your real life. Frustrations in games can turn into personal conflicts – with the potential to be very scary and even dangerous.

Free premium accounts, game tokens, skins, or weapons are often phishing attempts. Hackers may use these offers to capture your password, then steal the account or your identity.

## Passwords

Passwords are the keys to your digital life. Make sure they are at least 10 characters long – including letters, numbers and symbols to make them harder to crack. Passphrases can be easier to remember, but harder to crack.

Don't write your passwords down. Consider using a secure password manager. Two-factor authentication – either a physical security key or an app delivering time-based one-time passwords, like Authy or Google Authenticator gives you an extra layer of security.

Don't share passwords with friends. It's the same as giving them the keys to your house or your car – plus the power to see everything you've done and even impersonate you online. For the same reasons, don't save usernames and passwords on shared computers, and always log out when you're finished using someone else's device.

## Know and Manage Your Friends

Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) up to date with your daily life.

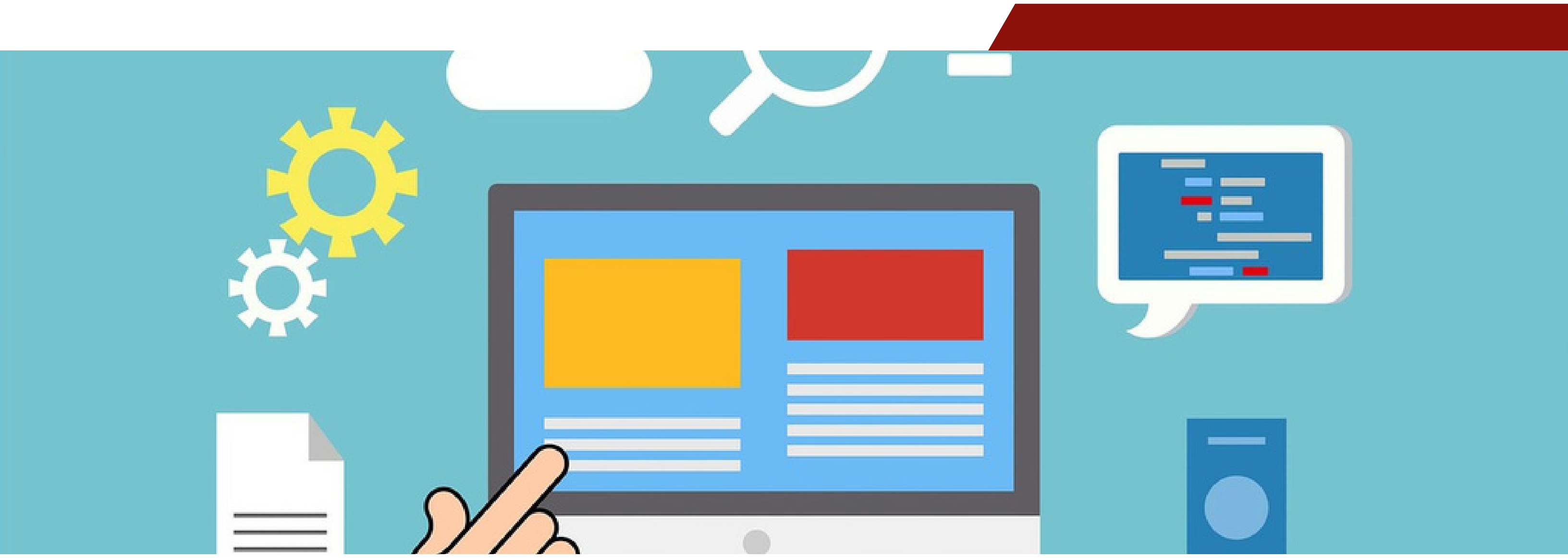
Also, you don't have to accept friend requests from everyone. If you don't know someone, it's perfectly fine not to accept their request to connect.

## Check Your Child's Credit

According to the Federal Trade Commission, it's a good idea to check your child's credit report regularly. This will allow you time to fix any errors or address any issues before they take out that fist loan or apply for their first job.

Cyber criminals are accessing credit of children from a young age. Sadly, by the time the issue comes up, it is often too late to determine what happened.

# RESOURCES



Stop.Think.Connect. Parent and Educator Resources: This webpage outlines essential resources and materials for parents and educators to help start the discussion about cyber safety and cybersecurity with children and students. Find information about safe social media practices, what it means to "be online," how to become a good digital parent, and more. stopthinkconnect.org/

Be Cyber Smart: This campaign is designed to inspire the younger generation of Americans to take responsibility for their own cyber safety. Learn about cybersecurity basics, common scams, and how to report cybersecurity incidents. dhs.gov/be-cyber-smart

StopRansomware.gov: This website is a one-stop resource where public and private sector entities can find U.S. government tools, information, and resources to help reduce the risk of ransomware attacks and improve resilience. The site includes a specific K-12 resource section, which includes information geared towards IT staff, students, parents, and administrators.

Wisconsin Department of Public Instruction Resources for Families DPI put together a comprehensive list of resources that can support raising a digital native. This site also includes an interactive resource for families and students to complete together. dpi.wi.gov/internet-safety/parents

## WHAT SHOULD YOU DO RIGHT AWAY?

Use strong, unique passwords and set up 2 factor authentication.

Think before you click/download.

Check your privacy settings on your network and all social media accounts.

Consider long term effects of what is shared online.

Discuss cybersecurity with your child.