



LOOKING FOR A JOB?

CYBER TIPS FOR YOUNG PROFESSIONALS

STOP.THINK.CONNECT.™ CAMPAIGN

WHAT DOES YOUR ONLINE PRESENCE SAY ABOUT YOU?

As a young professional, you've grown up using computers and the Internet. However, as information you share on the Internet becomes increasingly accessible to others, what steps are you taking to protect yourself? Young professionals must tailor their Internet behavior to protect themselves and their budding careers. It's important to determine how you will portray yourself—your personal brand—online as you look for a new job or as you grow in your current one. The Department of Homeland Security's [DHS] Stop.Think.Connect.™ Campaign offers suggestions for enhancing your online presence and avoiding potential embarrassing mistakes and security pitfalls to ensure you can have a smarter, safer online experience.

The 2013 Employment Screening Benchmarking Report by HireRight unveils that 61% of employers currently use, or plan to use, social media in their recruiting efforts.

Many young professionals are in the process of looking for a job. However, according to a 2013 survey by Microsoft, 84% of U.S. recruiters think it's proper to consider personal data posted online when evaluating a candidate and to do online research using search engines and social networking sites. On Device Research, 1 in 10 people ages 16 to 34 were rejected from a job based on the content of their social media profiles. When looking for a new job, be sure to remember these tips:

- **Rethink the Internet.** Cyber criminals are lurking. Your former and future employers are likely on the web to find out more about you. What you say and do is visible to others, and cannot be deleted. With newer digital applications, even your music tastes are visible to others. Make smart choices and think about how those online decisions might influence others' opinions of you.
- **Set Up Privacy Restrictions.** Your online social media network has likely expanded to include managers and colleagues who, depending on your privacy settings, have access to your photos, comments, check-ins, and status updates. Take the time to set up the appropriate settings for the various members of your network—keep your personal and professional world separate by customizing what your best friends see versus what your work and peripheral friends see.
- **Manage your Online Brand.** Have you checked yourself out recently online? Performing a quick search of yourself online is important to see what is being posted about you by others on the Internet. Consider setting up RSS feeds and alerts for searches on different variations of your name with your school[s], place[s] of employment, and other distinguishing details. For your social media accounts, regularly scan to see what pictures and content others are posting about you. Make sure to remove any evidence of questionable behavior, even if it's from college or high school. Only you can manage your online identity.

ON THE JOB CYBER TIPS FOR YOUNG PROFESSIONALS

It is important to consider the consequences of bad cyber hygiene when you're on the job. You should be sure to remember these tips:

- **Be Device Savvy.** It's important to protect all of your devices that connect to the Internet, including computers, smart phones, gaming systems, and other web-enabled devices, from viruses and malware by avoiding phishing schemes and installing trusted anti-virus software. Be sure to check with your IT department before downloading non-company issued software. Also, be careful when you mix your work and personal devices [e.g. hooking your personal phone to your work laptop]. Find out your employer's rules on syncing work email to your personal smart phone to ensure that does not pose a security threat.
- **Navigate Safely.** When you're doing online banking and shopping from your office, check to be sure the sites you navigate are secure. One quick clue to determine whether a website is safe is if the URL begins with "https://". The "s" means secure. Also, when using a public computer—such as one at your local library—avoid typing personal information because of key loggers and ensure you properly log out if you check your employee webmail.
- **Think Before You Act.** You should be wary of messages that implore you to act immediately or offer something that sounds too good to be true. Never willingly provide personal information or data on your organization, including its structure and networks. When you receive suspicious emails like these, do not respond and delete them. Also, find out if your employer wants you to notify the IT department when you receive these types of emails via the company network.
- **Spread the Word.** You will be considered a cyber-savvy individual—and will be appreciated by your employer—if you encourage your colleagues and clients, as applicable, to be web wise. Educate them about the Stop.Think.Connect.™ Campaign's efforts and suggest they get involved by sharing the information offered below.

HOW TO GET INVOLVED

Help the Campaign educate and empower Americans to take steps to protect themselves and their families online. To get involved, become a Friend of the Campaign by visiting www.dhs.gov/stopthinkconnect. Once you are a Friend, there are many ways to stay involved:

- **Blog, tweet or post about Stop.Think.Connect.™** and safe practices when it comes to new technology.
- **Spread the word.** Promote Stop.Think.Connect.™ messages and resources within your offices and social groups.
- **Volunteer within your community** to mentor kids and teens on the basics of online safety.
- **Consider a career in cybersecurity** if you enjoy science, technology, engineering or math.

Learn more about the Stop.Think.Connect.™ Campaign at www.dhs.gov/stopthinkconnect.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.

