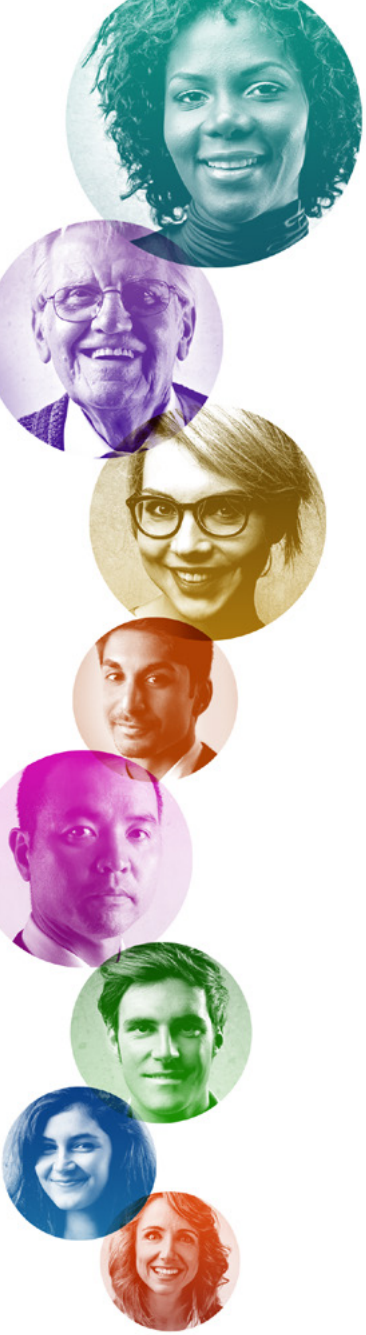


YOUNG PROFESSIONALS TIP CARD

As a young professional, you are more than likely accustomed to using the Internet in your everyday life, but the risks that come with that use could greatly impact you and your career. Making smart online decisions now can help you personally and professionally throughout your life.

DID YOU KNOW?

- **31 percent of all identity theft cases** in 2012 occurred in people ages 20-29.[1]
- Only **18 percent** of young adults claim they are **comfortable with what their friends post about them online**, and 32 percent say that the information about them online is what they choose for the public to see.[2]
- **40 percent** of companies have a **social media policy in the workplace**.[3]

SIMPLE TIPS

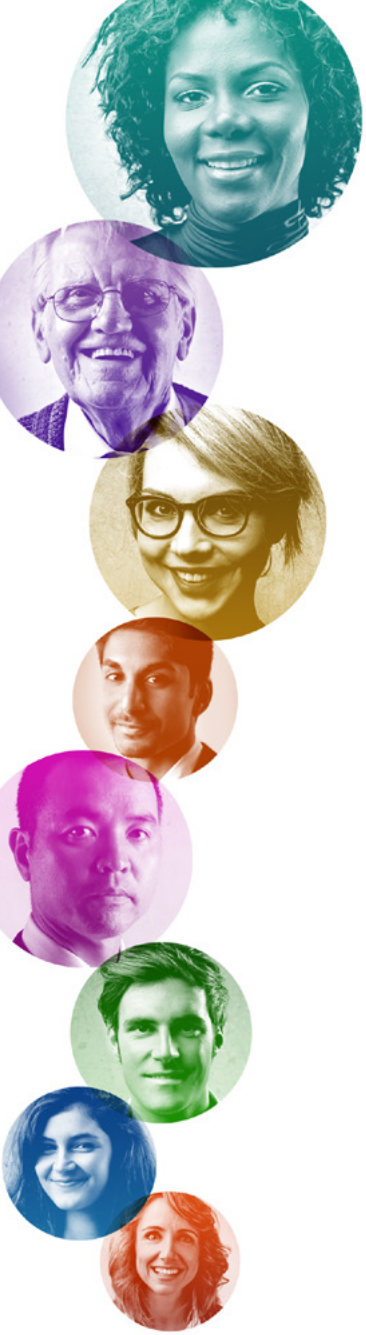
1. Trust your feelings. If something doesn't feel right when you are online, stop what you're doing. If an email or website seems suspicious, report the problem to the system administrator.
2. Think before you click. Don't open emails or download attachments from strangers.
3. Keep your personal information private. Avoid sharing your name, address, telephone number, and other personal information when using the Internet.
4. Remember to protect your cell phone and tablet. Use a PIN or password to lock the devices. The same tips for being safer online apply when you access the Internet from any device.
5. Make sure your profile picture is professional. This is public regardless of your privacy settings. When someone searches you on Google, they will see your profile picture.
6. Consider your pages for websites like Facebook, Twitter, and LinkedIn your live resume. Always remember that even if you delete things, it is likely not gone forever. Google, Facebook and other companies keep a digital footprint of everything. This could in turn be a post or picture that a future employer may see.
7. Although it's great to network with others, be careful who you befriend. Simply because someone with mutual friends wants to add you on a website or app does not mean they are trustworthy. Only add people you personally know and have met before on your personal pages. Think about the information you share online about yourself or your family and if you really want a person you don't know well seeing that information too.

---

[1] Federal Trade Commission, 2012

[2] Pew Research Center, "Teens, Social Media, and Privacy." May 2013

[3] Society for Human Resource Management, December 2012



8. Avoid oversharing online or in person. As a young professional, it may be very exciting to share what you do at work with others. Remember your organization's security standards and be careful what you say, especially in public settings. You never know who may be overhearing your conversations. Also put away your work identification or badge when out in public and when using public transportation.

RESOURCES AVAILABLE TO YOU

US-CERT.gov

US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit www.us-cert.gov/cas/tips for more information.

Justice.gov

The Department of Justice Computer Crime and Intellectual Property Section tells you where to report hacking, password trafficking, spam, child exploitation, and other Internet harassment. Visit www.justice.gov/criminal/cybercrime/reporting for more information.

OnGuardOnline.gov

This website, run by the Federal Trade Commission (FTC), is a one-stop shop for online safety resources available to individuals of all ages.

StaySafeOnline.org

The National Cyber Security Alliance offers instruction on security updates, free antivirus software, malware software removal, and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If you think a site has collected your personal information in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
- If someone has had inappropriate contact with you, report it to www.cybertipline.com and they will coordinate with the Federal Bureau of Investigation and local authorities.
- If you receive an online solicitation, make a report at www.cybertipline.com or call 1-800-843-5678.
- If you are the victim of online fraud, report it to the Department of Justice at www.justice.gov/criminal/cybercrime/reporting.

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.