Who Is Watching You?: How to Protect Yourself Online

Learning Objectives:

1. To understand how online privacy is essential to keeping yourself, reputation and personal information safe and secure.
2. To articulate the connection between how an individual member utilizes the Internet and the reputation of Zeta Tau Alpha.
3. To utilize strategies to improve online privacy and security.

Technical Requirements:

Laptop and projector *if* you would like to show the video at the beginning of the workshop
Flip chart and markers

Time Needed:

20 minutes

Group Size:

Entire chapter

Physical Setting:

Any facility where the group can sit comfortably, facing the facilitator

Preparation:

Watch the Online Privacy video sent by Zeta Tau Alpha via e-mail (can also be found on the ZTA website, Facebook page and YouTube channel). Read the two articles about Online Privacy in the Winter edition of *Themis* magazine (2011). You can find these online at zetataualpha.org > Students > Programming > Multimedia.

Resources:

Andrews, Erin (2011, Winter). Guard Your Privacy in Age of Social Media. *Themis,* 2.
Martin, Ashley (2011, Winter). Who's Watching You?: How to Protect Yourself Online. *Themis,* 8-11.

INTRODUCTION (1 minute)

The facilitator should introduce himself/herself and the program topic. Ask for the audience's attention and interaction during the discussion.

In just a few short years, social media has turned into one of the most popular forms of communication. Facebook has over 500,000 million users who spend more than 7 billion minutes on the site each month. The average user posts around three things a day on Facebook.

Add any information about how your chapter uses social networking tools for communication and more, as well as how prevalent use is in your chapter/at your college.

The Internet has become the place where we socialize, catch up and even get our news. Yet, controlling the information you supply on the web, especially on social networking sites, is key to keeping yourself, reputation and personal information safe and secure. What you post online can affect your safety, as well as your future career.

ZTA recently sent a short video to you via e-mail about online privacy. So let's spend a few minutes following up on that important topic and how it relates to you as an individual and to Zeta Tau Alpha.

If you have the ability to play the ZTA Online Privacy video (through the link sent via e-mail or from the ZTA website, Facebook page or YouTube channel) do so at this time.

DISCUSSION ABOUT ONLINE PRIVACY (15 minute)

What do you think are some of the dangers that can be encountered from not guarding your online privacy?

Allow time for the group to answer. Some points that should arise include: identity theft; employers, university administrators, and others seeing things that are personal to you; predators seeking new victims; obtaining computer viruses; etc.

Always remember the more open you are online, the more risk you have.

To reduce your risks, what information should you steer clear of posting online?

Allow time for the group to answer. Some points that should arise include:
* *Private information, unflattering photos, overly personal statuses, etc.*
* *Contact information: Address, phone number, e-mail address, birth date, <u>location</u>, etc.*
    * This might sound scary, but it's a real danger. When someone has your current location because you post it through programs like Facebook Places application or foursquare, they know where you are and can find you. They also know where you are <u>not,</u> leaving your home open to threat. There have been news reports across the country of people using this information to break in to homes or even to stalk individuals.

Once information is on the Internet, it's out there for public consumption and is even be searchable from sites like Google. When you post something, think about whether or not you are prepared for others to see it. It's common practice for employers and recruiters to search Facebook and others sites for information about a job candidate. A good rule of thumb is to "only post things that you would be happy for your family or a future employer to view."

What are some other strategies to protect yourself online?

Allow time for the group to answer. On the next page is a list of tips from the referenced Themis *article.*

Review all 10 with chapter. We suggest you even put them on a flip chart for the group to see.

Strategies for Online Privacy
- Check and adjust social media privacy settings often to control who sees specific information about you. *Note that sites update setting options regularly, so you need to check them often.*
- Only "friend" people you know. *This is important because your friends could be sharing your information depending on their privacy settings.*
- Only post/provide information and items that contribute to a positive reputation of yourself.
- Never reveal personal information, especially your address, phone number and current location.
- Understand online application settings (through Facebook, Twitter, websites, etc.). *These often provide outside sources information about you and your preferences.*
- Use an Internet browser to search for your own profile so you can see what is searchable by others.
- Keep your computer programs and software up-to-date, including Internet browsers and anti-virus software. *These programs can block unwanted files and viruses.*
- Clear your cache and cookies in your Internet browser regularly. *Each time you visit a website, it leaves temporary info called cache and cookies in your browser.*
- Only provide personal information *(like address, date of birth, banking info)* to secure sites *(look for the lock icon on the page).*
- Use public Wi-Fi and computers with caution. *Always be sure to log out of sites, like email or social networking sites, when on these networks.*

What does the information you currently have posted online or on social media sites portray about you?

Allow time for the group to answer after each of the following questions.

How would others in the campus community view you if they accessed your profile?

How would future employers view you if they accessed your profile?

How does the information you have posted on your profile represent Zeta Tau Alpha?

What have you seen posted online that might harm ZTA's reputation?

One of the most important things you can do to protect yourself online is to make sure the information you share about yourself (and others share about you) portrays a positive image. These posts create a picture of who you are and how you want to be seen. Additionally, because people know you are a Zeta, and you likely show that you are a Zeta through your online presence, our chapter and organization are also connected to how you portray yourself.

Who has responsibility to address a sister who has posted something that could negatively affect her or our organization?

Allow time for the group to answer. If your chapter has an officer or strategies that help monitor online/ Facebook presence, make sure those are mentioned.

Additionally, the conclusion that we are hoping arises is that it is everyone's responsibility to help each other and Zeta Tau Alpha by confronting negative, potentially dangerous or detrimental online behavior. You might have to push this point with the group.

CONCLUSION (4 minutes)

As we close, let's take a minute to review Zeta Tau Alpha's policy about Internet usage.

Review the information in the box below.

If you haven't already watched the Online Privacy video ZTA sent, check your e-mail or look on the ZTA Facebook page or YouTube Channel. There are also articles in this issue of *Themis* (available on the ZTA website) about online privacy, including one from Zeta alumna and sportscaster Erin Andrews, who has taken a public stance on protecting privacy after she was stalked in 2009, and her stalker posted videos of her online.
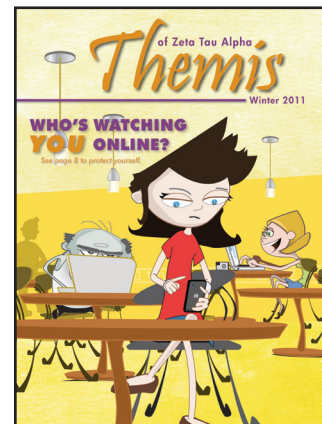
In conclusion, think carefully about your online actions — from what photos you post on Facebook to updating foursquare about where you're eating dinner, from buying items online to your use of public computers in the campus library. And remember, **the more open you are, the more risk you have.**

Internet and Electronic Mail Service Policy:

Any individual or entity who creates or maintains a Zeta Tau Alpha website on behalf of a colony, chapter or an individual member, and any individual or entity using the Zeta Tau Alpha name or letters in Internet communications (such as e-mail accounts, mailing lists, bulletins, social networking sites, co-sharing sites, chat rooms, discussion groups, etc) shall comply with the following terms and conditions. Zeta Tau Alpha Fraternity reserves the right to (although it shall be under no obligation to) remove links or access to sites that do not comply with these policies.

1. All websites and internet communication (services) shall comply with any and all appropriate federal, state and local laws; college and university rules and regulations; National Panhellenic Conference rules and regulations; and the *Constitution and Bylaws of Zeta Tau Alpha* and policies.
2. Services shall not be used in a way that defames, abuses, harasses or threatens other individuals.
3. Services shall not contain material that is obscene, pornographic or otherwise offensive to a person of ordinary sensibilities.
4. All services shall promote a positive image of college students, alumnae, the college/university and ZTA.
5. No services shall include links to personal/commercial sites that are inconsistent with the values and standards of Zeta Tau Alpha.
6. Services shall not include product endorsements or other personal/commercial advertising unless approved in writing by the National President.
7. Services shall not include any copyrighted material from other sources or trademarks owned by third parties without the express written consent of the copyright or trademark owner.
8. Services shall include no references to alcohol, illegal drugs or hazing with the exception of educational material about these issues.
9. Responsible use of the Internet is incumbent upon every member of the Fraternity. Inappropriate use of language or the sharing of sensitive Fraternity information (such as Rituals or information revealed to members through Rituals) on a chapter website, the National Fraternity website or other Internet avenue is strictly forbidden.
10. All services shall be in good taste and conform to all Zeta Tau Alpha policies.
11. All information provided on chapter and colony websites shall be kept as up to date as possible. If possible, each website shall provide the ZTA e-mail address (zetataualpha@zetataualpha.org)
12. For safety and public concerns, members should avoid publishing personal information such as addresses, telephone numbers and personal calendars on the websites.