

TIP#1:

Don't Share Any Personal Information in Online Public Spaces!

- Don't give your personal information, such as your age where you live, or where you work, to strangers online, including in e-mail or chart rooms.
- Be careful of e-mails from unfamiliar accounts with friends' names attached, since cybercriminals can use them to phish for your personal info.
- Use a neutral screen name not your real name or a sexy nickname, your birthday or other private information.
- Don't use your birthday or other easy number sequence for your password.



Cyber Stalking Prevention Tips

TIP #2:

Be extremely cautious about meeting online acquaintances in person.

- If you choose to meet, do so in a public place and take a friend along.
- Don't assume the things strangers tell you online about themselves are true
 - Trust your gut (or intuition).

For more TIPS visit: www.utrgv.edu/IS



Cyber Stalking Prevention Tips

TIP#3:

Make sure that your ISP (internet service provider), cell phone service provider, and social sites you frequent have an acceptable privacy policy that prohibitis cyber stalking.

- Use an internet provider that has a privacy policy and a trak reord of responding to privacy concerns and complaints.
- Services such as Facebook change their privacy polices frequently, so check your privacy settings regularly to make sure you're sharing information only with people you trust people you trust.
- Some sites allow you to see how your profile is viewed by others test yours, and make sure you reveal only what is absolutely necessary.
- Information.



Cyber Stalking Prevention Tips

TIP#4:

If you experience contact with someone that is unpleasant or hostile, log off immediately and report the incident to your ISP (Internet Service Prvider).

- Most chat/bulletin boards also have a reporting system for unpleasent encounters.
- If a situatino or incident online makes you fear for your safety, contact a local law enforcement agency.
- If you experience online hostility, log off and surf else where.



Cyber Stalking Prevention Tips

TIP#5:

When you are online, only type things you would actually say to someone face-to-face.

- Think about how your words might be interpreted without the context of body language and voice.
- Do not respond to unwanted messages or engage in personal exchanges with people that you do not know.
- Be extremely cautious of how much information you choose to post and share.
 - The words you type online will leave a digital footprint.





TIP#6:

If you are breaking up with an intimate partner, especially if they are abusive, troubled, angry, or difficult, reset passwords on all of your online accounts.

- This includes e-mail and social networking accounts, credit card accounts, bank accounts, and anything online you do not want former partners to access.
- Change your verification Information (e.g., passwords, pin numbers, and security questions) to something someone cannot guess.
- You may want to get a new cellphone and/or a credit card account that your former partner doesn't know about.
- Figure out what information family and friends are posting about you. Help them learn better privacy practices.





Cyber Stalking Resources

ISO

Information Security Office www.utrgv.edu/IS IS@utrgv.edu (956) 665-7823

Office of Victim Advocacy & Violence Prevention www.utrgv.edu/OVAVP OVAVP@utrgv.edu (956) 665-8287

NATIONAL CENTER FOR VICTIMS OF CRIME Stalking Resource Center www.ncvc.org/src

UTRGV Police
www.utrgv.edu/POLICE
POLICE@utrgv.edu

Edinburg: (956) 665- 7151 Brownsville: (956) 882- 8232

Vaqueros Care

Vaqueros Care Report It Form www.utrgv.edu/reportit

The University of Texas
Rio Grande Valley
Information Security Office

