Did you know?

Online postings leading to eventual in-person meetings have been used to commit violent crimes. **http://craigscrimelist.org**

Tech-savvy criminals can use social media to find out when you are not home. **http://pleaserobme.com/why**

Once you share digital content, you can no longer control it.

Your best way to fight back is to report cyberstalking.

It is a **crime**, and reporting it is easier than you think!

- Print out any harassing emails (with the full header), instant messages, or private messages.
- Save any harassing text messages, voicemails, or phone numbers. Never delete them.
- Keep a log of any unwanted contacts. Write down or bookmark the username and profile URL of anyone who harasses you on a social network.
- File a report with USCPD or your local law enforcement agency.
- Talk to someone about your experience. Cyberstalkers rely on fear, do not let them win.

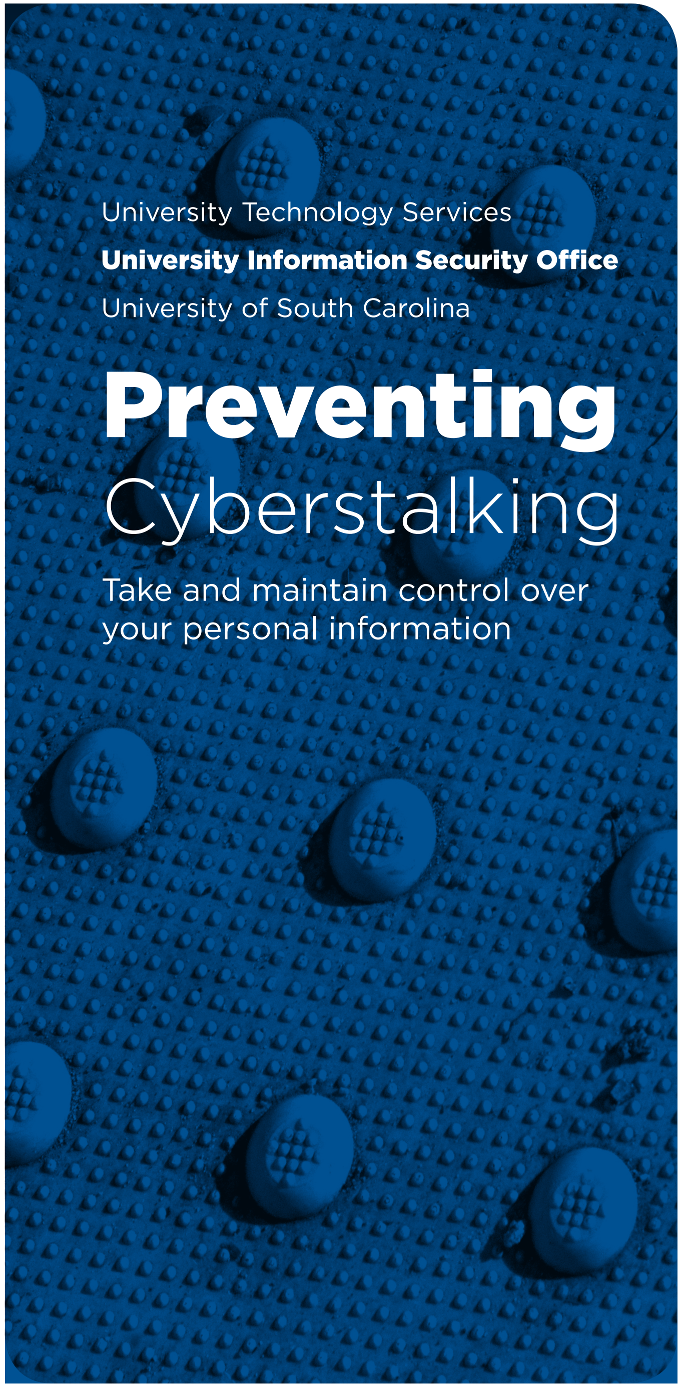
Contact Us

University Information Security Office
1244 Blossom Street
Columbia, SC 29208
803-777-1800
security@sc.edu

www.security.sc.edu

UNIVERSITY OF
SOUTH CAROLINA

The University of South Carolina does not discriminate in educational or employment opportunities or decisions for qualified persons on the basis of race, color, religion, sex, national origin, age, disability, genetics, sexual orientation or veteran status.



University Technology Services

University Information Security Office

University of South Carolina

Preventing Cyberstalking

Take and maintain control over your personal information

UNIVERSITY OF
SOUTH CAROLINA

What's so intimidating about a "cyberstalker"?

Everything.

Cyberstalking, at first glance, may seem harmless enough. So someone enjoys thumbing through your Facebook photos, but what's the big deal? Sure, it's creepy. But it's just like someone having a crush on you, right? **Wrong**.

As a society, we share much more information publically than we used to. Sure, a stalker may be able to look through your photos. **They may also be able to look though your friend's photos of you.** According to how you maintain your privacy settings, a stalker could quickly learn way too much about your life.

It may not concern you that they could learn about your favorite TV shows, genre of music, or hobbies. **But, what if they could learn where you are?** Perhaps they know what you're doing, even what you're wearing. The cause for concern is increasing, isn't it?

Nothing is off limits on the Internet, and once you post something...it never really goes away. It's time to reevaluate the way you safeguard your personal information on the web. The more information you provide, the easier a target you become.

It's time to take a stand against cyberstalking.

Social Media and Your Privacy

According to Facebook, around 600,000 suspicious log-ins are stopped each day. Think about that. **That's the number of attempts they successfully stop.** Imagine how many they fail to notice! Most of the time, compromised Facebook accounts are used to spread those irritating SPAM messages we all occasionally see. But, what if there were other intentions? It could be a hacker looking for your personal information, a potential stalker trying to find out where you like to go each Tuesday night, or a jealous ex trying to smear your reputation.

Snapchat started 2014 off with a bang, having over 4.6 million users' information leaked. **Usernames and phone numbers** were compromised. Let that sink in. Unsuspecting Snapchat users could be looked up by username, or even telephoned! That sounds like a great way to become a victim of a cyberstalker.

The only way to reduce the threat of having your personal information stolen is to safeguard it and change the way you share it. How much information do you want to give a company? **What are they going to do with it?** Do you really want all of your Tweets or Instagram photos to be open to public viewing?

Remember, once something is online, you can't get it back.

What can you do?

- Enable multi-factor or "login approval" on social sites when it is available to help combat unwanted logins.
- Only accept follows & friend requests from people you know.
- Don't "tag" yourself or others in photos. Ask others to give that same respect to you, or remove their tags.
- Don't post too much information. Your birthday, address, phone number, and email address are private.
- Block users who SPAM or harass you. Print threatening messages to provide as evidence.

Mobile Technology

Use a PIN or password to keep others from using your mobile device. This routine may seem inconvenient, but you'll be glad you enabled it if your device is ever lost, stolen, or picked up by a curious acquaintance.

Use a "remote-wipe" tool to quickly erase your photos and data from a lost or stolen device.

Be mindful of "location tracking." If this feature is enabled, you could be providing a real-time map of your location and daily routine.

If you think you are a victim of a cyberstalker, don't be afraid. Find comfort from your friends and quickly notify USCPD.