# Tips to protect yourself from Cyberstalkers

## What is cyberstalking?

Cyberstalking's definition is quite simply, “the use of the internet, or other electronic means, to harass and intimidate a selected victim”.

Cyberstalkers have been known to fit GPS devices to their victims' cars, use geolocation spyware on their phones, and obsessively track their victims' whereabouts through social media.

Cyberstalkers might target their victims on social media, trolling and sending threatening messages; they might hack emails, to communicate with the victim’s contacts, including friends and even employers. Social media stalking can include faking photos or sending threatening private messages.

Cyberstalkers will spread malicious rumors and make false accusations, or even create and publish revenge porn. They might also engage in identity theft and create fake social media profiles or blogs about their victim.

# How to avoid being stalked online

One good exercise you should carry out now is to Google yourself and find out just what information a potential Cyberstalkers could find online. You may be shocked by how easy it is to track you down. Not to mention, find your home address, phone number, and other personal details.

And if that's bad, you might want to check how much data someone could compile on you if they had access to your friends' and family's social media, too. For instance, they might find out which bar you were in, with which friends, or where you'll next be going on holiday and when.

You might even find stuff purporting to be from you that someone else has uploaded: a fake blog, or a Craigslist account putting your phone number and home address out there. This is how Cyberstalkers get started - Googling their victims and finding out everything they can.



CS4b

CyberSecurity4biz.com

can your business survive without its data?

# Tips for protecting yourself from Cyberstalkers

## Increase your privacy settings

Take a good look at your social media accounts and if you haven't done already, enable strong privacy settings.

- Make your posts 'friends only' so that only people you know get to see them.
- Don't let social networks post your address or phone number publicly. (You might even want to have a separate email address for social media)
- If you need to share your phone number or other private information with a friend, do so in a private message - not in a public post.
- Use a gender-neutral screen name or pseudonym for your social media accounts — not your real name
- Leave optional fields in social media profiles, like your date of birth, blank.
- Only accept friend requests from people you have actually met in person. Set your social networks to accept friend requests only from friends of friends.
- Disable geolocation settings. You may want to also disable GPS on your phone.

If other personal data is up on the web outside your social media accounts, start removing it. In the case of your SSN being displayed, Google will help you remove that. You may need to contact third party websites to get some of the data taken down.

If you are using an online dating service, don't provide your full ID on the site or over email. Only give out your phone number to someone you've actually met and wouldn't mind seeing again. The best security advice is to not even give your full name online, only your first.

Be cautious of any incoming phone calls or emails which ask you to give personal information, however reasonable the purported request. If a bank or credit card company phones, get off the phone, and use another phone (for instance, if they rang your landline, use your cellphone) to ring back to verify, using the HQ or branch phone number that's on your paperwork — not the one you've just been given. And never, never, never give out your SSN.

# Secure your PC and phone

Securing your data won't help you if your smartphone or PC is hacked. To prevent being stalked online you should build basic security into your online life.

## What is catfishing?

Catfishing is a form of fraud or abuse where someone creates a fake online identity to target a particular victim. Catfishers may lure their victims into providing intimate photos or videos, then blackmail them, or may develop a relationship and then ask for money for a sudden emergency.

Catfishers can be very convincing, but you can discover their scam in several ways.

- If all their online photos are selfies or studio shots, with no other friends, no family, and no context, that's a big clue.
- Do a Google reverse image search against the online photo on a dating site. You may find the person has multiple online profiles with the same photo but different names.
- Ask if you can do a video call on Skype. Guess what? Catfishers will usually make their excuses - and you won't hear from them again.

# What to do if you're cyberstalked

If you're being stalked online don't wait and hope the problem will go away — act immediately.

- Make it clear to the Cyberstalkers that you don't want to be contacted. Put it in writing, and warn them that if they continue, you'll go to the police. Don't engage with them at all once you have issued this warning.
- And if they continue, go to the police. Many police departments have a special cyberstalking team, but they're not going to quibble about a cyberstalking definition. If you've been threatened or you're being harassed and intimidated, then they'll deal with it—whether it's on Facebook, email or through spyware on your phone.
- If you think someone is tracking you through spyware, don't use your own computer or phone to get help - borrow a family or friend's phone.
- Get your computer and phone checked over by a professional for spyware or other signs of compromised accounts.
- Change all your passwords.
- In the case of social media stalking, use your privacy settings to block the person, and then report the abuse to the network. You can easily find out how to report cyberstalking in most social networks' help and support pages.
- If you have been sent abusive or threatening emails, you probably know the stalker's ISP - the bit after the @ in their email address. Contact abuse@domainname or postmaster@domainname. Most ISPs take cyberstalking very seriously. If they're using Gmail, there's a reporting mechanism you can use at https://support.google.com/mail/contact/abuse.
- You can filter abusive emails to a separate folder so that you don't have to read them.
- If you think the Cyberstalkers might harass you in the workplace, tell your employer.

Save copies of any communications involved, including your own, police reports, and emails from the networks. Back up the evidence on a USB stick or external drive.

## Cyberstalking laws

Cyberstalking is subject to general laws on harassment, such as the Violence Against Women Act 1994 in the US.