



Fighting Digital Stalking

with Frank Ahearn of www.FrankAhearn.com

How Modern Technology Has Changed Stalking

"Digital" and "privacy" don't go together!

- Fake digital identities can be created in minutes, and used to stalk someone.
- Harassment, extortion, fraud, theft... all of these are potential "stalking" threats.
- We as users only have so much knowledge of how technology works.
- The digital world can invade your physical world quite easily. We all have 2 identities.

Avoiding Data Security Mistakes

Often, we ignorantly volunteer our private data.

- Telling the truth online poses a HUGE security risk.
- Never be "geographically accurate," which helps stalkers to find you.
- You can use prepaid phones, PO boxes, backup email addresses, etc. to protect yourself when doing business online.
- You must give out some information online; using "fake" information helps limit what real information you give up.
- Take responsibility for your digital security. Do some research to make sure the sites and services you use are legitimate.
- Don't underestimate data thieves. They can be very sophisticated and subtle.
- Privacy is something we make for ourselves.

How To Identify Digital Stalking

If you're looking for warning signs, it's too late.

- Before you deal with someone, interact with them on video to prove they're "real."

- Before you use a website or do business with it, source it out and do a few minutes of homework.
- From this point forward, start doing stuff to protect your privacy.

3 Steps To "Harden Your Digital Presence"

You have to separate who you are online and who you are offline.

- Your online life doesn't have to reflect your offline life.
- Your digital presence is what you choose to let people know about you.
- Have a second mobile number for your Internet life.

Future Digital Stalking Threats

There are 3 big threats on the horizon:

- **Mobile phone apps** that can download your phone number for use in scams and fraud.
- **Reverse photo lookup** is going to become a bigger problem, too. Right now, sites like tineye.com allow you to look up a photo and see where else it appears... which might allow a stalker to locate you based only on your photo, if you've used it elsewhere.
- **Database reports** available to the general public are a big problem. If you give someone your mobile number and they then run it through a database, that information can be used against you.
- Remember, if it's too good to be true, it is... even when it comes to socializing.
- We can trust our gut in personal exchanges. Apply that attitude to the online world.

Prepare. Train. Survive.