THE GEEK PROFESSOR®

How to Destroy Yourself Online

SHARING ONLINE

Data posted online is visible to **everyone**, good or bad and will remain online forever in most cases. Do you really want your future employer, future schools, or future love interests to see what you're posting? Do you really want people *now* to see it?

Be particularly cautious with:

- Private thoughts and feelings
- Controversial political or religious topics
- Personal information (yours or others')
- Travel plans, schedule, etc.
- Hobbies that might help someone guess passwords or use to bully you.
- Information about addictions, medical problems, or other exploitable weaknesses
- Data about your location and valuables you carry or own.

PROTECTING PHOTOS

Before uploading a photo, check to see if:

- At full size, does the photo show keys, fingerprints, documents, embarrassing personal information? Check edges and reflective surfaces too!
- Does the photo contain geo-tag information that would lead a person right to your house or location? Most phones geotag by default, but you can easily check in Windows 7 by right-clicking the file and looking through the photo's properties.

GETTING TRICKED

Never assume what you see is what you get. People really will spend a huge amount of time and effort pretending to be something they're not in order to gain your trust and eventually get what they want. Even people you know personally (and have met in real life) might have lost control of their accounts or lost their computer/phone/etc. Always verify friend requests and any communications that seem "off".

ACCOUNT HIJACKING

To prevent **your** accounts from getting hacked, use good password security:

1. Make good passwords that are different for every site. Write them down if you have to, but you can use "rules" or "tricks" like those described in the seminar for anything but super-important accounts (like your e-mail or any account that is attached to your money).
2. Always use HTTPS security when logging into an account and make sure the "S" is there from login to logout. For Firefox users, a good plugin is HTTPS-Everywhere (available at *eff.org*).

TRUSTING WEBSERVICES

Because businesses have proven they're unable or unwilling to keep your information to themselves, it's best to treat them as any stranger and keep as much to yourself as you can.

Fill in the minimum necessary and evaluate if its necessary to use your real data at all! Have a set of fake data prepared that you can use for things like name, birthdate, answers to challenge questions, etc. In some cases, the best option is to not associate with the company or service at all.

ONLINE ADDICTION

Sadly, addiction is a natural part of the human condition and the Internet is a tempting playground for someone looking for an escape. Look for the signs of a problem and get help if necessary.

1. Set **reasonable** limits – Everyone should be clear as to how many hours a day, how much money, and what priorities must be completed first.

2. Watch for signs of dependence – Are you/they exceeding the agreed-to limits regularly? If the limits are reasonable, but you/they can't keep to them you should re-evaluate the limits or look at admitting there's a problem.

Two things to keep in mind: some people are more prone to addiction than others and it's best to avoid situations that can cause problems. Certain games are reported to be more addictive than others and researching these online before even trying them is a good idea (ex. World of Warcraft and Farmville).

Second, it's very important to set *reasonable* limits. I once talked with a lady who thought her son had a problem because he wouldn't keep to the one hour a day rule she set. One hour isn't enough time for **any** activity let alone gaming. If you're not sure what's fair and what makes sense, ask people who've dealt with this before, but especially people who do the same activity and seem to have it under control.