

OPSEC and Social Networking

The Interagency OPSEC Support Staff



What is a Social Networking Site?

Social Networking Sites (SNS) allow people to collaborate and connect to share information and ideas.



Why use an SNS?

Personally

- Fun, exciting, entertaining, useful for maintaining relationships

Professionally

- Marketing, manage public image, connect with customers, solicit ideas and feedback.

The Danger

Bad guys use it, too:

- Stalkers
- Thieves
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- Etc.



For Example:

From the headlines

“Doh! Senior U.S. politician blunders by blogging about secret trip to Iraq ... while in the country” - Daily Mail Reporter

“Could Twitter robbers get to you?” – NBC

“Twitter gets you fired in 140 characters or less” – MSNBC

“MySpace Evicts 90,000 Sex Offenders” – ABC News

“Pennsylvania Man Charged With Using MySpace Account to Drug, Rape Teen Girl” – Fox News

Terrorists, Too

“Information about government personnel, officers, important personalities, and all matters related to those (resident, work place, times of leaving and returning, wives and children, places visited).”

- the Al Qaeda handbook



Critical Information

- What you want to keep from them
- What they want from you

These are not always the same list. Know your adversary to learn their goals and what's important to them.

Critical Information

Things You Should NOT Share on SNS

- Names and photos of you, your family and co-workers
- Usernames, passwords, network details
- Job title, location, salary, clearances
- Physical security and logistics
- Mission capabilities and limitations
- Schedules and travel itineraries
- Social security number, credit cards, banking information
- Hobbies, likes, dislikes, etc.

“Do’s”

Remember Computer Security

An adversary won't waste time on the “human factor” if they can go after the computer system directly.

- Hacking
- Theft
- Planted code



“Do’s”

Consider All the Players

Before posting data to an SNS, ask:

- Who owns the company?
- Who are their partners?
- Where are they hosted?
- Who has access to the data?

Some might be adversaries or affiliated.

“Do’s”

Modify Your Search Profile

Search profile: the data about you that is visible when someone is searching for “friends”

What might be publicly visible even if your profile isn't:

- Name
- Photo
- List of networks and groups
- List of friends
- Age/ Sex/ Location



“Do’s”

Reasonable Suspicion

Social engineering and “conning” start with becoming a friend.

They:

- Like what you like
- Hate what you hate
- Understand you



Be especially cautious about dating sites

“Do’s”

Verify Supposed “Real” Friends

Old Jimmy Smith from the high school swim team OR adversary?

They can get the data from:

- Yearbooks
- Other SNSs
- Your posts/profile

VERIFY BEFORE ADDING!

“Do’s”

Watch Your Friends

You didn’t post sensitive pictures of you and your kids, but your brother, wife, mother, or friend did.



“Do’s”

Treat Links and Files Carefully

Would you follow a link in e-mail? Would you download and run an attachment? Then why do you do these things on SNSs?



Verify before acting!

“Do’s”

Question the Utility of an SNS


- Do you really have a purpose for using an SNS, or do you use it “just because”
- Are you very careful with the data and understand data aggregation issues?
- Are you willing to find and learn all the security controls and keep up with them as they change?

Do you really need the risk of an SNS?

“Don’ts”

Don’t Discuss work

- Assume the adversary will find you and read what you post.
- Search engines make it easy. Poor security makes it possible.

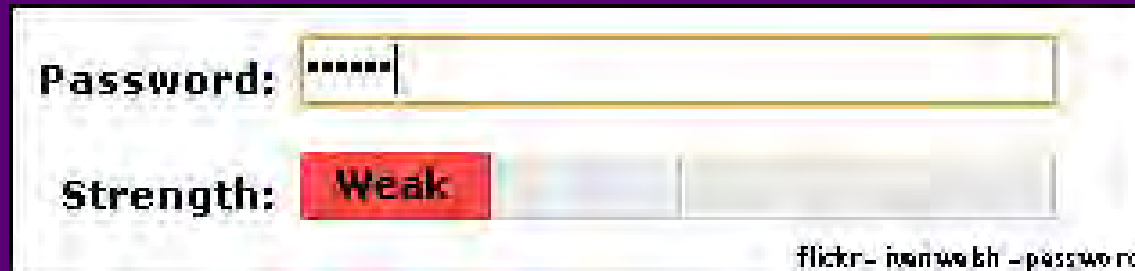
Top 25 Social Networks Re-Rank
(Ranked by Monthly Visits, Jan '09) 

Rank	Site	UV	Monthly Visits	Previous Rank
1	facebook.com	68,557,534	1,191,373,339	2
2	myspace.com	58,555,800	810,153,536	1
3	twitter.com	5,979,052	54,218,731	22
4	fixster.com	7,645,423	53,389,974	16
5	linkedin.com	11,274,160	42,744,438	9
6	tagged.com	4,448,915	39,630,927	10
7	classmates.com	17,296,524	35,219,210	3
8	myyearbook.com	3,312,898	33,121,821	4
9	livejournal.com	4,720,720	25,221,354	6
10	imeem.com	9,047,491	22,993,608	13
11	reunion.com	13,704,990	20,278,100	11
12	ning.com	5,673,549	19,511,682	23
13	blackplanet.com	1,530,329	10,173,342	7
14	bebo.com	2,997,929	9,849,137	5
15	hi5.com	2,398,323	9,416,265	8
16	yuku.com	1,317,551	9,358,966	21
17	cafemom.com	1,647,336	8,586,261	19
18	friendster.com	1,568,439	7,279,050	14
19	xanga.com	1,831,376	7,009,577	20
20	360.yahoo.com	1,499,057	5,199,702	12
21	orkut.com	494,464	5,081,235	15
22	urbanchat.com	329,041	2,961,250	24
23	fubar.com	452,090	2,170,315	17
24	asiantown.net	81,245	1,118,245	25
25	tickle.com	96,155	109,492	18

“Don’ts”

Don’t Use the Same Passwords

- To use only one password for everything is to hand your life to the first bad guy that works at any webservice you register with.



“Don’ts”

Don’t Give Away Passwords

Then Schmidt came to a page saying that "we'll find your friends and family who are already members and also automatically invite any nonmembers to join (it's free!)."
It instructed her to enter the password for her Yahoo e-mail account.

"I thought I was just signing up to read my friend's message," Schmidt said. "At no time did I think I was authorizing them to access my online address book."

*David Lazerus
Los Angeles Times
April 16, 2008*

“Don’ts”

Don’t Give Away Passwords



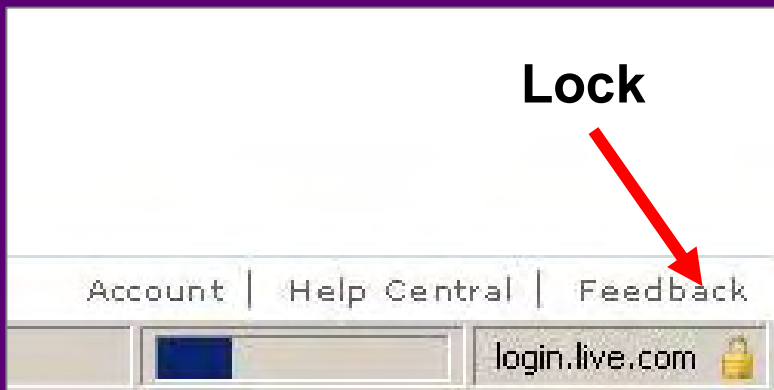
Never give away a password to any account to anyone **EVER!!!**

This should be a life rule, for everything you do, not just SNS.

“Don’ts”

Don’t Use Unsecured Logon at Public Hotspots

Most SNSs do NOT have a secure login capability. Remember that when using them



“Don’ts”

Don’t Depend on the SNS for Security

But it’s private ... right?

- Hackers
- Incorrect or incomplete settings
- Sharing data with “partners”
- Sale of data during bankruptcy



“Don’ts”

Don’t Trust Add-Ons

- Plugins, Games, Applications –
 - written by Who Knows
 - and does Who Knows What.

The SNS didn’t make the application, someone else did. Do you know who? What their motives are? What they put in the code?

“Don’ts”

Don’t Be Too Generous with Permissions

- Create groups (such as “poker club”, “co-workers”, “family”) -- organize friends based on the access you want them to have.
 - Set permissions for:
 - Your status, photos, postings etc

“Don’ts”

Don’t Post Personal Information

Real friends already know your home address, phone number, etc. Don’t broadcast that to strangers.



“Don’ts”

Don’t Post What the Public Can’t Know

No matter what, things you post might spread. If you’re not comfortable with it being public knowledge, don’t post it.



“Life’s tough. It’s even tougher if you’re stupid.”

- John Wayne

