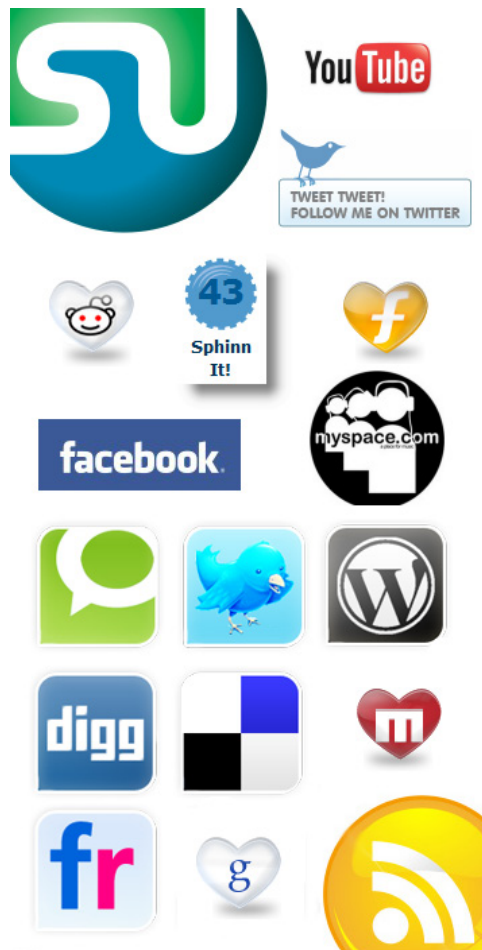


Tips for using social media safely

Facebook, MySpace, Twitter and all the rest are great. Take a look at these top tips to avoid opening the door on data loss, identity theft and malware infection.

1. Know the rules - Make sure you know what policies are in place for using the social networking site.
2. Use secure passwords - What's behind a password? Your life! If it's cracked, your life's for sale. Make it really secure - use at least 8 characters and mix in upper and lower case, numbers and symbols.
3. Check default settings - Social media sites have large numbers of connected users. Make sure you check each site's default settings so your details aren't on public display and minimise the amount of personal information you provide.
4. Be picture prudent - Be careful what pictures you show and try to avoid adding compromising or embarrassing images that might harm you, your friends or your family.
5. Beware of Big Brother - Using social media sites as a diary is OK if you want family, friends (and enemies), your boss and anyone else to know everything about you.
6. Secure your computers - Stay out of harm's way - only use computers with up-to-date security software and effective firewalls.
7. Think before you click - Never click on links just because you know the sender - some malware takes control of a user's account and then automatically sends infected messages to all the user's contacts in an attempt to infect them. If the email looks dodgy it probably is.
8. Stranger danger - Be wary of spammers trying to



get your details by sending unsolicited invitations. If you don't know the person, the best thing to do is to ignore the request.

Passwords

Let's face it - everyone has problems with creating and remembering secure passwords. That's why we decided to help.

Tips on how to create and remember your passwords:
Use the first letters of a sentence that you will remember,

"I have 3 cats: Fluffy, Furry and Shaggy" gives: lh3c:FF&S, or "Bouncing tigers have every right to ice-cream" becomes: Bther2I-C.

Take the name of the website and then add your personal twist, like your height or your friend's home address (e.g. "AmazonOceanRd6'2"). Avoid using your own contact details like your phone number or house number.

Remove the vowels from a word or phrase e.g. "I like eating pancakes" becomes: llktnngpncks".

Use a phrase from your favourite book and then add the page, paragraph or chapter number.

The Do's/Don'ts of creating passwords

Do:

1. Mix letters, numbers and symbols, and use case sensitivity (upper and lower case letters)
2. The longer the better. Use passwords that are longer than 6 characters.
3. Change your passwords at least every 60 days, cycling the numeric values up or down makes the new password easy to remember.
4. Try copying and pasting at least some of the characters in your password that way keyloggers

won't be able to track your keystrokes.

Don't:

1. Don't use words or phrases or numbers that have personal significance. It is very easy for someone to guess or identify your personal details like date of birth.
2. Avoid writing your password down, use a reputable password manager to manage all your passwords.
3. Don't use the same password for several logins, especially if they involve sensitive financial or other personal information.
4. Don't tell anybody your password.
5. When registering on websites that ask for your email address, never use the same password as your email account.

There's No Such Thing As 'Cyber'

How can you tell the difference between a real report about online vulnerabilities and someone who is trying to scare you about the security of the internet because they have an agenda, such as landing lucrative, secret contracts from the government?

Here's a simple test: Count the number of times they use the adjective "cyber." Nobody uses the word "cyber" anymore, except people trying to scare you and trying to make the internet seem scary or foreign. (Think, for instance, of the term "cyberbullying," which is somehow much more crazy and new and in need of legislation than "online bullying.")

When was the last time you said, "I saw this really cool video in cyberspace" or "My cyber connection is really slow today"? Of course, no one speaks like that anymore. The internet is no longer distant or foreign (though it thankfully remains beautifully weird). It's familiar and daily. It's the internet. It's so ordinary, Wired.com stopped capitalizing it more than five years ago.

Need an adjective to describe something that is internet-based? Try "online."

But when it comes to scaring senators, presidents and the nation's citizens into believing

the Chinese, the Russians or Al Qaeda are stealing all our secrets or bringing down the power grid, the internet somehow morphs back into "cyberspace."

Here's a good example of the "cyber" test from a pretty interesting story from The Washington Post about the National Security Agency disabling (rather ineptly, it seems) an online forum used by radical Islamic fundamentalists to plan terrorist attacks.

The Post uses the adjective 12 times in describing how the NSA and CIA bickered over whether NSA "cyber-warriors" should use hacking techniques to take down a message board that suspected Al Qaeda were using to make plans. In a brilliant stroke of "cyberwar," the NSA "cyber-operators" took down the CIA-sponsored honeypot message board where extremists were being monitored, somehow inflicting collateral damage on some 300 innocent servers in the process.

Forbes got into the "cyber" action this week as well. Amit Yoran, a respected security expert who runs a company that sells computer security services to the government, wrote a long post on a Forbes blog this week to defend the concept of "cyberwar," in no small part because this blog ranted about how that term is used to hype militarization of the internet and feed a new and very dangerous arms race.

Yoran says the debate doesn't matter (even as he falls firmly in the cyberwar camp), but what's important is that everyone recognize that the dangers of underestimating online risks is worse than "the impact of misrepresenting or miscalculating risk [...] in the sub-prime market," which led to "cascading global financial meltdown." Gulp.

That sounds scary. Bad firewalls will lead to something worse than a global financial meltdown? (That sounds suspiciously like what Michael McConnell told President Bush to scare him into creating a secret government "cybersecurity" plan.)

Those looking for a reality check might check how many times Yoran uses "cyber" in the body of his piece?

The answer: 42. (Yes, we think that's funny, too.)

Yoran and Forbes also fail to mention that his company, NetWitness, markets computer security equipment to the government and has a vested interest in the outcome of this debate.

