Six in ten Americans are wireless Internet users:

- sharp increase from a similar survey last year (51%)
July Pew Study: Wireless

- 76% use wireless devices to take photos
- 54% use phones to send photos or videos to others
- 38% use a Web browser on their mobile
- 34% use their mobile devices to send or receive email
- Only 23% use their devices to tap into social networks
• QUESTIONS
What Kids Search For When They Search the Web

Also Michael Jackson, Fred (Fred Figglehorn is a fictional character whose YouTube channel has become a hit among kids.) & eBay

Top Ten Youth Searches: Symantec Study August 2009

<table>
<thead>
<tr>
<th>Teen (13-18)</th>
<th>Tween (8-12)</th>
<th>7 &amp; Under</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youtube</td>
<td>Youtube</td>
<td>Youtube</td>
</tr>
<tr>
<td>Facebook</td>
<td>Google</td>
<td>Google</td>
</tr>
<tr>
<td>Google</td>
<td>Facebook</td>
<td>Facebook</td>
</tr>
<tr>
<td>Sex</td>
<td>Sex</td>
<td>Porn</td>
</tr>
<tr>
<td>MySpace</td>
<td>Club Penguin</td>
<td>Club Penguin</td>
</tr>
<tr>
<td>Porn</td>
<td>Youtube.com</td>
<td>Yahoo</td>
</tr>
<tr>
<td>Yahoo</td>
<td>You Tube</td>
<td>Webkinz</td>
</tr>
<tr>
<td>Youtube.com</td>
<td>Miniclip</td>
<td>You Tube</td>
</tr>
<tr>
<td>eBay</td>
<td>Yahoo</td>
<td>Games</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>eBay</td>
<td>Miniclip</td>
</tr>
</tbody>
</table>
Symantec Study August 2009

- Average number of threats per site on the Dirtiest Web Sites list is roughly 18,000, compared to 23 threats per site for all sites rated by Norton Safe Web.

- 40 of the Top 100 Dirtiest Web Sites have more than 20,000 threats per site.

- Viruses are the most common threat represented on the Dirtiest list, followed by Security Risks and Browser Exploits.
OSTWG established to review and evaluate:

- The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;

- The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;

- The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and

- The development of technologies to help parents shield their children from inappropriate material on the Internet.
GENERAL CONCLUSIONS & RECOMMENDATIONS REGARDING PARENTAL CONTROL TECHNOLOGIES

- **No single “silver-bullet” solution or technological “quick-fix”**
- **Empower** parents and guardians with diverse array of tools
- **“Layered” approach** to online safety that views them as one of many strategies or solutions
- Technical solutions can **supplement**, but can never supplant, the educational and mentoring role.
- Products and services need to be designed with **the families’ needs in mind**—easy to use, accessible, flexible, and comprehensible for the typical parent. They need to provide different features for the varying needs of all the children in the household.

- Government should **avoid inflexible, top-down technological mandates**. Instead, policymakers should focus on encouraging collaborative, multifaceted, multi-stakeholder initiatives and approaches to enhance online safety.

- **Engage our youth** in constant dialogue and always be willing to talk to them about difficult issues, challenges, or content they face online.
Trends

Ethics

Safety

Security
Trends

- In-house curriculum
- Health/student services
- Internet safety providers-including security
- Industry/government crossing over into safety
- Research based---program evaluation
- Positive messaging
Positive Messaging

- Manage a positive personal reputation
- Protect the privacy of others
- Value relationships with others
- Respect the ownership of intellectual property
- Manage personal safety
- Protect the technology used at school
Topics of Interest

Safety
- Cyberbullying
- Sexting

Ethics
- ORM
- Plagiarism
  - See Digital Literacy Tour

Security
- Identity Theft
- Malware
- Passwords
- Backing up Files
- WebCams
- Phishing/pharming
How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging

- 4% of cell-owning teens (12-17) say they have sent sexually suggestive nude or nearly nude images of themselves to someone else via text messaging.

- 15% of cell-owning teens (12-17) say they have received.

- Older teens are much more likely to send and receive these images; 8% of 17-year-olds with cell phones have sent a sexually provocative image by text and 30% have received a nude or nearly nude image on their phone.
The teens who pay their own phone bills are more likely to send “sexts”: 17% of teens who pay for all of the costs associated with their cell phones send sexually suggestive images via text; just 3% of teens who do not pay for, or only pay for a portion of the cost of the cell phone send these images.

Focus groups revealed three main scenarios for sexting:

1) exchange of images solely between two romantic partners

2) exchanges between partners that are shared with others outside the relationship and

3) exchanges between people who are not yet in a relationship, but where at least one person hopes to be.
Resources

- National Center for Prosecution of Child Abuse
  (http://www.ndaa.org/apri/programs/ncpca/ncpca_home.html)

- National District Attorneys Association

- ‘Photograph’ a film about ’sexting’ and cyber bullying (http://www.cybersafekids.com.au/)
Cyberbullying
Victims 3x’s more likely to show signs of depression

14% (7-10) are harassed through text messaging

(Cyber Psychology and Behavior 2(7) )
Cyberbullying

- < 10% reported experiencing cyberbullying in the previous 30 days
- ~8% admitted to cyberbullying others in the previous 30 days
- ~ 5% were both cyberbullied and the cyberbully in the previous 30 days

As expected, these figures increase significantly when looking at lifetime experiences.

Classroom-based survey - random sample of ~2,000 middle-school students from a large school district in the United States whether or not they had experienced cyberbullying. Cyberbullying Research Center
Broad Generalizations about Cyberbullying

The percent of youth who admit to cyberbullying others at some point in their lives range from about **11% to as high as 20%**.

**Adolescent girls** are just as likely, if not more likely than boys to experience cyberbullying (as a victim and offender) (Kowalski et al., 2008; Hinduja & Patchin, 2009)

Cyberbullying is related to low self-esteem, suicidal ideation, anger, frustration, and a variety of other emotional and psychological problems (Hinduja & Patchin, forthcoming; Patchin & Hinduja, 2006; Patchin & Hinduja, in review)

Cyberbullying is related to other issues in the ‘real world’ including school problems, antisocial behavior, substance use, and delinquency (Hinduja & Patchin, 2007; Hinduja & Patchin, 2008)

**Traditional bullying** is still more common than cyberbullying (Lenhart, 2007; Smith et al., 2008)

Traditional bullying and cyberbullying are closely related: those who are bullied at school are bullied online and those who bully at school bully online (Hinduja & Patchin, 2009; Ybarra, Diener-West, & Leaf, 2007)

Hinduja & Patchin, 2010
Resources

- Olweus Bullying Prevention Program
- Cyberbullying Research Center
- Stop Cyberbullying Now
  (http://stopbullyingnow.hrsa.gov/adults/default.aspx)
  - HRSA Human Resources and Services Administration
- The Kind Campaign
  (http://www.kindcampaign.com/)
Proactive

Positive behavior

Proactively monitor
- ask to see websites and accounts
- search child’s real name, nickname, screen name, friends name, school, clubs etc.
- Check cell phone logs, stored pictures

Block it
- Use block settings

Document it
- List web addresses-emails and dates
- Screen shots

Report it
- Local law enforcement
- CyberTipLine
- ISP of bully /cell phone provider
  - abuse@yahoo.com
  - abuse@youtube.com
Online Reputation Management

How to protect, manage & promote your online reputation
Online Reputation Management: Another Dimension to Digital Literacy?

Today most individuals’ lives are being crafted, digitalized, collected, recorded, archived and are searchable

Digital Mining is IN!
Digital Dossier

KnowWhereTheyGo.org
Online Reputation Management and Monitoring (ORM)

Online Reputation Management, or ORM, is the practice of consistent research and analysis of one’s personal or professional, business or industry reputation as represented by the content across all types of online media. It is also sometimes referred to as Online Reputation Monitoring, maintaining the same acronyms.

What is ORM?

ORM is a relatively new industry but has been brought to the forefront of professionals’ consciousness due to the overwhelming and many times unpredictable nature of both professional, journalistic content and amateur user-generated content (UGC), the latter of which there is far more, and not the least because of the wide number websites that offer such an opportunity to visitors. Typically, with very low barriers to entry—often just by creating a screenname, registering one’s birthday and a geographical location, and providing a valid email address to complete the account-creation process. Thus, the type of online content monitored in ORM spans professional, journalism sponsored by traditional news and media giants as well as user-created and user-generated blogs, ratings, reviews, and comments, and all manner of specialized websites about any particular subject, be it a person, group, company, business, product, event, concept, or trend.

ORM partly formed from a need to manage consumer generated media (CGM).

As CGM grow with the rise of social media and other similar user-based online content aggregators, it began to effect search results more and more, bringing with it increased attention to the matter of managing these results.

EBay was one of the first web companies to harness the power of CGM feedback. By using user generated feedback ratings buyers and sellers were given reputations that helped other users make purchasing and selling decisions. ReputationCalendar was one of the first companies that offered proactive manage online reputation. ClaimID is another company that early on provided online services designed to promote personal ORM.

The UK market for ORM will grow by around 30% in 2006, to an estimated value of £360 million.

What types of online media are monitored with ORM?

Specifically, the online media that is monitored in ORM is:

- Traditional/mainstream websites
- Social networks (e.g. Facebook, MySpace, Bebo)
- Social news/bookmarking sites
- Forums/discussion boards
- User-generated content (UGC)/Consumer Generated Media (CGM)
- Blogs
JULIA T. SUSMAN
President and Chief Executive Officer

Ms. Susman is a nationally recognized expert in government procurement and related areas in the fields of health care and information technology. As a senior business executive and savvy Washington insider, she provides clients with high-level consultation and advice on how to penetrate and succeed in federal and state markets.

Her specific areas of expertise are:
- Strategic and business planning
- Business development
- Market positioning and benchmarking
- Proposal management
- Federal health care and IT programs
- Congressional advocacy related to business capture and funding
- Decision and change management

For over 20 years, Ms. Susman has helped senior executives throughout industry work successfully within the federal procurement environment. In 1989, Ms. Susman created a unique Washington business consulting practice that marries knowledge of specific markets (Health and IT), specific understanding of procurement rules and how to bid and win government contracts, with her deep understanding of how Washington works. She knows how to impact decisions within agencies and on Capitol Hill to help achieve our clients' business goals. During the past few years, Ms. Susman has expanded this practice to help our clients understand and capture state business. She has applied the same distinct approach to state business consulting projects that has been so successful in her federal consulting practice.

Ms. Susman advises government officials on how to align policy and program operations with acquisition reform and the shift to performance-based contracting. Ms. Susman developed and taught both government and industry comprehensive health care training courses that addressed all aspects of federal contracting.

Brief Summary of Experience

Ms. Susman is the President and CEO and majority shareholder of Jefferson Consulting Group, LLC, a small, woman-owned Washington, DC-based business consulting, lobbying and government contracting. From 1993 to 1996, she was a senior executive, shareholder and a member of the Board of Directors of The Jefferson Group, the predecessor company to Jefferson Consulting Group.

Prior to joining The Jefferson Group, Ms. Susman managed the Washington operations of McDonnell Douglas' Health Information Systems Company. She was responsible for strategic planning, federal marketing, business development, congressional advocacy, proposal development and contract negotiations. Previously she served as Deputy Staff Director, Legislative Director and Deputy Chief Counsel to The U.S. Senate Veterans' Affairs Committee.

Ms. Susman also serves as Chair of the Health Affairs Committee of the National Defense Industrial Association (NDIA) and as a member of the Board of Directors of the Professional Services Council (PSC).
Personal Blogs

Our Version of Normal

sunday, august 31, 2008

Luppie Expecting a Baby Ticker

ADD & frustrated with school
HELP!! My oldest has the diagnosis of ADHD-Inattention. He is not hyperactive, but struggles greatly with the inattention side of it. He loses homework (in his locker, in his back pack, in folders and even possibly a black hole). He doesn't
MySpace Pages
Help Lists

new orleans craigslist > lost & found

search for: [ ] in [ ] lost & found [ ] Search [ ] only search titles [ ] has image

[ Mon, 26 Jan 20:25:29 ]

Mon Jan 26

missing - pic
LOST WALLET!!! REWARD IF FOUND!!! - (New Orleans)
Y files: Y files is still Missing - (Gretna) pic
Beagle - Jimmy Williams on - (St. Bernard Parish) pic
LOST TIGER CAT - (uptown/ulman) pic
Lost Female Cat - (Harvey-Burkley Estates) pic
Lost Male Cat - (Harvey-Burkley Estates) pic
I posted about the Buffy orange tabby - (Prytania/Tenato)

Sun Jan 25

CASH REWARD!!! CASH REWARD!!! - (New Orleans)
LOST DOG - (Audubon) pic
Lost bike lock in washenton park -
Found: Black Pomeranian - (Algiers Point)
Lost Sony Camera - (St Charles Ave)

Sat Jan 24

Found Almost a Year ago, Black/brownish persian cat - (Metairie Near Bucktown)
Puppy Cam
Google Hacking
YouTube
In the News…

Monster.com Hit With Possible Monster-Sized Data Breach

The company declined to cite the number of affected accounts, raising the possibility that every Monster user could be affected.

By Thomas Claburn
InformationWeek
January 30, 2006 07:25 AM

In addition to having lost their jobs, Monster.com job seekers may have lost some of their personal information to cyberthieves.

Monster reported Friday that criminals had breached its database and stolen contact and account data, including user IDs, passwords, e-mail addresses, names, phone numbers, and demographic data. This last category includes data of birth, gender, ethnicity, and in some cases, the state where the person resides.

A similar warning was posted on USAJobs.gov, a federal jobs Web site that depends on Monster as a technology provider.

A spokesperson for Monster declined to cite the number of affected accounts, raising the possibility that every Monster user could be affected. She said the number of users of the site is proprietary business information, as if revealing the breach total would reveal the total number of site users.

The possibility that most of site's users could be affected is consistent with the company's decision to notify users of the breach via a posting on its Web site rather than an e-mail message. "We thought it was prudent to notify them all," the spokesperson said, adding that certain job seekers outside the United States, such as those using the international version of Monster, were affected by the breach.
Few Secrets
Who’s Online?

75% of adults in the U.S. use the internet
  - up from 46% in 2000

93% of teens ages 12-17 use the internet
  - up from 73% in 2000

Pew Internet & American Life Project (2008)
Today’s Youth
Tomorrow’s Workforce
What we know about our footprints

<table>
<thead>
<tr>
<th>% of internet users who say the following is available about them online:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home address</td>
</tr>
<tr>
<td>Company or employer</td>
</tr>
<tr>
<td>Email address</td>
</tr>
<tr>
<td>Home phone number</td>
</tr>
<tr>
<td>Things you’ve written that have your name on it</td>
</tr>
<tr>
<td>Photo of you</td>
</tr>
<tr>
<td>Groups or organizations you belong to</td>
</tr>
<tr>
<td>Political party or affiliation</td>
</tr>
<tr>
<td>Cell phone number</td>
</tr>
<tr>
<td>Video of you</td>
</tr>
</tbody>
</table>

Pew Internet & American Life Project (2008)