CHITKARA UNIVERSITY

Cybersecurity: Organizational Implications

Objectives

- Learn about the top threats faced by organizations.
- Understand what is social computing and why organizations should be careful about it.
- Understand the risks associated with social media networking.
- Understand Intellectual property right and implications of software piracy.
- Understand cloud computing challenges for organization
- Learn about data privacy and security

Introduction

- Most of the information that organization collects about an individual likely to come under ***"PI"*** category.

PI is information that is, or can be about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Information about an Individual

CHITKARA UNIVERSITY

- Information the organization collects about an Individual is/are:
  - Social Security Number
  - DL Number or any ID card number
  - Bank account number
  - Home address or E-Mail address
  - Medical or Health Information

Threats from Insider

CHITKARA UNIVERSITY

- An insider threat is defined as:

"The misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employee, contractors and other trusted individuals."

- Insider attacks are caused by human actions such as mistake, negligence, reckless behavior, theft, fraud and even sabotage.

Types of Insiders

- **A malicious insider:** Malicious insider is motivated to adversely impact on an organization through a range of actions that compromise information, confidentiality, integrity and/or availability.

Types of Insiders

CHITKARA UNIVERSITY

- **A careless insider**: Can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
- **A tricked insider**: is a person who is “tricked” into or led to provide sensitive information of the organization.

Cybersecurity practice and privacy

CHITKARA UNIVERSITY

- In an organization cybercrimes do not happen on their own or in isolation, rather they take place due to weakness of cybersecurity practices and “privacy” which may get impacted when cybercrimes happen.

Privacy

- **Informational/ data privacy**: It is about data protection and the user's right to determine how, when and to what extent information about them is communicated to other parties.

Privacy

- **Communication Privacy**: This is in networks, where encryption of data being transmitted is important.
- **Territorial Privacy**: It is about protecting user's property- For example the user devices- from being assaulted by undesired content such as SMS or E-Mail spam messages.

Key Challenges

- **Industrial Espionage**: There are several tools available for web administrators to monitor an track the various pages and objects that are accessed on their websites. For example Network administrator can examine a large amount of traffic coming from an IP to organizations network.
- This may make them take an anticipative action in counter by launching a new promotion to thwart the impact of your new product campaign.

Key Challenges

- **IP-base blocking**: This process is often used for blocking the access of specific IP address and/or domain name.
- For example the industrial espionage activities that are out of control, your marketing research team may be blocked from accessing your competitor's website.

- **IP-base clocking**: There are websites that change their online content depending on a user's IP address or user's geographic location.
- For example, your competitor web tool recognizes one of your technical employees surfing its site and display incorrect information of the product, thus making it impossible to obtain accurate competitive information.

- **Cyberterrorism**: refers to direct intervention of a threat source toward your organization's website.
- One example of this occurred in 1997 where the pentagon simulated a cyberattack. Through this attack they disrupt military communications, electrical power and network in several cities.

- **Confidential Information leakage:** An organization may be protected from external threats by your firewall and antivirus solution but you can protect from the attacks which are caused due to internal employees.

Software Piracy

- From a legal point of view software piracy is an IPR violation.
- Use of pirated software increases serious threat and risks of cybercrime and computer security when it comes to legal liability.
- One of lapses exploited by cybercriminals is the vulnerability of non genuine computer software.

Software Piracy

CHITKARA UNIVERSITY

- Non-genuine software can potentially disrupt smooth functioning of an organization's operations by adversely affecting the system security infrastructure. The most often quoted reasons by employees for use of pirated software are:
  - Pirated software is cheaper and more readily available.
  - Many others use pirated software anyways.
  - Latest versions are available faster when pirated software is used.

Web Threats for Organizations

CHITKARA UNIVERSITY

- Today most of the business applications are web based, especially with the growing adoption of cloud computing.
- Due to certain dependencies on internet, cybercriminals find it convenient to use the Net for committing crimes.

Challenges in an Organization

CHITKARA UNIVERSITY

- Employees Time wasted on Internet Surfing
- Enforcing Policy Usage in the Organization
- Monitoring and Controlling Employee's Internet Surfing.
- Keeping Security Patches and Virus Signature up to date
- Surviving in the Era of Legal Risks
- Bandwidth Wastage Issues
- Mobile workers Pose Security Challenges
- Challenges in Controlling Access to Web Applications
- The Need for Protecting Multiple Offices and Locations

Employees Time wasted on Internet Surfing

- This seems very sensitive topic in the organizations that claim to have a “liberal culture”.
- Every organization wants to have the finger on the pulse of employees, but when you challenge the employee surfing net then it can harbor anger and ill feeling between employees.

...cont.

- Organizations need to discipline an employee for internet misuse. One way of doing this is through computing Guidelines.
- Organizations need software tools, which once installed, monitor employee Internet activities in the background.
- It is hard to challenge who is using the web during work hours for personal reasons and who is using it in context of the task assigned.

...cont.

- Mindless and objective less surfing on the Internet seems to be disease, that may:
  - Waste employee productivity
  - Waste bandwidth

How to Monitor Employees

CHITKARA UNIVERSITY

- Constantly monitor the network, classify the finding and then report.
- To hold meetings to discuss the issues the need to agree on an action plan.
- Need to report the action taken.

One such tool to monitor employees is MessageLabs Security SafeGuard tool.

Cookies and Internet activities

CHITKARA UNIVERSITY

- Cookies are pieces of information that get passed to your browser by server on the internet. They get stored on your hard drive and are returned to the server when requested.
- Cookies come in two types:
  - Session Cookies
  - Persistent Cookies

Session Cookies

CHITKARA UNIVERSITY

- A session cookie is also called transient cookie.
- It lasts only for the duration of the internet session, that ism it is not persistent.
- Session cookies is not retained after the browser is closed.

Persistent Cookies

CHITKARA UNIVERSITY

- Persistent cookies are also known as stored cookies.
- Persistent cookies lasts beyond the browser session, they remain in the hard disk until expires or deleted by the user.
- Hence cookies helps to track a user on browser.

Enforcing Policy Usage in the Organization

- A security policy is a statement produced by the senior management of an organization or by a board or committee to dictate what type of role security plays within organization.

Monitoring and Controlling Employees Inte Surfing

- A powerful prevention can be created through effective monitoring and reporting of employees internet surfing.

Keeping Security Patches and Virus Signat up to date

CHITKARA UNIVERSITY

- It is necessary for IT staff to keep security system up to date with security signatures, software patches etc.

Bandwidth Wastage Issues

- Today's applications are bandwidth hungry due to increasing image content in messages.
- Using sophisticated policy controls, you can get such tools to block banned websites, download.

Mobile workers pose security challenges

CHITKARA UNIVERSITY

- Mobile workers uses PDA's to connect with their company network when they are on the move, this means there is a significant part of the workforce that remains unprotected.
- You need tools that extend web protection and filtering to remote users, including policy enforcement.

Challenges in Controlling Access to Web Application

CHITKARA UNIVERSITY

- As large number of organizations applications are web based from web mail to social networking so employees often tend to use these applications to bypass corporate guidelines on security.
- Organizations need to decide what type of access they should provide to employees based upon the nature of working style.

Security and Privacy implications from Clou Computing

CHITKARA UNIVERSITY

- According to a report cloud computing is one of the top 10 cyber threats to organization. Some piquant issues regarding cloud computing are:
  - How vendor handle data encryption
  - What about user authentication
  - Who will own the liability in case of data breach.
- Basically putting data in cloud may impact privacy rights.

- There is much legal uncertainty about privacy rights in cloud, hence organizations should think about the privacy scenario in terms of "**user spheres**". There are three types of spheres:
  - User Sphere
  - Recipient Sphere
  - Joint Sphere

User Sphere

- Here data is stored on users desktop's, PC, laptop, mobile phones, RFID chips etc.
- Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.

Recipient Sphere

- Here data lies with the recipient, Servers and databases of network providers, service providers or other parties with whom data recipient share data.

Joint Sphere

- Here data lies with web service providers server and database. This is the in between sphere.

Social Media Tools

CHITKARA UNIVERSITY

Social Media Marketing: Security Risks

CHITKARA UNIVERSITY

- According to a survey by marketing professionals usage of social media sites by large business to business organizations shows below:
  - Facebook is used by 37%
  - LiknkdIn is used by 36%
  - Twitter is used by 36%
  - You Tube is used by 22%
  - My Space is used by 6%

Data breach offense and data stealing

- Cybercriminals are on lookout for exploiting information to their advantage, they are using number of internet channels such as Web, E-mail, instant messaging, Voice over Internet to launch attack.
- Phishing is one of the major threat.

Social Networking Tools

- Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
- Professional networking tool LinkedIn is used to connect with community of top executives.
- Facebook as the social group or social community tool used to allow people to connect and share information.
- Wikipedia used for brand building.

2/3rd US households use social networks, twice as many as a year ago

98% of students at UNC use Facebook

Facebook has over 400 million “active” users, half of which login on any given day, 100 million via their mobile device

U.S. Facebook users 55 and older grew 922% in 2009 (now ~ 10 million)

How do we communicate today

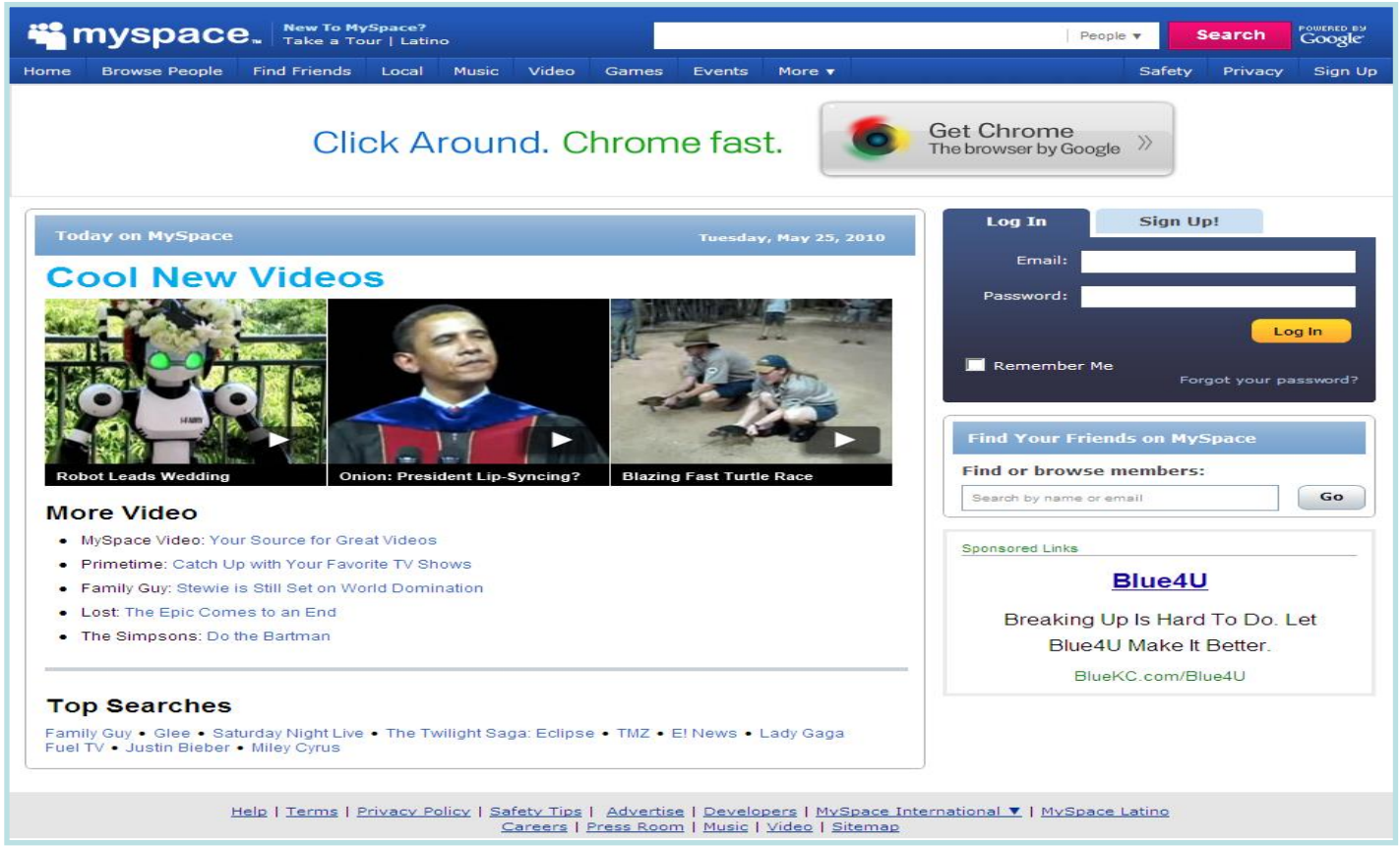
CHITKARA UNIVERSITY

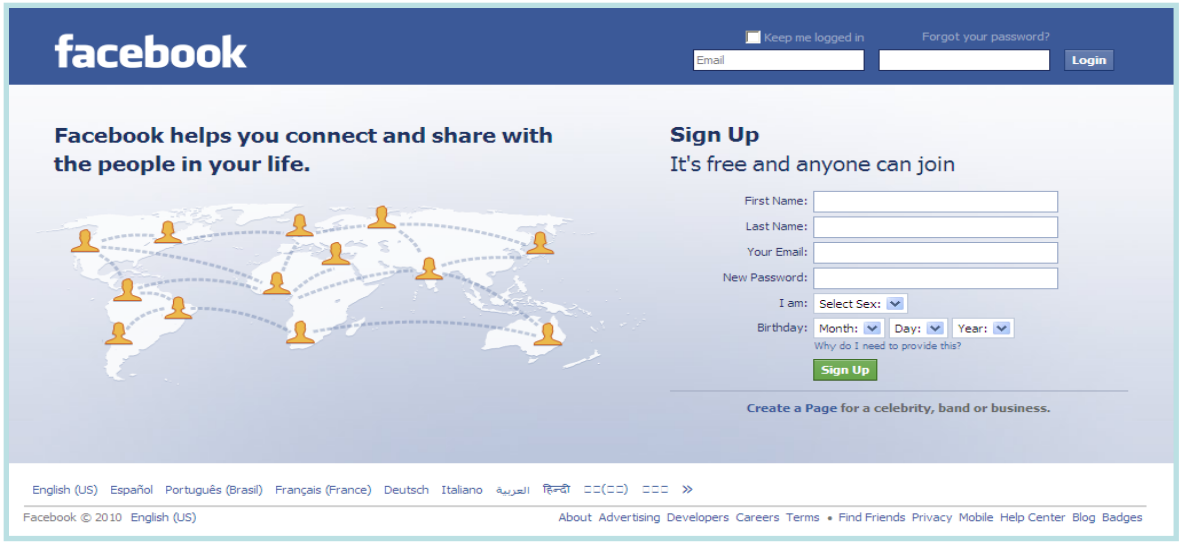
- I can write you a letter by snail mail.
- I can call you.
  - From my office phone or mobile device.
  - From my computer running Skype.
- We can video conference.
- I can be your Facebook friend.
- I can access your Myspace page.
- I can follow you on Twitter.
- I can actually visit you in person?!

“MySpace is a place for friends.”

“MySpace is Your Space.”

“MySpace keeps you connected.”





"Giving people the power to share and make the world more open and connected."

"Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick frequent answers to one simple question:

What are you doing?"

Why Use Social Media

- It's where the students are
- Provides a sense of community
- Seen as a forum to postulate views
- Fun way to stay connected with old friends or make new friends
- Forum for communication (individual/group/mass) and collaboration
- Allows for self-expression and self-representation

What are security Risks

- **Malware distribution**
- **Cyber-bullying** ("trolling," emotional abuse)

- **Privacy concerns**
  - Information about you that *you* post
  - Information about you that *others* post
  - Information about you the *social networking sites* collect and share with others

What are security Risks

- Can result in social engineering, identity theft, financial fraud, infected computers, stalking, child abuse, sexual predation, defamation, lawsuits, mad boyfriend/girlfriend/spouse/parent, unwanted legacy, embarrassment, …

Take my stuff, please!

May 6, 2010 ... I am going **on vacation** the end of July and first week of August (Maine). Today the ACL guest editor was confirmed. This is going to be fun.
twitter.com/acontinuouslean/status/13511554783 - Cached

twitter.com/ShaniDavis2010/statuses/11954707145 - Cached

Twitter / Christian Louboutin: Hey guys ,I'm **on vacation** ...
Hey guys ,I'm **on vacation** next week , I'll reply to all your questions when I return!Take care ;)
twitter.com/LouboutinWorld/status/11098562936 - Cached

Twitter / Don Braid: **On vacation** in Banff. Am I ...
May 6, 2010 ... **On vacation** in Banff. Am I dreaming? #ableg #abpc #banff #ablib #wap.
twitter.com/DonBraid/status/13526777881 - Cached

Twitter / Hunter Pecunia: Loving being **on vacation** a ...
Mar 15, 2010 ... Loving being **on vacation** at the beautiful white, chilly, beach in Florida. At least my hotel has a hot tub! Haha!!
twitter.com/hunterpecunia/status/10546398591 - Cached

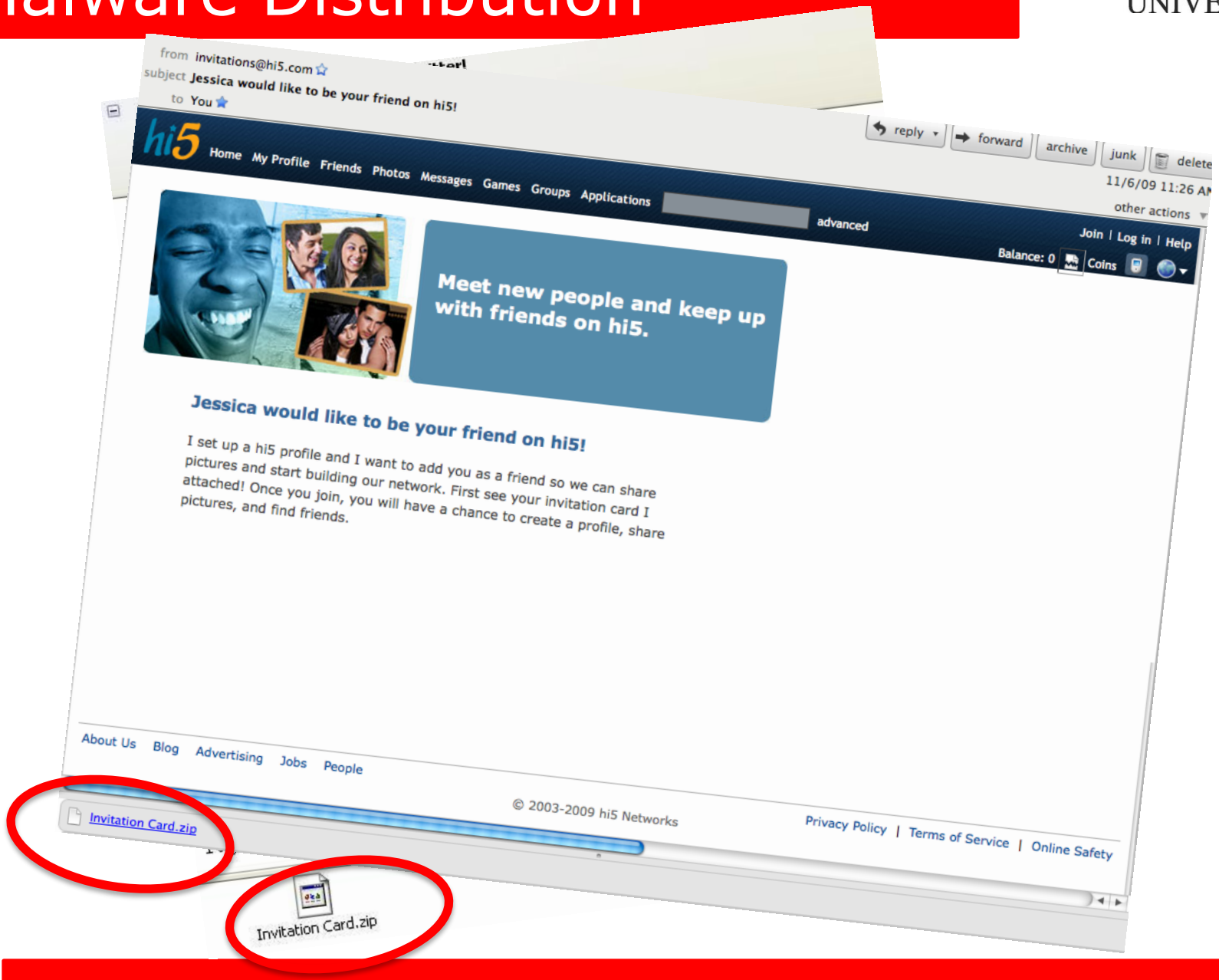
Malware Distribution

CHITKARA UNIVERSITY

- Similar to other threats that can lead to downloading/installing malware
  - Malicious ads
  - Wall posts, inbox or chat messages with malicious links from “Friends” (hijacked user account)
  - “My wallet was stolen and I’m stuck in Rome. Send me cash now.”
  - Spam email pretending to be from Facebook admins

Malware Distribution

CHITKARA UNIVERSITY



Who is Peeking

CHITKARA UNIVERSITY

- Friends\family
- Friends of friends\family
- Parents
- Employers and co-workers
  - Dec 2009 study commissioned by Microsoft said 79% of recruiters & hiring mgrs researched applicants online
  - CareerBuilder.com study – 45% of employers use social networks to screen job candidates
- Customers
- Universities
- Marketing companies\vendors
- Criminals\hackers
- Government agencies (IRS, SRS!)
- EVERYONE ELSE

CHITKARA UNIVERSITY

The Evolution of Facebook "Privacy"

(blue = default availability of your personal data)

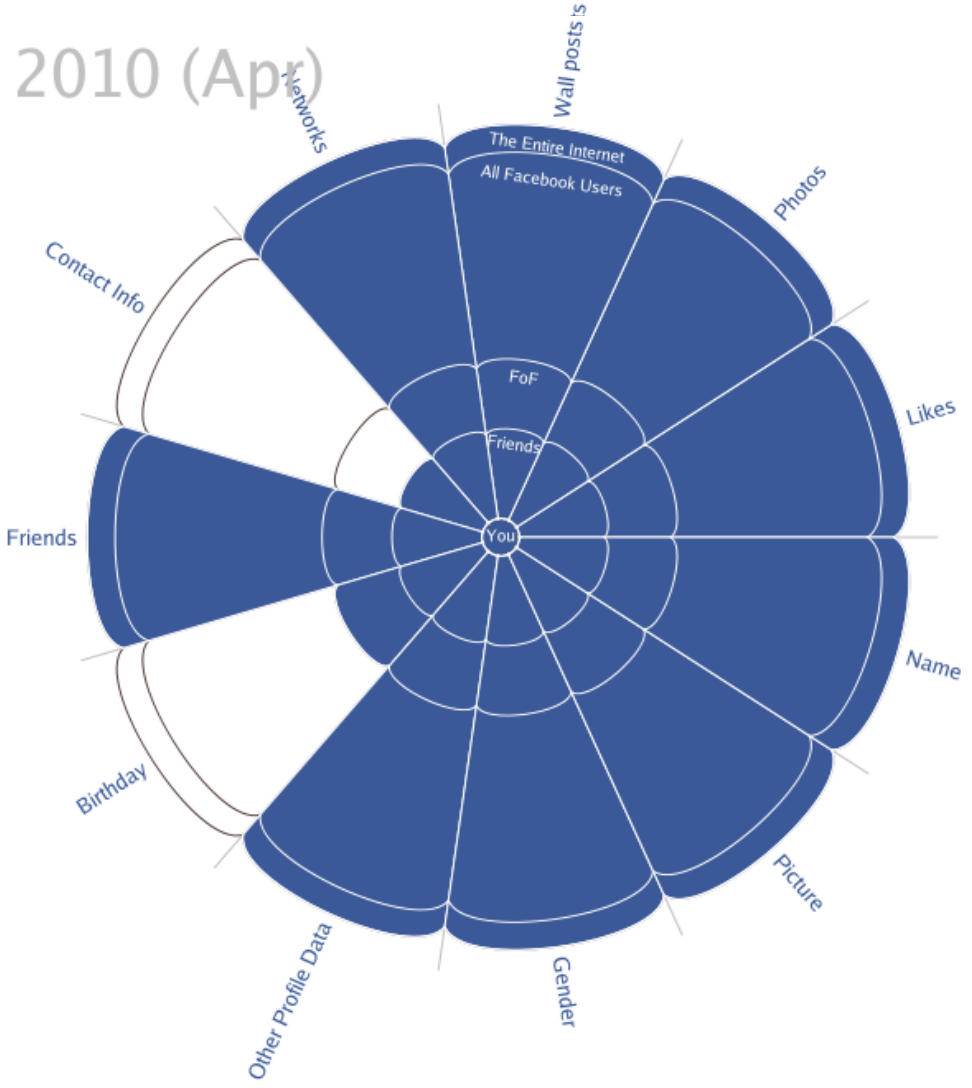


Chart by Matt McKeon: http://mattmckeon.com/facebook-privacy/#

- Within the past year, 9 percent of social network users experienced some form of abuse, such as malware infections, scams, identity theft, or harassment.
- Many social network users are inexperienced about risks. Forty percent had posted their full birth date, exposing them to identity theft.
- Twenty-six percent of Facebook users with children had potentially exposed them to predators by posting the children's photos and names.

Tips for safer social Networking

CHITKARA UNIVERSITY

1. Use a strong, unique password (don't use the same password on multiple sites; don't use eID password on social networking sites)
2. Provide as little personal information as possible – avoid revealing birth date, address, etc.

Tips for safer social Networking

CHITKARA UNIVERSITY

3. Understand and customize the privacy settings in all of your social networking accounts
4. Don't allow 3rd party applications to access your information (if possible)
5. Be careful about what you post
   a. Photos of self or others
   b. Opinions on controversial topics
   c. Don't rip classmates, professors, coworkers, employers, etc. – it WILL come back to haunt you

Tips for safer social Networking

CHITKARA UNIVERSITY

6. Don’t post anything related to your employer (unless you’re authorized)
7. Supervise your kids’ use of social networking sites.
8. Be suspicious of friend/follow requests, ads, 3rd party applications, chat messages, etc.
9. Minimize exploration – don’t carelessly click on lots of ads, videos, games, etc.

Tips for safer social Networking

CHITKARA UNIVERSITY

10. Use built-in and add-on features in web browsers to warn you of malicious sites
    a. Anti-phishing filters in IE and Firefox
    b. Web of Trust
    c. Adblock Plus
11. Think before you click

IPR

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

Why Should I Protect My IP? Can I Benefit from It?

Importance of protecting Intellectual Prope

CHITKARA UNIVERSITY

- protection to an invention for the exclusive use of it by
- its inventor
- leverage business
- legal recognition to the invention
- enables its enforcement in the court of law
- incentive for further development
- public use
- huge source of information
- source for further developmental work by third party
- encourage fair trading
- contribute to social and economic development

Classification of IPR

Intellectual Property Rights are generally classified as follows:

- Invention: Patents
- Letters, numbers, words, colors, phrase, sound, smell, logo, shape, picture, or combination of these: Trademark
- Art, literature, music, broadcast and computer programs: Copyright
- 2D/3D product design: Design Registration
- New plant varieties: Plant Breeder's right
- Confidential information: Trade secret