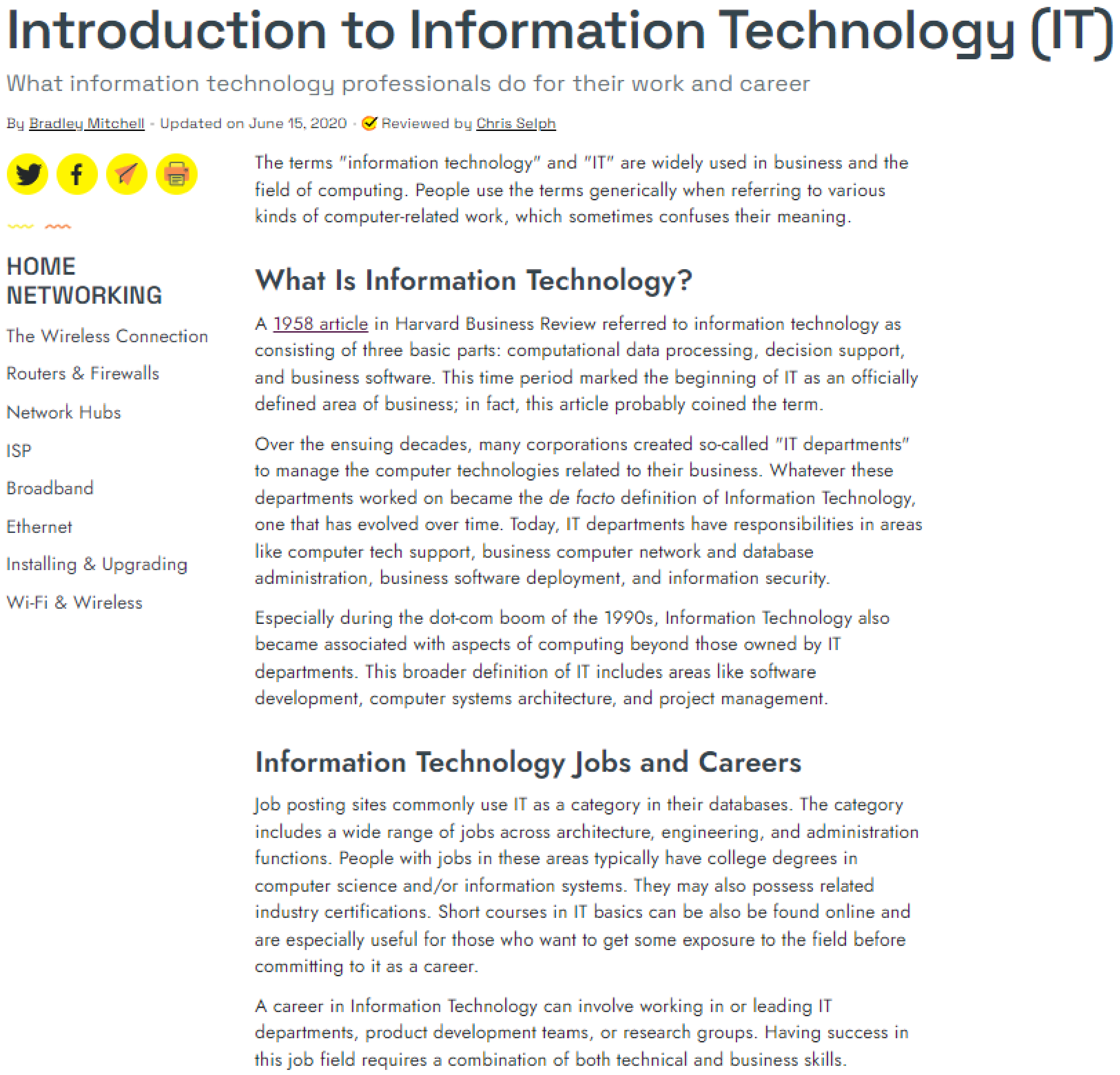
PP Outlines Solved

1. Introduction to IT



Introduction to Information Technology (IT)

What information technology professionals do for their work and career

By Bradley Mitchell · Updated on June 15, 2020 · Reviewed by Chris Selph

The terms "information technology" and "IT" are widely used in business and the field of computing. People use the terms generically when referring to various kinds of computer-related work, which sometimes confuses their meaning.

What Is Information Technology?

A 1958 article in Harvard Business Review referred to information technology as consisting of three basic parts: computational data processing, decision support, and business software. This time period marked the beginning of IT as an officially defined area of business; in fact, this article probably coined the term.

Over the ensuing decades, many corporations created so-called "IT departments" to manage the computer technologies related to their business. Whatever these departments worked on became the *de facto* definition of Information Technology, one that has evolved over time. Today, IT departments have responsibilities in areas like computer tech support, business computer network and database administration, business software deployment, and information security.

Especially during the dot-com boom of the 1990s, Information Technology also became associated with aspects of computing beyond those owned by IT departments. This broader definition of IT includes areas like software development, computer systems architecture, and project management.

Information Technology Jobs and Careers

Job posting sites commonly use IT as a category in their databases. The category includes a wide range of jobs across architecture, engineering, and administration functions. People with jobs in these areas typically have college degrees in computer science and/or information systems. They may also possess related industry certifications. Short courses in IT basics can be also be found online and are especially useful for those who want to get some exposure to the field before committing to it as a career.

A career in Information Technology can involve working in or leading IT departments, product development teams, or research groups. Having success in this job field requires a combination of both technical and business skills.

Issues and Challenges in Information Technology

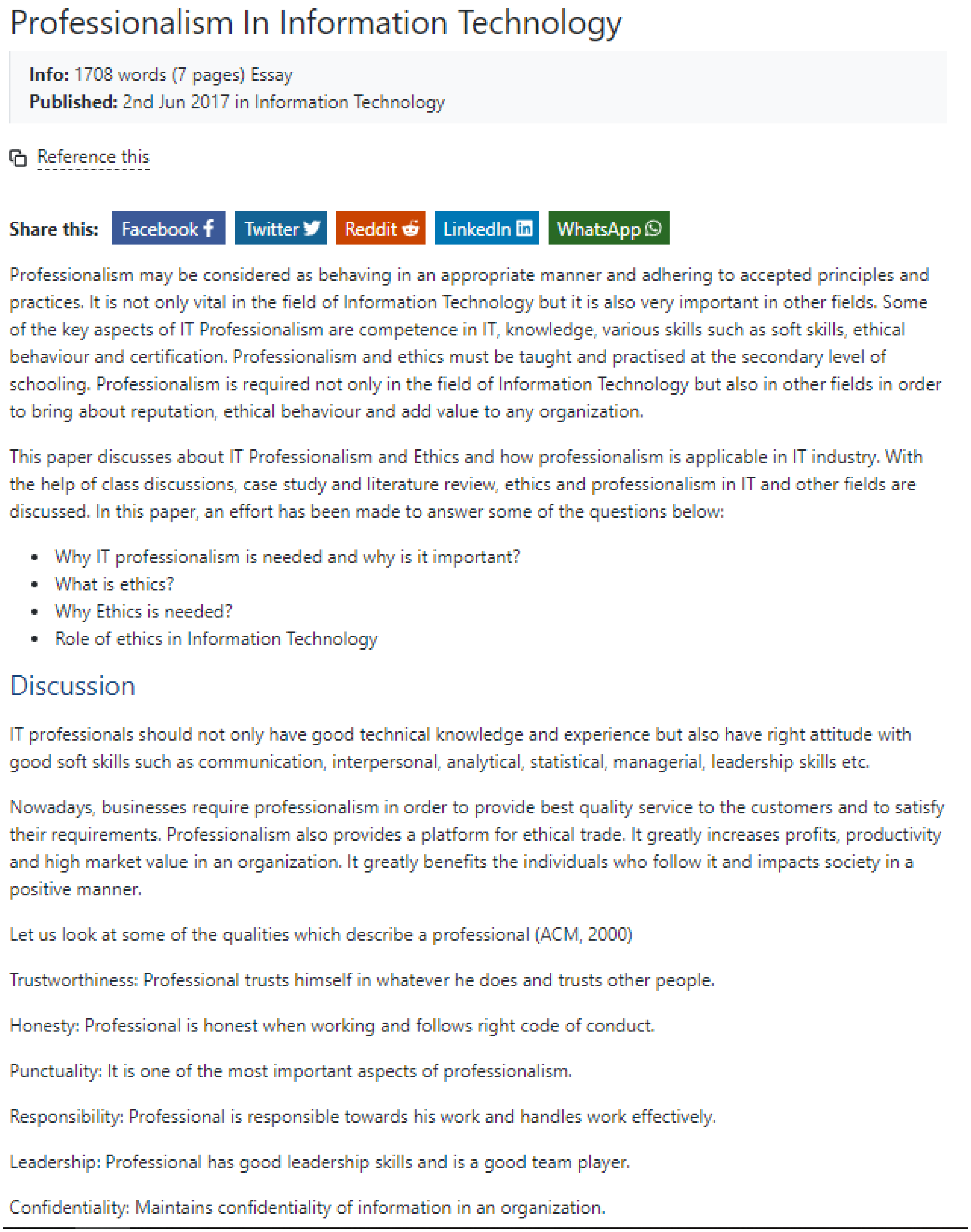
- As computing systems and capabilities continue expanding worldwide, "data overload" has become an increasingly critical issue for many IT professionals. Efficiently processing huge amounts of data to produce useful business intelligence requires large amounts of processing power, sophisticated software, and human analytic skills.
- Teamwork and communication skills have also become essential for most businesses to manage the complexity of IT systems. Many IT professionals are responsible for providing service to business users who are not trained in computer networking or other information technologies but who are instead interested in simply using IT as a tool to get their work done efficiently.
- System and network security issues are a primary concern for many business executives, as any security incident can potentially damage a company's reputation and cost large sums of money.

Computer Networking and Information Technology

Because networks play a central role in the operation of many companies, business computer networking topics tend to be closely associated with Information Technology. Networking trends that play a key role in IT include:

- Network capacity and performance: The popularity of online video has greatly increased the demand for network bandwidth both on the Internet and on IT networks. New types of software applications that support richer graphics and deeper interaction with computers also tend to generate larger amounts of data and hence network traffic. Information technology teams must plan appropriately not just for their company's current needs but also this future growth.
- Mobile and wireless usages: IT network administrators must now support a wide array of smartphones and tablets in addition to traditional PCs and workstations. IT environments tend to require high-performance wireless hotspots with roaming capability. In larger office buildings, deployments are carefully planned and tested to eliminate dead spots and signal interference.
- Cloud services: Whereas IT shops in the past maintained their own server farms for hosting email and business databases, some have migrated to cloud computing environments where third-party hosting providers maintain the data. This change in computing model dramatically changes the patterns of traffic on a company network, but it also requires significant effort in training

2. Professionalism in the field of IT



Professionalism In Information Technology

Info: 1708 words (7 pages) Essay
Published: 2nd Jun 2017 in Information Technology

Professionalism may be considered as behaving in an appropriate manner and adhering to accepted principles and practices. It is not only vital in the field of Information Technology but it is also very important in other fields. Some of the key aspects of IT Professionalism are competence in IT, knowledge, various skills such as soft skills, ethical behaviour and certification. Professionalism and ethics must be taught and practised at the secondary level of schooling. Professionalism is required not only in the field of Information Technology but also in other fields in order to bring about reputation, ethical behaviour and add value to any organization.

This paper discusses about IT Professionalism and Ethics and how professionalism is applicable in IT industry. With the help of class discussions, case study and literature review, ethics and professionalism in IT and other fields are discussed. In this paper, an effort has been made to answer some of the questions below:

- Why IT professionalism is needed and why is it important?
- What is ethics?
- Why Ethics is needed?
- Role of ethics in Information Technology

Discussion

IT professionals should not only have good technical knowledge and experience but also have right attitude with good soft skills such as communication, interpersonal, analytical, statistical, managerial, leadership skills etc.

Nowadays, businesses require professionalism in order to provide best quality service to the customers and to satisfy their requirements. Professionalism also provides a platform for ethical trade. It greatly increases profits, productivity and high market value in an organization. It greatly benefits the individuals who follow it and impacts society in a positive manner.

Let us look at some of the qualities which describe a professional (ACM, 2000)

Trustworthiness: Professional trusts himself in whatever he does and trusts other people.

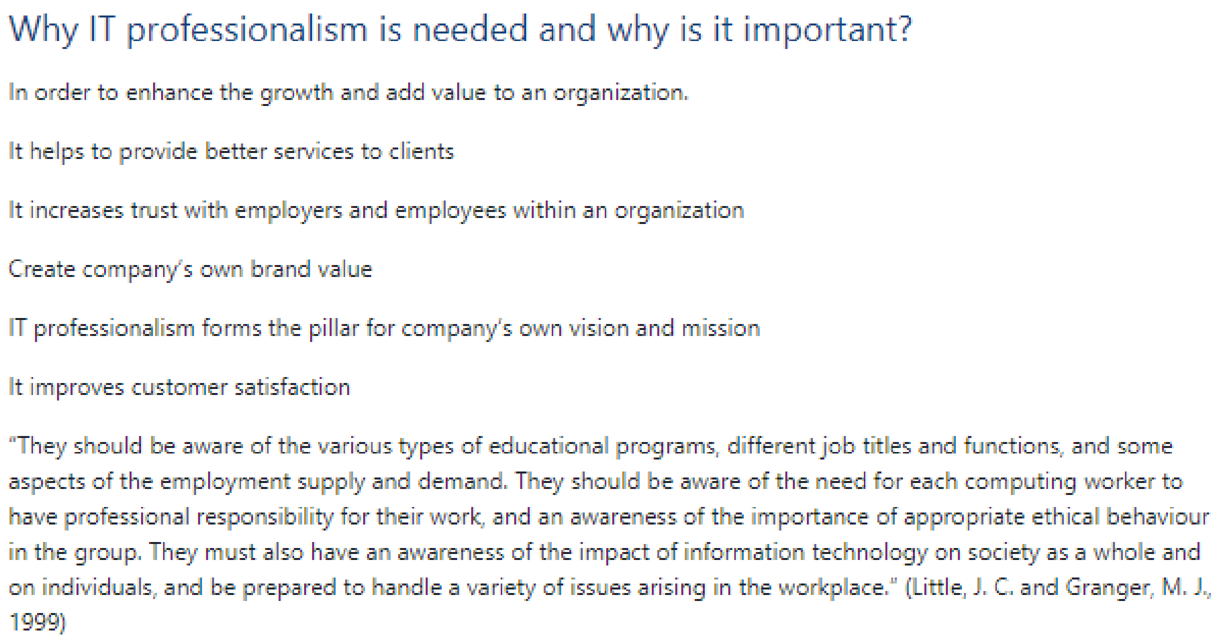
Honesty: Professional is honest when working and follows right code of conduct.

Punctuality: It is one of the most important aspects of professionalism.

Responsibility: Professional is responsible towards his work and handles work effectively.

Leadership: Professional has good leadership skills and is a good team player.

Confidentiality: Maintains confidentiality of information in an organization.



Why IT professionalism is needed and why is it important?

In order to enhance the growth and add value to an organization.

It helps to provide better services to clients

It increases trust with employers and employees within an organization

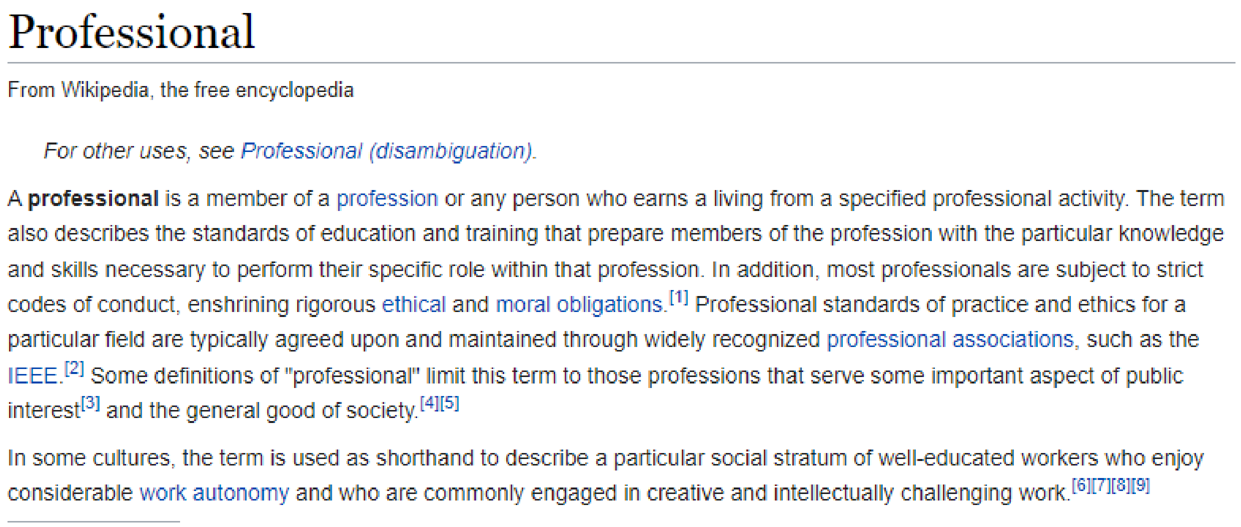
Create company's own brand value

IT professionalism forms the pillar for company's own vision and mission

It improves customer satisfaction

"They should be aware of the various types of educational programs, different job titles and functions, and some aspects of the employment supply and demand. They should be aware of the need for each computing worker to have professional responsibility for their work, and an awareness of the importance of appropriate ethical behaviour in the group. They must also have an awareness of the impact of information technology on society as a whole and on individuals, and be prepared to handle a variety of issues arising in the workplace." (Little, J. C. and Granger, M. J., 1999)

Professional in general



Professional

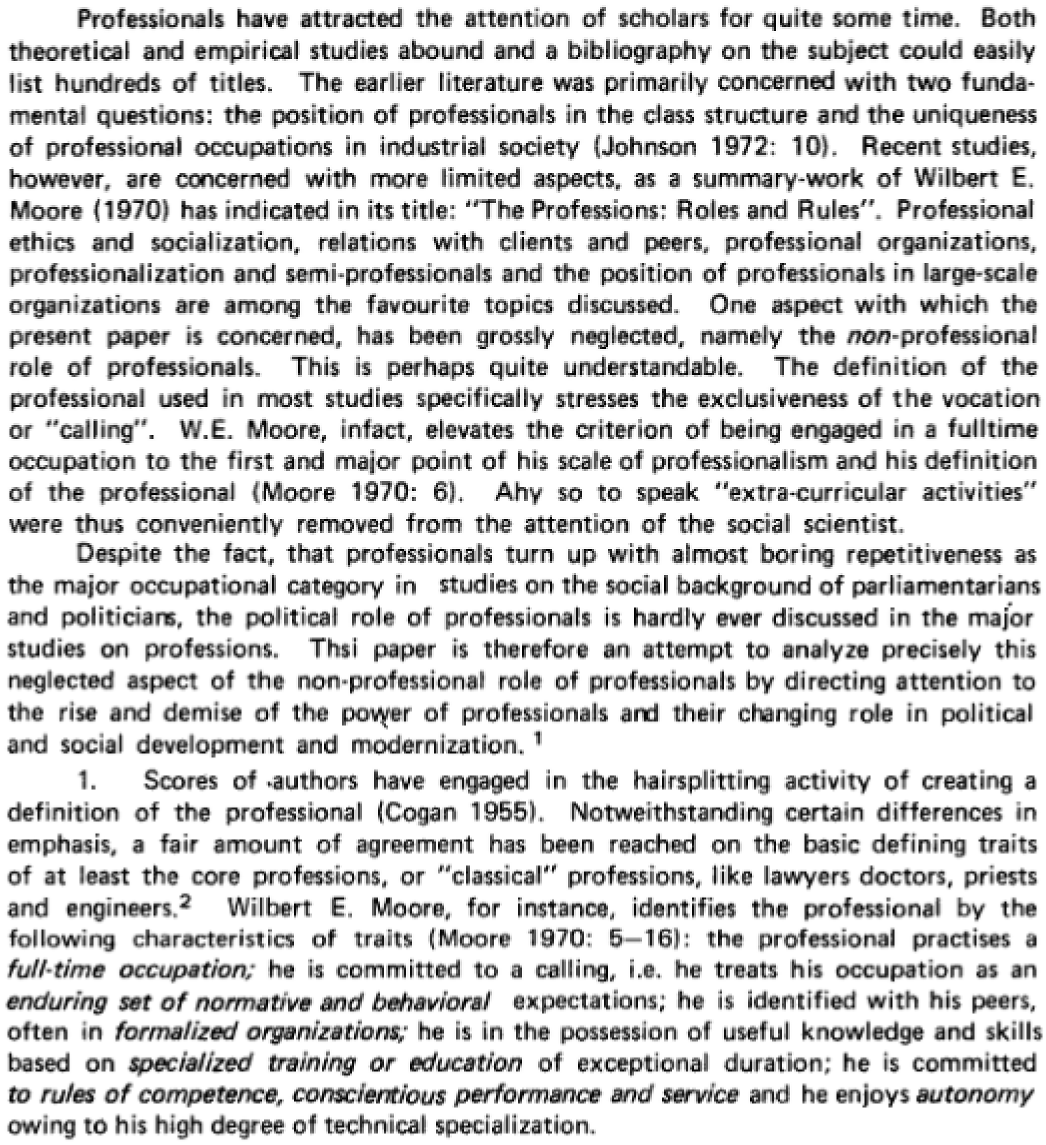
From Wikipedia, the free encyclopedia

For other uses, see Professional (disambiguation).

A **professional** is a member of a profession or any person who earns a living from a specified professional activity. The term also describes the standards of education and training that prepare members of the profession with the particular knowledge and skills necessary to perform their specific role within that profession. In addition, most professionals are subject to strict codes of conduct, enshrining rigorous ethical and moral obligations.[1] Professional standards of practice and ethics for a particular field are typically agreed upon and maintained through widely recognized professional associations, such as the IEEE.[2] Some definitions of "professional" limit this term to those professions that serve some important aspect of public interest[3] and the general good of society.[4][5]

In some cultures, the term is used as shorthand to describe a particular social stratum of well-educated workers who enjoy considerable work autonomy and who are commonly engaged in creative and intellectually challenging work.[6][7][8][9]

Professionalism role in our society

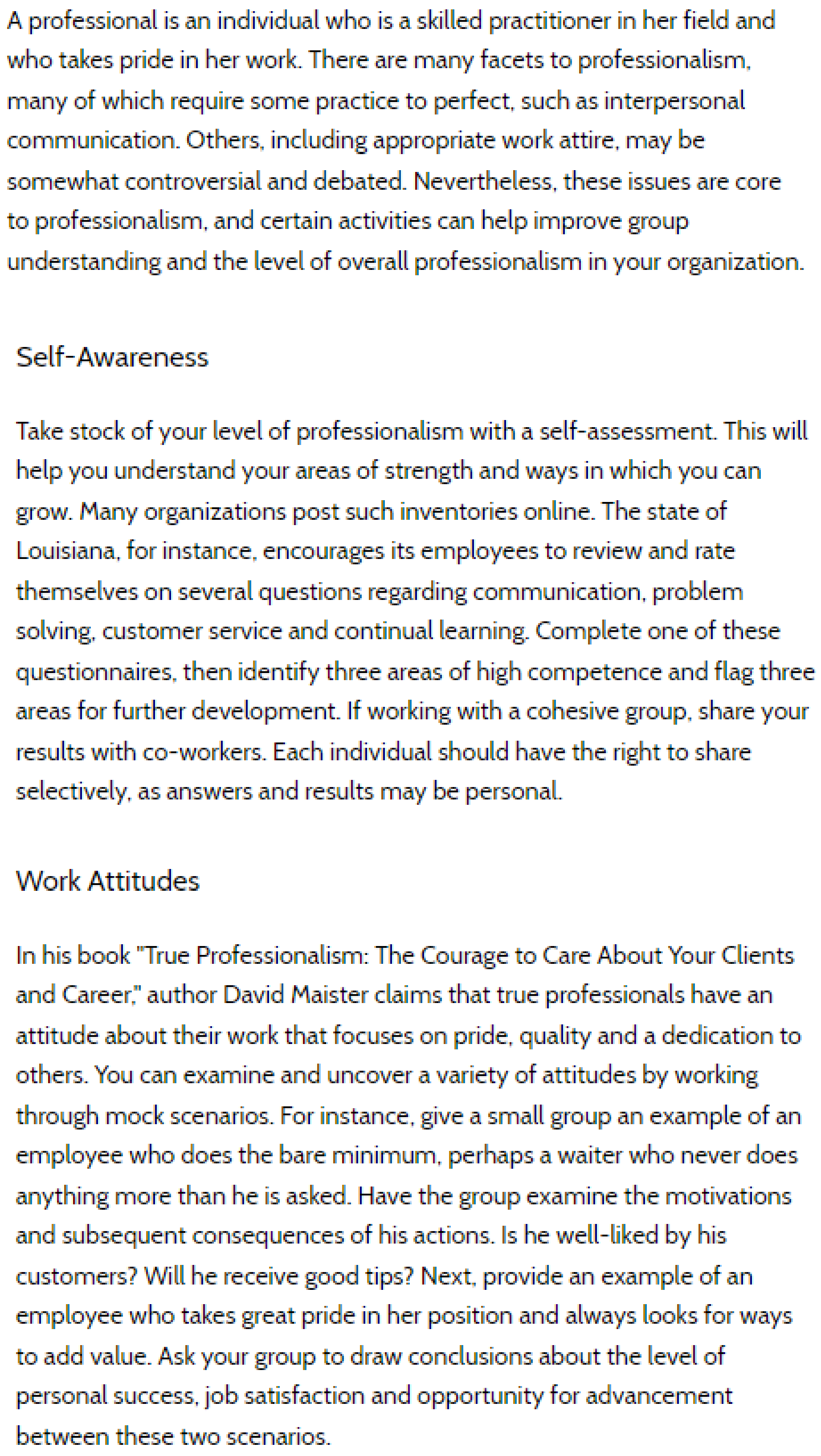


Professionals have attracted the attention of scholars for quite some time. Both theoretical and empirical studies abound and a bibliography on the subject could easily list hundreds of titles. The earlier literature was primarily concerned with two fundamental questions: the position of professionals in the class structure and the uniqueness of professional occupations in industrial society (Johnson 1972: 10). Recent studies, however, are concerned with more limited aspects, as a summary-work of Wilbert E. Moore (1970) has indicated in its title: "The Professions: Roles and Rules". Professional ethics and socialization, relations with clients and peers, professional organizations, professionalization and semi-professionals and the position of professionals in large-scale organizations are among the favourite topics discussed. One aspect with which the present paper is concerned, has been grossly neglected, namely the *non*-professional role of professionals. This is perhaps quite understandable. The definition of the professional used in most studies specifically stresses the exclusiveness of the vocation or "calling". W.E. Moore, infact, elevates the criterion of being engaged in a fulltime occupation to the first and major point of his scale of professionalism and his definition of the professional (Moore 1970: 6). Ahy so to speak "extra-curricular activities" were thus conveniently removed from the attention of the social scientist.

Despite the fact, that professionals turn up with almost boring repetitiveness as the major occupational category in studies on the social background of parliamentarians and politicians, the political role of professionals is hardly ever discussed in the major studies on professions. Thsi paper is therefore an attempt to analyze precisely this neglected aspect of the non-professional role of professionals by directing attention to the rise and demise of the power of professionals and their changing role in political and social development and modernization. [1]

1. Scores of authors have engaged in the hairsplitting activity of creating a definition of the professional (Cogan 1955). Notweithstanding certain differences in emphasis, a fair amount of agreement has been reached on the basic defining traits of at least the core professions, or "classical" professions, like lawyers doctors, priests and engineers.[2] Wilbert E. Moore, for instance, identifies the professional by the following characteristics of traits (Moore 1970: 5–16): the professional practises a *full-time occupation;* he is committed to a calling, i.e. he treats his occupation as an *enduring set of normative and behavioral* expectations; he is identified with his peers, often in *formalized organizations;* he is in the possession of useful knowledge and skills based on *specialized training or education* of exceptional duration; he is committed *to rules of competence, conscientious performance and service* and he enjoys *autonomy* owing to his high degree of technical specialization.

Professionalism Activities



A professional is an individual who is a skilled practitioner in her field and who takes pride in her work. There are many facets to professionalism, many of which require some practice to perfect, such as interpersonal communication. Others, including appropriate work attire, may be somewhat controversial and debated. Nevertheless, these issues are core to professionalism, and certain activities can help improve group understanding and the level of overall professionalism in your organization.

Self-Awareness

Take stock of your level of professionalism with a self-assessment. This will help you understand your areas of strength and ways in which you can grow. Many organizations post such inventories online. The state of Louisiana, for instance, encourages its employees to review and rate themselves on several questions regarding communication, problem solving, customer service and continual learning. Complete one of these questionnaires, then identify three areas of high competence and flag three areas for further development. If working with a cohesive group, share your results with co-workers. Each individual should have the right to share selectively, as answers and results may be personal.

Work Attitudes

In his book "True Professionalism: The Courage to Care About Your Clients and Career," author David Maister claims that true professionals have an attitude about their work that focuses on pride, quality and a dedication to others. You can examine and uncover a variety of attitudes by working through mock scenarios. For instance, give a small group an example of an employee who does the bare minimum, perhaps a waiter who never does anything more than he is asked. Have the group examine the motivations and subsequent consequences of his actions. Is he well-liked by his customers? Will he receive good tips? Next, provide an example of an employee who takes great pride in her position and always looks for ways to add value. Ask your group to draw conclusions about the level of personal success, job satisfaction and opportunity for advancement between these two scenarios.

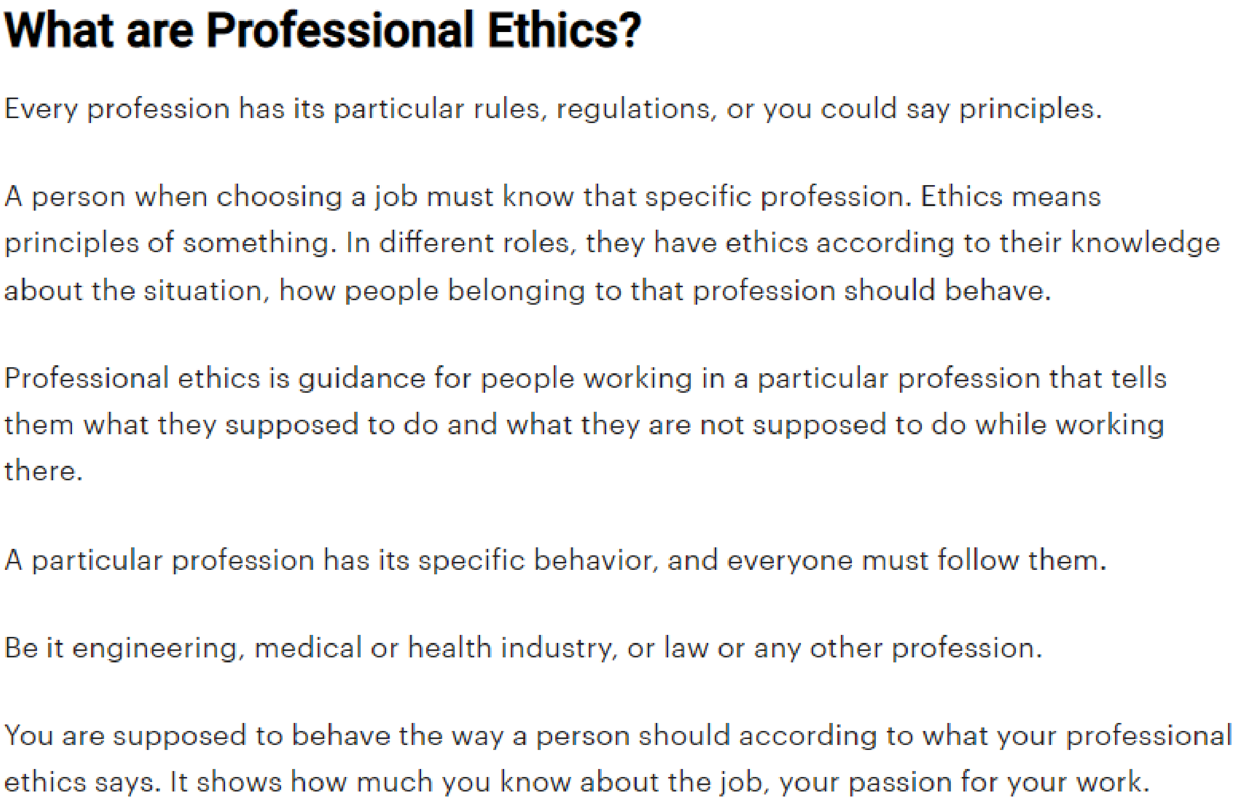
Communication

The ability to listen carefully and to communicate your ideas and feelings effectively can greatly improve working relationships and can lead to greater productivity. In one activity, a pair of employees can be charged with deciding the appropriate time needed for an upcoming project. As each employee will play an active role in the project, allow each to take a turn explaining his workload and ability to finish the task in the specific time frame. Encourage them to practice self-advocacy by using "I" statements rather than "you" statements. For example, one might say, "I can complete this task in one month rather than two weeks because of competing priorities." This encourages employees to take ownership of their roles and not blame others by saying, "You aren't giving me enough time to get this done." Each individual should restate the needs of her colleague to encourage validation and active listening.

Managing Appearances

Each employee is an ambassador of the organization, and the way that he presents himself can either improve or diminish the view of the organization in the eyes of others. Ask a small group to brainstorm specific aspects of attire and physical grooming that they've seen in past jobs. Next, ask them to honestly evaluate the first impressions that were associated with those individuals. For example, if a man shows up each day in a crumpled suit and a scraggly beard, what does that say about his care for himself and the company's image? Likewise, if a colleague comes to work in neatly pressed slacks, is well-groomed and has an encouraging smile, how does this make you feel about working with him? Although there may not be group consensus on each scenario, it's important to solicit the sincere opinions of numerous people and allow a conversation to develop.

3. Professional Ethics



What are Professional Ethics?

Every profession has its particular rules, regulations, or you could say principles.

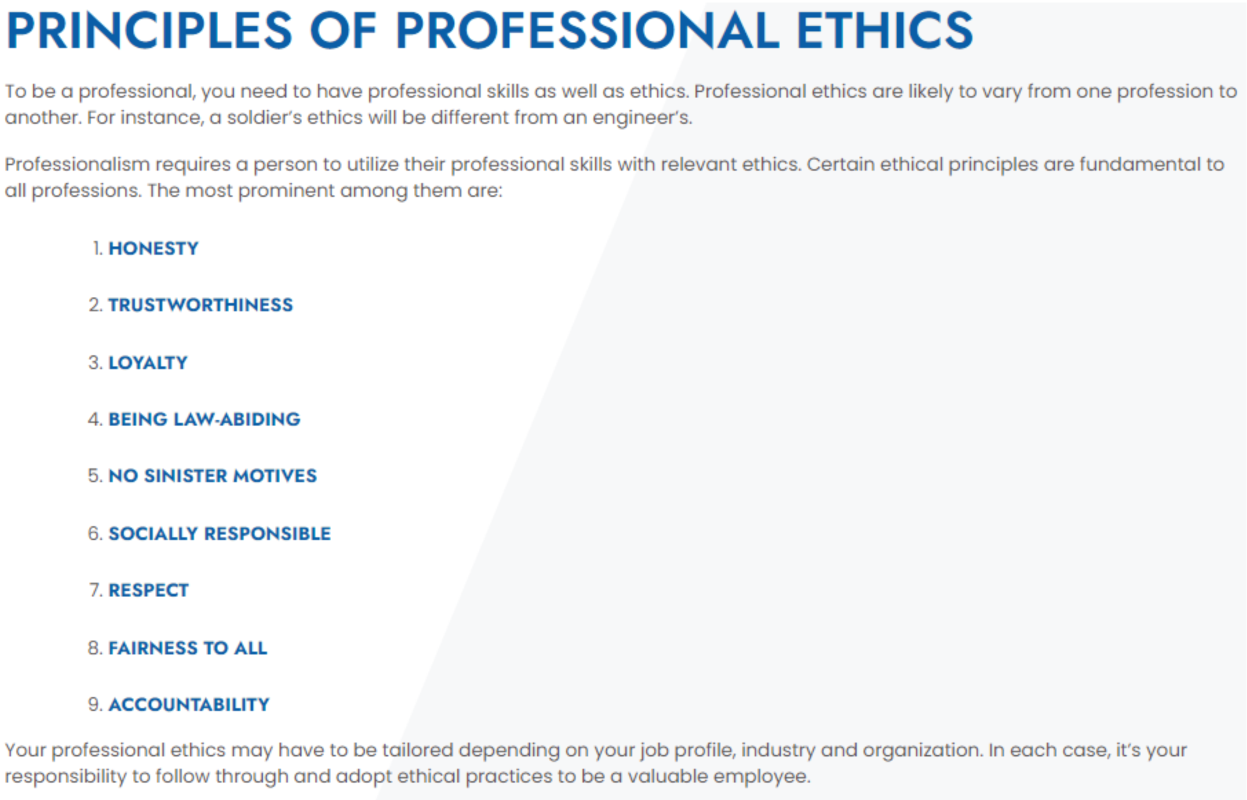
A person when choosing a job must know that specific profession. Ethics means principles of something. In different roles, they have ethics according to their knowledge about the situation, how people belonging to that profession should behave.

Professional ethics is guidance for people working in a particular profession that tells them what they supposed to do and what they are not supposed to do while working there.

A particular profession has its specific behavior, and everyone must follow them.

Be it engineering, medical or health industry, or law or any other profession.

You are supposed to behave the way a person should according to what your professional ethics says. It shows how much you know about the job, your passion for your work.



PRINCIPLES OF PROFESSIONAL ETHICS

To be a professional, you need to have professional skills as well as ethics. Professional ethics are likely to vary from one profession to another. For instance, a soldier's ethics will be different from an engineer's.

Professionalism requires a person to utilize their professional skills with relevant ethics. Certain ethical principles are fundamental to all professions. The most prominent among them are:

1. **HONESTY**
2. **TRUSTWORTHINESS**
3. **LOYALTY**
4. **BEING LAW-ABIDING**
5. **NO SINISTER MOTIVES**
6. **SOCIALLY RESPONSIBLE**
7. **RESPECT**
8. **FAIRNESS TO ALL**
9. **ACCOUNTABILITY**

Your professional ethics may have to be tailored depending on your job profile, industry and organization. In each case, it's your responsibility to follow through and adopt ethical practices to be a valuable employee.

CODES OF CONDUCT

The codes of conduct for any profession are established by combining the above-mentioned ethics with professional skills. They outline the acceptable standards of behavior, quality of service and social responsibility that every professional in the field has to follow.

These codes of conduct also aim to safeguard the wellness of professionals and help them achieve their expectations without compromising on things like work-life balance, quality of work and personal and professional development.

There are a lot of benefits that professional skills-based codes of conduct offer to various stakeholders. Let's take a look at the beneficiaries and what they get from professionalism:

- **PUBLIC:**

If the codes of conduct are adhered to, the general public is assured of a standardized service and will trust an individual's professional skills.

- **CLIENTS:**

An ethical professional would lend confidence to clients about quality, transparency and assured service.

- **PROFESSIONAL COMMUNITY:**

Adherence to the codes of conduct by professionals benefits even other members of the same profession. They're able to develop and implement processes and frameworks that further reduce the likelihood of unprofessional activities or unlawful steps. Ethics also prevent a person from exploring the loopholes in the rules and misuse the system.

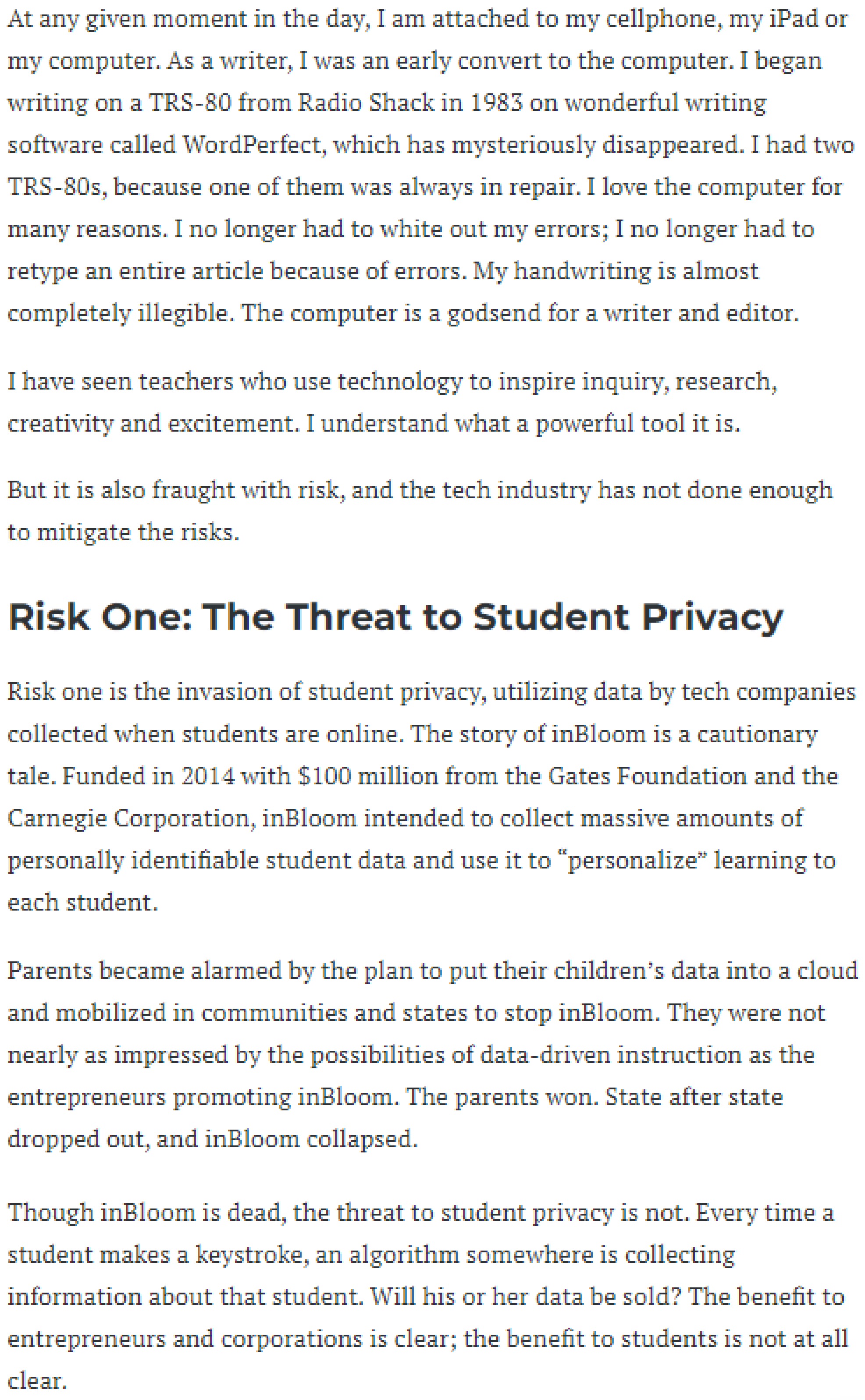
- **PROFESSION:**

By following the codes of conduct and working ethically, a professional will be able to enhance the value and scope of the profession and pave the way for its popularity among the masses.

- **OTHER STAKEHOLDERS:**

Strong ethical conduct enhances the reputation of a profession and people from other walks of life see it as a reliable and respectable field that is comfortable to deal with.

4. Misuse of IT and their Risks



At any given moment in the day, I am attached to my cellphone, my iPad or my computer. As a writer, I was an early convert to the computer. I began writing on a TRS-80 from Radio Shack in 1983 on wonderful writing software called WordPerfect, which has mysteriously disappeared. I had two TRS-80s, because one of them was always in repair. I love the computer for many reasons. I no longer had to white out my errors; I no longer had to retype an entire article because of errors. My handwriting is almost completely illegible. The computer is a godsend for a writer and editor.

I have seen teachers who use technology to inspire inquiry, research, creativity and excitement. I understand what a powerful tool it is.

But it is also fraught with risk, and the tech industry has not done enough to mitigate the risks.

Risk One: The Threat to Student Privacy

Risk one is the invasion of student privacy, utilizing data by tech companies collected when students are online. The story of inBloom is a cautionary tale. Funded in 2014 with $100 million from the Gates Foundation and the Carnegie Corporation, inBloom intended to collect massive amounts of personally identifiable student data and use it to "personalize" learning to each student.

Parents became alarmed by the plan to put their children's data into a cloud and mobilized in communities and states to stop inBloom. They were not nearly as impressed by the possibilities of data-driven instruction as the entrepreneurs promoting inBloom. The parents won. State after state dropped out, and inBloom collapsed.

Though inBloom is dead, the threat to student privacy is not. Every time a student makes a keystroke, an algorithm somewhere is collecting information about that student. Will his or her data be sold? The benefit to entrepreneurs and corporations is clear; the benefit to students is not at all clear.

Risk Two: The Proliferation of 'Personalized Learning'

Personalized learning, or “competency-based education,” are both euphemisms for computer adaptive instruction. Again, a parent rebellion is brewing, because parents want their children taught by a human being, not a computer. They fear that their children will be mechanized, standardized, subjected to depersonalized instruction, not “personalized learning.” While many entrepreneurs are investing in software to capture this burgeoning industry, there is still no solid evidence that students learn more or better when taught by a computer.

Risk Three: The Extensive Use of Technology for Assessment.

Technology is highly compatible with standardized testing, which encourages standardized questions and standardized answers. If the goal of learning is to teach creativity, imagination, and risk-taking, assessment should encourage students to be critical thinkers, not accepting the conventional wisdom, not checking off the right answer. Furthermore, the ability of computers to judge essays is still undeveloped and may remain so. Professor Les Perelman at MIT demonstrated that computer-graded essays can get high scores for gibberish and that computers lack the “intelligence” to reason or understand what matters most in writing.

Risk four: The Cyber Charter School

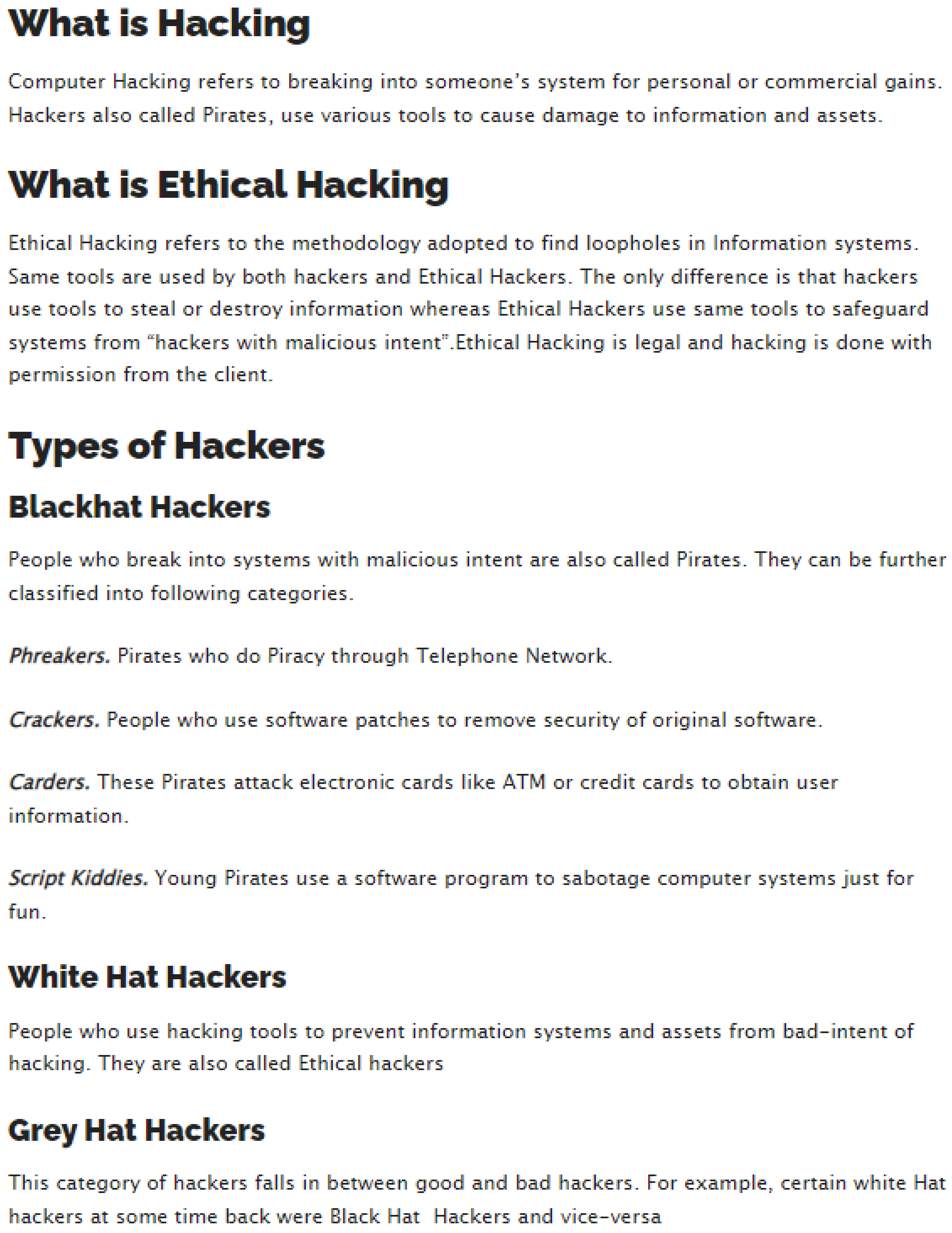
Most such virtual schools, or cyber charters, are operated for profit; the largest of them is a chain called K12 Inc., which is listed on the New York Stock Exchange. Its executives are paid millions of dollars each year. Its biggest initial investor was the junk bond king Michael Milken. Numerous articles in publications such as the New York Times and the Washington Post have documented high student attrition, low teacher wages, low student test scores and low graduation rates. Yet the company is profitable.

Risk Five: Money in Edtech

The tech industry wields its money in dubious ways to peddle its product. The market for technology is burgeoning, and a large industry is hovering around the schools, eager for their business. In November 2017, the New York Times published an expose of the business practices of the tech industry in Baltimore County. It documented payola, influence peddling and expensive wining and dining of school officials, which resulted in nearly $300 million of spending on computers that received low ratings by evaluators and that were soon obsolescent. This, in a district that has neglected the basic maintenance of some of its buildings.

The greatest fear of parents and teachers is that the tech industry wants to replace teachers with computers. They fear that the business leaders want to cut costs by replacing expensive humans with inexpensive machines, that never require health care or a pension. They believe that education requires human interaction. They prefer experience, wisdom, judgment, sensibility, sensitivity and compassion in the classroom to the cold, static excellence of a machine.

5. Hacking and Ethical Hacking



What is Hacking

Computer Hacking refers to breaking into someone's system for personal or commercial gains. Hackers also called Pirates, use various tools to cause damage to information and assets.

What is Ethical Hacking

Ethical Hacking refers to the methodology adopted to find loopholes in Information systems. Same tools are used by both hackers and Ethical Hackers. The only difference is that hackers use tools to steal or destroy information whereas Ethical Hackers use same tools to safeguard systems from "hackers with malicious intent".Ethical Hacking is legal and hacking is done with permission from the client.

Types of Hackers

Blackhat Hackers

People who break into systems with malicious intent are also called Pirates. They can be further classified into following categories.

Phreakers. Pirates who do Piracy through Telephone Network.

Crackers. People who use software patches to remove security of original software.

Carders. These Pirates attack electronic cards like ATM or credit cards to obtain user information.

Script Kiddies. Young Pirates use a software program to sabotage computer systems just for fun.

White Hat Hackers

People who use hacking tools to prevent information systems and assets from bad-intent of hacking. They are also called Ethical hackers

Grey Hat Hackers

This category of hackers falls in between good and bad hackers. For example, certain white Hat hackers at some time back were Black Hat Hackers and vice-versa

Categories of Hacking

1) Windows Hacking
2) Database Hacking
3) Web Hacking
4) Network Hacking

Windows Hacking

Hackers can attack windows in many ways. Most common of them are:

1) Corrupt the Windows Registry.
2) Hack the Administrator user account.
3) Change the appearance of the desktop.

So it is advisable to take backup of your windows registry from time to time. Steps are:

Go to **Run** tab Type **Regedit** press **Enter** and a new screen showing registry configuration will appear. Now go to **File** and select **export** option to **save** file where you want.

In case, user account "Admin" is hacked, you can use following software tools to recover your admin password.

1) ERD Commander
2) Dream Pack PL
3) Admin Hack

One can download this software for respective windows versions and make bootable CD to recover the admin password.

To protect administrator password from being hacked, one should deploy strict security policies in operating systems. In windows operating systems, Go to **Control Panel** Look for **administrative tools** then **Security Policy** and **disallow** any password changes.

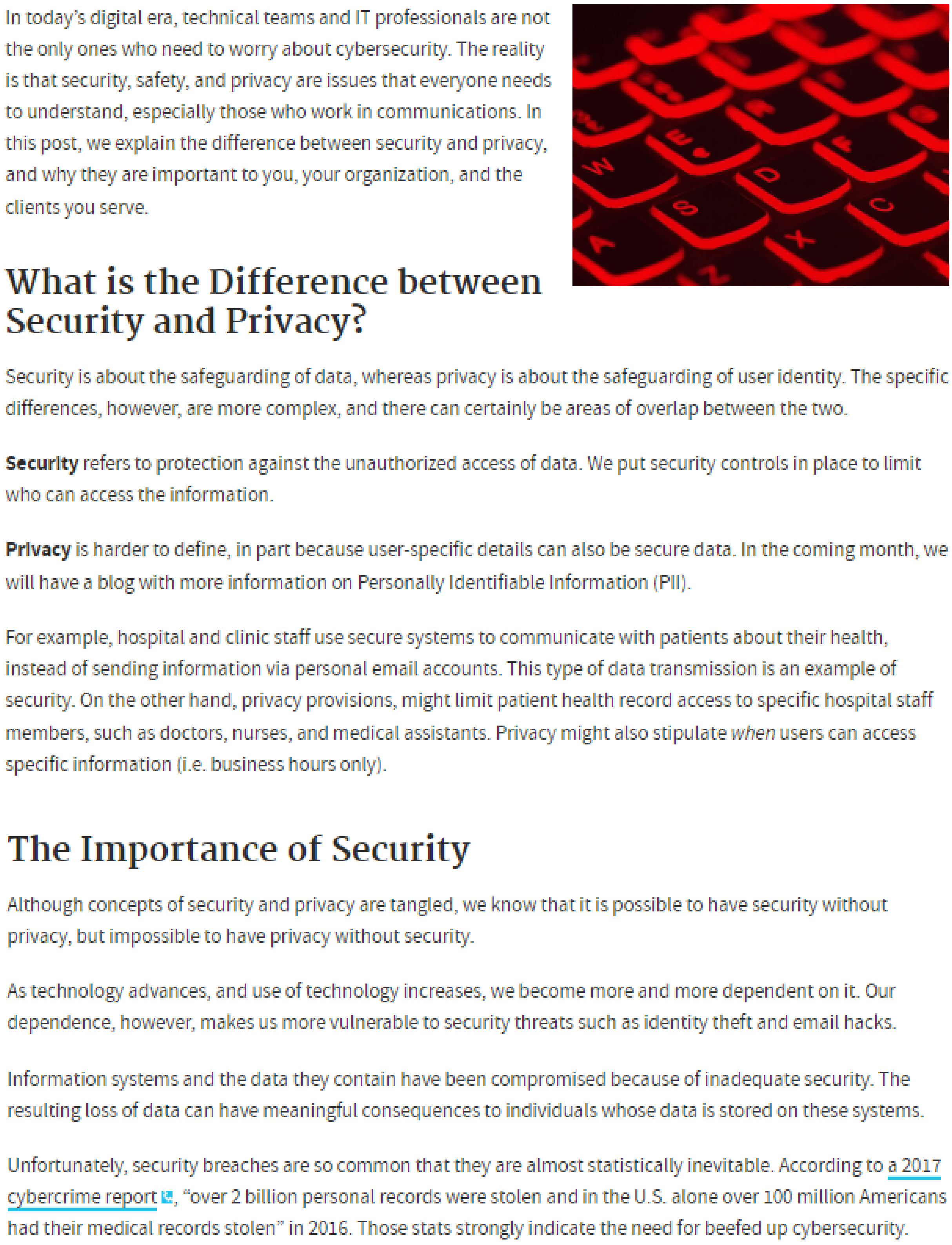
Other methods of Hacking

- ***Phishing.*** It is a technique used by hackers to hack passwords of emails or e-commerce websites. People usually fall prey to phishing emails they get in their inbox. The emails appear to be legitimate and trustworthy and fall prey to them. The hacker asks users to log in from their mail IDs and then redirected to his website where they collect user login information.
- ***Botnets***. Sometimes hackers do not carry out hacking manually rather they make use of robots. The robots do hacker’s job automatically
- ***Keyloggers.*** This is a new technique adopted by hackers to steal information. Also called hardware key logger, a device is installed on one of the ports of the motherboard. Whatever user types in from the keyboard is recorded.

What to do if been hacked?

- **Cut-Off your Internet connection.** If you suspect that you are being hacked, the first thing to do is to cut-off internet from your system in order to stop the further intrusion.
- **Turn On Firewall.** Sometimes we turn off windows firewall in order to install some software. From a security point of view , we should always turn on firewalls. Hardware firewall is another good option to install. It acts as an isolator between external Network and your internal systems.
- **Contact your Internet Service Provider.** It is a good practice to contact your ISP in the case of hacking because they have their own policy and guidelines for any malicious intrusion.

6. Information Security and Privacy (Cyber Security)



In today's digital era, technical teams and IT professionals are not the only ones who need to worry about cybersecurity. The reality is that security, safety, and privacy are issues that everyone needs to understand, especially those who work in communications. In this post, we explain the difference between security and privacy, and why they are important to you, your organization, and the clients you serve.

What is the Difference between Security and Privacy?

Security is about the safeguarding of data, whereas privacy is about the safeguarding of user identity. The specific differences, however, are more complex, and there can certainly be areas of overlap between the two.

Security refers to protection against the unauthorized access of data. We put security controls in place to limit who can access the information.

Privacy is harder to define, in part because user-specific details can also be secure data. In the coming month, we will have a blog with more information on Personally Identifiable Information (PII).

For example, hospital and clinic staff use secure systems to communicate with patients about their health, instead of sending information via personal email accounts. This type of data transmission is an example of security. On the other hand, privacy provisions, might limit patient health record access to specific hospital staff members, such as doctors, nurses, and medical assistants. Privacy might also stipulate *when* users can access specific information (i.e. business hours only).

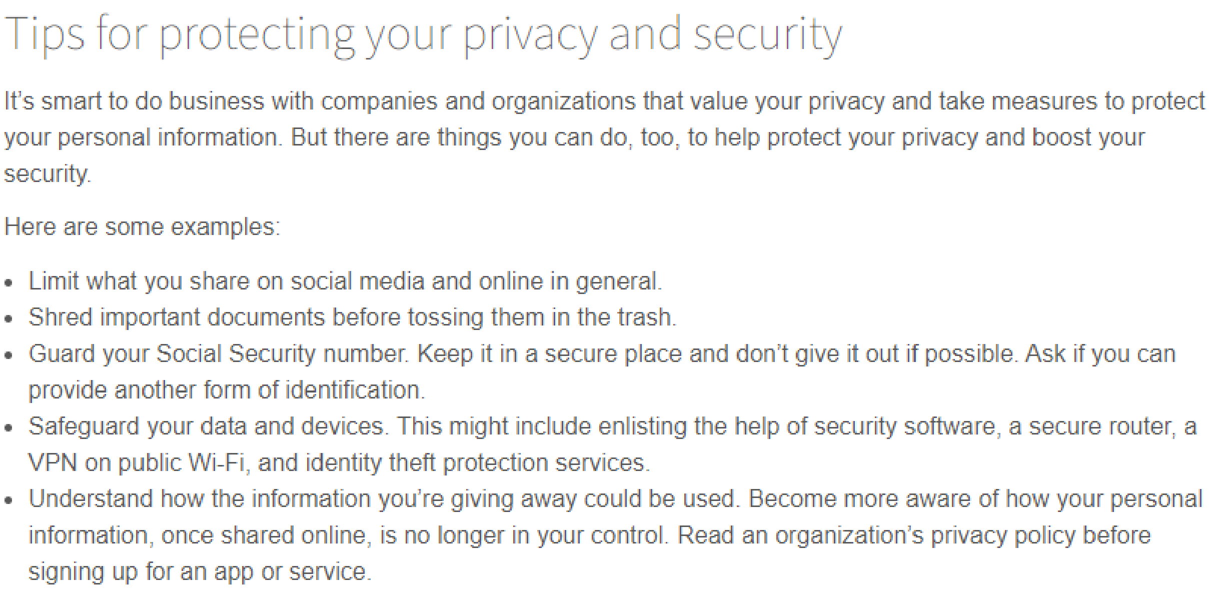
The Importance of Security

Although concepts of security and privacy are tangled, we know that it is possible to have security without privacy, but impossible to have privacy without security.

As technology advances, and use of technology increases, we become more and more dependent on it. Our dependence, however, makes us more vulnerable to security threats such as identity theft and email hacks.

Information systems and the data they contain have been compromised because of inadequate security. The resulting loss of data can have meaningful consequences to individuals whose data is stored on these systems.

Unfortunately, security breaches are so common that they are almost statistically inevitable. According to a 2017 cybercrime report, "over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen" in 2016. Those stats strongly indicate the need for beefed up cybersecurity.



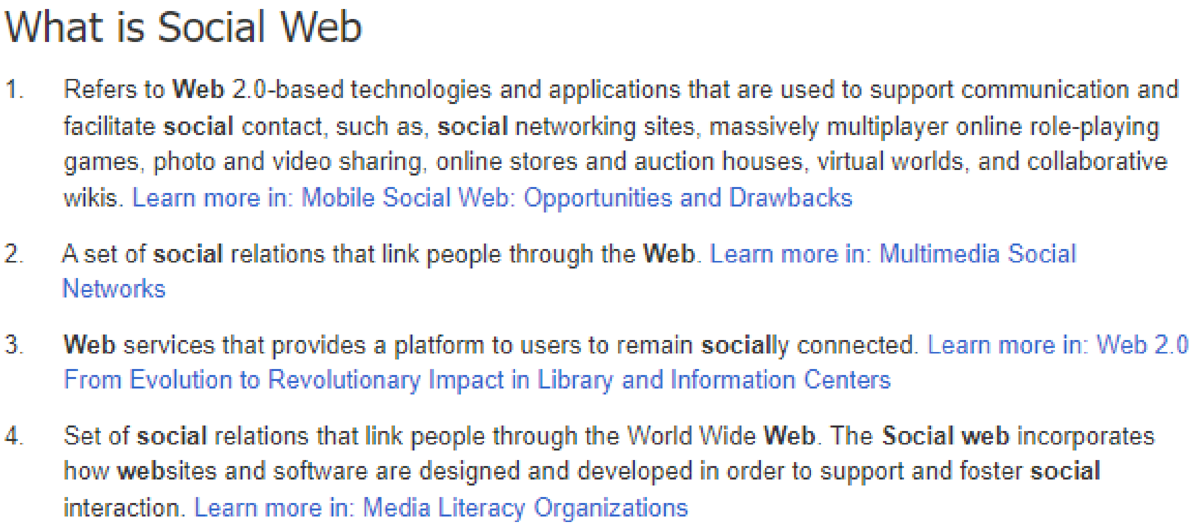
Tips for protecting your privacy and security

It's smart to do business with companies and organizations that value your privacy and take measures to protect your personal information. But there are things you can do, too, to help protect your privacy and boost your security.

Here are some examples:

- Limit what you share on social media and online in general.
- Shred important documents before tossing them in the trash.
- Guard your Social Security number. Keep it in a secure place and don't give it out if possible. Ask if you can provide another form of identification.
- Safeguard your data and devices. This might include enlisting the help of security software, a secure router, a VPN on public Wi-Fi, and identity theft protection services.
- Understand how the information you're giving away could be used. Become more aware of how your personal information, once shared online, is no longer in your control. Read an organization's privacy policy before signing up for an app or service.

7. What is Social Web?



What is Social Web

1. Refers to **Web** 2.0-based technologies and applications that are used to support communication and facilitate **social** contact, such as, **social** networking sites, massively multiplayer online role-playing games, photo and video sharing, online stores and auction houses, virtual worlds, and collaborative wikis. Learn more in: Mobile Social Web: Opportunities and Drawbacks

2. A set of **social** relations that link people through the **Web**. Learn more in: Multimedia Social Networks

3. **Web** services that provides a platform to users to remain **social**ly connected. Learn more in: Web 2.0 From Evolution to Revolutionary Impact in Library and Information Centers

4. Set of **social** relations that link people through the World Wide **Web**. The **Social web** incorporates how **web**sites and software are designed and developed in order to support and foster **social** interaction. Learn more in: Media Literacy Organizations

5. **Web**sites and mobile applications that agent's use to communicate and participate in a digital culture. Agents on the **social web** often use text, images, and videos as a means of communicating and interacting. Learn more in: Seven Traits of Personal Learning Environments for Designing Quality Online Learning Programs: A Systems View of Connectedness

6. A perceived evolution of the **Web** in a direction that is driven by 'collective intelligence,' realized by information technology, and characterized by user participation, openness, and network effects. Learn more in: Embracing the Social Web for Managing Patterns

7. is a type of **Web** application which emphasizes the end-users involvement, the relationships between them and the shared interests of the community Learn more in: A Model-Driven Engineering Approach for Defining Rich Internet Applications: A Web 2.0 Case Study

8. Also known as **web** 2.0, the **social web** is part of a set of applications or **web**sites with the same characteristics and capabilities that offer users the potential to create content. Learn more in: The Evolutional Genesis of Blogs and the Integration of Communication Networks

9. The perceived evolution of the **Web** in a direction that is driven by 'collective intelligence,' realized by information technology, and characterized by user participation, openness, and network effects. Learn more in: Using Wiki for Managing Knowledge in Agile Software Development

10. Also known as **Web** 2.0, the **Social Web** is an aggregation of **social** interaction and collaboration technologies, including blogs, podcasts, wikis, **social** networking, photo and video sharing, and simulated 3-D virtual worlds. Learn more in: Social Capital, Social Networks, and the Social Web: The Case of Virtual Volunteering

11. A set of **social** relations that link people through the World Wide **Web**. The **Social Web** encompasses how **Web**sites and software are designed and developed in order to support and foster **social** interaction. Learn more in: Social Machines

12. A perceived evolution of the **Web** in a direction that is driven by 'collective intelligence,' realized by information technology, and characterized by user participation, openness, and network effects. Learn more in: A Knowledge Management Model for Patterns

13. An umbrella term that includes **social** media and **social** networking sites, like Facebook and MySpace. Learn more in: Leveraging User-Specified Metadata to Personalize Image Search

14. The perceived evolution of the **Web** in a direction that is driven by 'collective intelligence,' realized by information technology, and characterized by user participation, openness, and network effects. Learn more in: Developing a Glossary for Software Projects

15. Is a set of **social** relations that link people through the World Wide **Web**. Learn more in: From Mainframe to Cloud

16. The perceived evolution of the **Web** in a direction that is driven by 'collective intelligence,' realized by information technology, and characterized by user participation, openness, and network effects. Learn more in: Using Wiki for Agile Software Development

17. The **web social** is a environment that brings people together to talk, share ideas and common interests, or make new friends, for collaboration and sharing of data. Learn more in: Smart Communities: Promoting Scientific Publications Through Academic Social Networks

8. Social responsibilities of IT Professional

Fortunately, this new cyber world has also given rise to a fast-growing new breed in the workforce that includes direct and indirect IT (cyber) professionals. According to US Department of Labor (DOL), IT jobs are projected to grow 12 percent from 2014 to 2024, faster than the average for all occupations. Many of these professionals, from all industries, are helping to build a useful and productive society. However, the cybersecurity environment is constantly changing, so the methods to protect ourselves must evolve with those changes. Most employees have the benefit of cybersecurity awareness resources through their work. However, what about small businesses, mom and pop operations, the unemployed, and retirees? As IT professionals, both direct and indirect (those with IT skills but whose primary roles are not IT), do we have a social responsibility? I believe we do! In addition to our job duties, what can we, as individuals, do for the betterment of society? Some ideas are listed below.

Cybersecurity – A major area in which IT professionals can do significant good in the community is in cybersecurity and cybersecurity awareness. IT professionals can offer guidance and expertise ranging from coding or app-writing clinics for juniors and seniors in high schools to cybersecurity awareness for various groups such as community groups, churches, small businesses, chambers of commerce, etc. Two especially vulnerable groups that can benefit from the latter activities are K-12 children who are targets on the internet and social media for sexual predators, and retirees who are generally dependent on their retirement assets but with very little knowledge to protect themselves and their assets online from cyber criminals.

Promote STEM – Seek out opportunities to present to schools and groups to encourage young people in K-12, especially the under-represented groups, including minorities and women,to consider careers in theScience, Technology, Engineering, and Mathematics (STEM) fields; help provide a window into your professional world.

Help your colleagues – Assist colleagues within the organization to leverage technology to improve processes and/or explore innovative opportunities which are especially useful in times of lean budgets. If done collaboratively and with grace, this action could also help IT professionals build strong lasting relationships across departments/units within the organization.

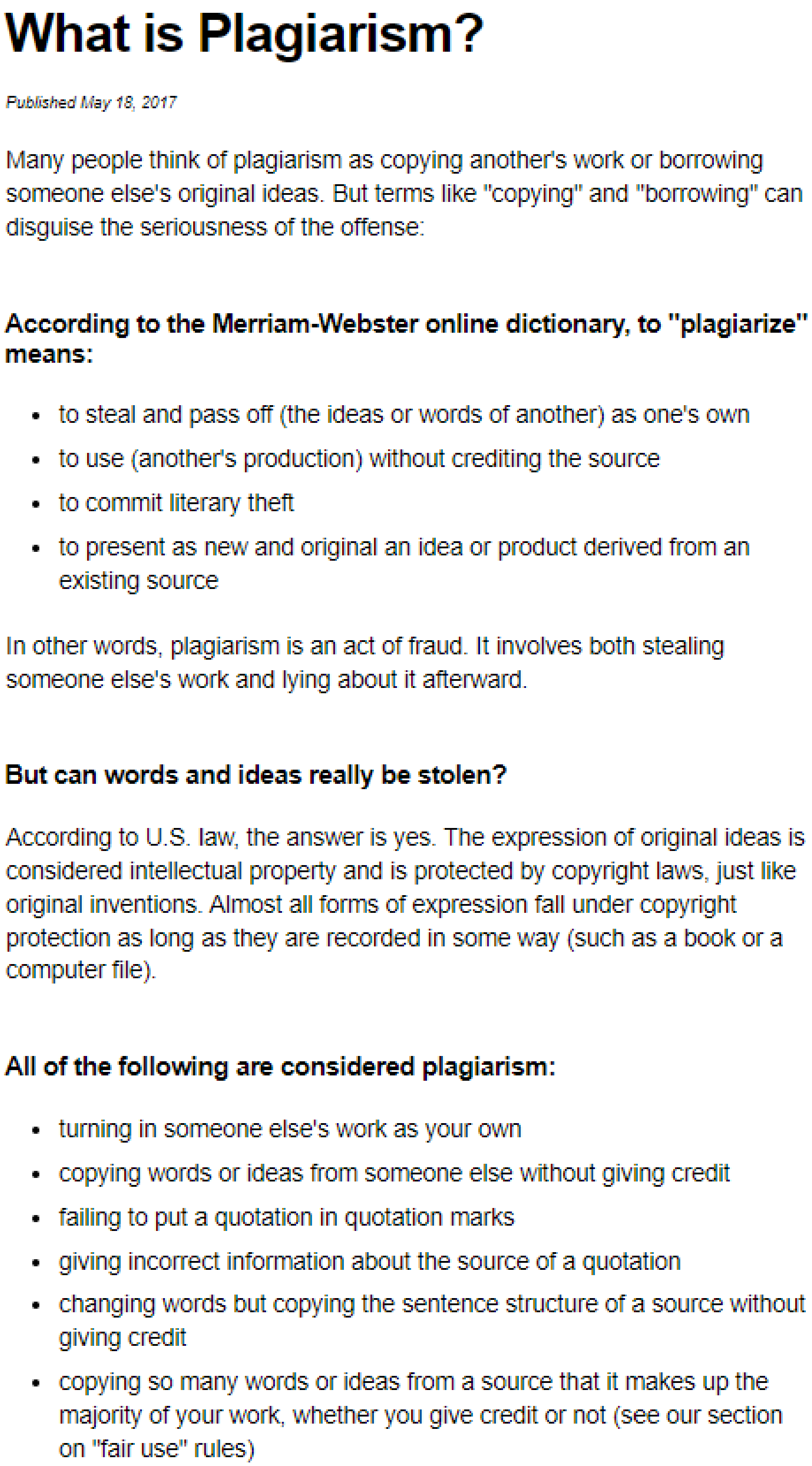
Participate – Participate in established industry security organizations such as the Multi-State Information Sharing & Analysis Center (MS-ISAC), Information Sharing and Analysis Organizations (ISAOs), InfraGard (partnership between the FBI and members of the private sector), Stop- Think-Connect (national public awareness campaign by Dept. of Homeland Security), or in other professional technology organizations.

Go beyond your comfort zone – Leverage volunteers with subject matter knowledge in other fields, e.g. environmental care, animal welfare, or betterment of human living conditions. Help them go further in their volunteer activities using your IT skills such as web, systems design, database, programming, security, or IoTs.

Share your passion – Be a mentor in and for your field.

Spread your knowledge – A major social contribution of IT professionals is the sharing of knowledge and skills through voluntary participation in professional organizations, seminars, conferences, user groups, standards organizations, advisory groups, one-on-one consultations, etc. Over the years, I have had the privilege of working with or knowing numerous successful IT professionals who are leaders in their fields. The one major common attribute of these passionate individuals is their willingness to collaborate with colleagues and others.

9. What is Plagiarism?



What is Plagiarism?

Published May 18, 2017

Many people think of plagiarism as copying another's work or borrowing someone else's original ideas. But terms like "copying" and "borrowing" can disguise the seriousness of the offense:

According to the Merriam-Webster online dictionary, to "plagiarize" means:

- to steal and pass off (the ideas or words of another) as one's own
- to use (another's production) without crediting the source
- to commit literary theft
- to present as new and original an idea or product derived from an existing source

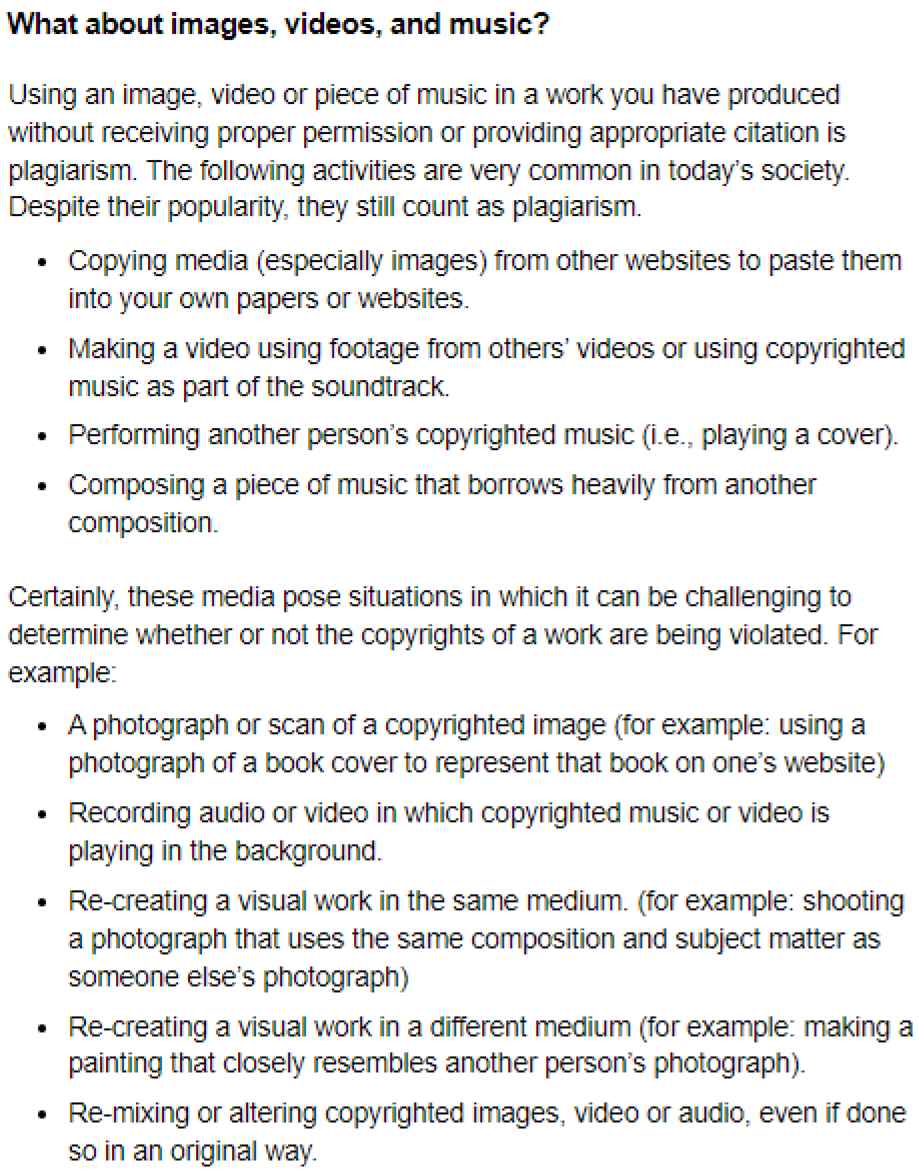
In other words, plagiarism is an act of fraud. It involves both stealing someone else's work and lying about it afterward.

But can words and ideas really be stolen?

According to U.S. law, the answer is yes. The expression of original ideas is considered intellectual property and is protected by copyright laws, just like original inventions. Almost all forms of expression fall under copyright protection as long as they are recorded in some way (such as a book or a computer file).

All of the following are considered plagiarism:

- turning in someone else's work as your own
- copying words or ideas from someone else without giving credit
- failing to put a quotation in quotation marks
- giving incorrect information about the source of a quotation
- changing words but copying the sentence structure of a source without giving credit
- copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not (see our section on "fair use" rules)



What about images, videos, and music?

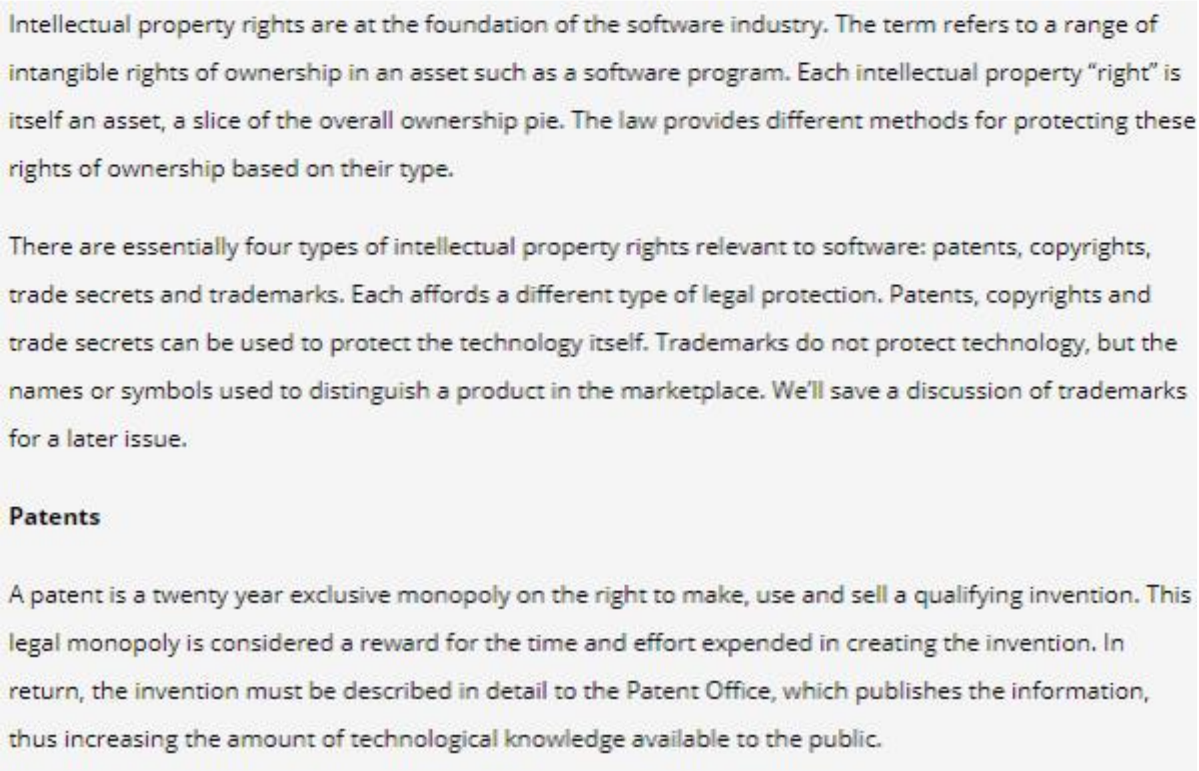
Using an image, video or piece of music in a work you have produced without receiving proper permission or providing appropriate citation is plagiarism. The following activities are very common in today's society. Despite their popularity, they still count as plagiarism.

- Copying media (especially images) from other websites to paste them into your own papers or websites.
- Making a video using footage from others' videos or using copyrighted music as part of the soundtrack.
- Performing another person's copyrighted music (i.e., playing a cover).
- Composing a piece of music that borrows heavily from another composition.

Certainly, these media pose situations in which it can be challenging to determine whether or not the copyrights of a work are being violated. For example:

- A photograph or scan of a copyrighted image (for example: using a photograph of a book cover to represent that book on one's website)
- Recording audio or video in which copyrighted music or video is playing in the background.
- Re-creating a visual work in the same medium. (for example: shooting a photograph that uses the same composition and subject matter as someone else's photograph)
- Re-creating a visual work in a different medium (for example: making a painting that closely resembles another person's photograph).
- Re-mixing or altering copyrighted images, video or audio, even if done so in an original way.

10. Intellectual property and Software laws

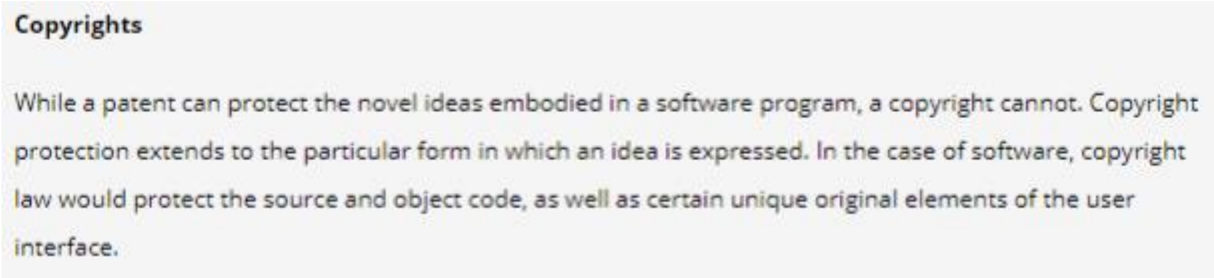


Intellectual property rights are at the foundation of the software industry. The term refers to a range of intangible rights of ownership in an asset such as a software program. Each intellectual property "right" is itself an asset, a slice of the overall ownership pie. The law provides different methods for protecting these rights of ownership based on their type.

There are essentially four types of intellectual property rights relevant to software: patents, copyrights, trade secrets and trademarks. Each affords a different type of legal protection. Patents, copyrights and trade secrets can be used to protect the technology itself. Trademarks do not protect technology, but the names or symbols used to distinguish a product in the marketplace. We'll save a discussion of trademarks for a later issue.

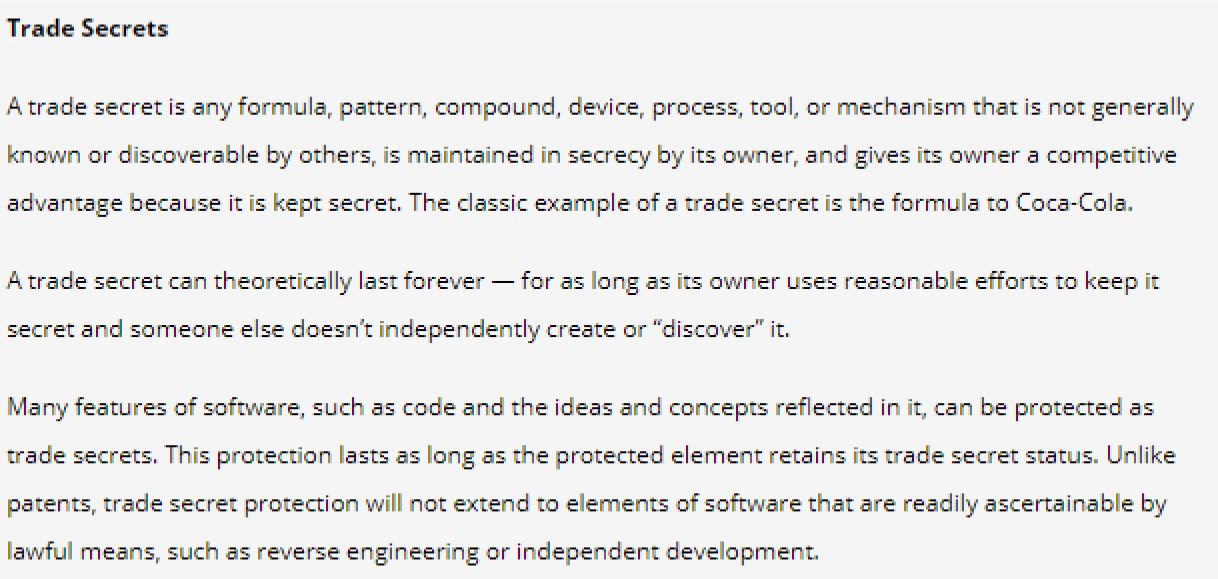
Patents

A patent is a twenty year exclusive monopoly on the right to make, use and sell a qualifying invention. This legal monopoly is considered a reward for the time and effort expended in creating the invention. In return, the invention must be described in detail to the Patent Office, which publishes the information, thus increasing the amount of technological knowledge available to the public.



Copyrights

While a patent can protect the novel ideas embodied in a software program, a copyright cannot. Copyright protection extends to the particular form in which an idea is expressed. In the case of software, copyright law would protect the source and object code, as well as certain unique original elements of the user interface.



Trade Secrets

A trade secret is any formula, pattern, compound, device, process, tool, or mechanism that is not generally known or discoverable by others, is maintained in secrecy by its owner, and gives its owner a competitive advantage because it is kept secret. The classic example of a trade secret is the formula to Coca-Cola.

A trade secret can theoretically last forever — for as long as its owner uses reasonable efforts to keep it secret and someone else doesn't independently create or "discover" it.

Many features of software, such as code and the ideas and concepts reflected in it, can be protected as trade secrets. This protection lasts as long as the protected element retains its trade secret status. Unlike patents, trade secret protection will not extend to elements of software that are readily ascertainable by lawful means, such as reverse engineering or independent development.

THE END!