الجامعة الإسلامية العالمية شيتاغونغ
International Islamic University Chittagong

PREPARED FOR:

Course Code: CSE-6261

Course Title: Computer Ethics and Cyber Law.

SUBMITTED TO:

Dr. Md. Monirul Islam

Professor

Department of CSE
International Islamic University, Chittagong

SUBMITTED BY:

Name : Amena Akhter Chowdhury

ID No : MC-181206

Semester : 2nd

Department : CSE

Submission Date: 9 July, 2019

Table of Contents

Introduction

Web privacy is the privacy and security level of personal data published via the Web. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.

Web privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development.

Virtually all business, most government agencies and many individuals now have web sites. It's important to keep secured that websites. To save the data stored in the online through web, privacy to protect that data is very much important. People with only a casual concern for web privacy need not achieve total anonymity. Internet users may protect their privacy through controlled disclosure of personal information. The revelation of IP addresses, non-personally-identifiable profiling, and similar information might become acceptable trade-offs for the convenience that users could otherwise lose using the workarounds needed to suppress such details rigorously. On the other hand, some people desire much stronger privacy. In that case, they may try to achieve *Internet anonymity* to ensure privacy — use of the Internet without giving any third parties the ability to link the Internet activities to personally-identifiable information of the Internet user. In order to keep their information private, people need to be careful with what they submit to and look at online.

Background History

Online security hasn't been creating in the straight line and we didn't have the present insurance when we had associated that first PC to the web. Not only hackers are the dangers to your online privacy as some recent scandals showed us that some government agencies monitor your online history. You might have thought that you had found the way on how to protect your private data online. The concept online privacy had become to be an issue in early 90s when users started their journey through the web. The Internet wasn't that widespread during this era as only available way of connection is dial–up. As with most new technology the biggest benefit was that there weren't enough skilled computer users who will use the technology to steal your personal information.

There were not many sites that required that you type in your personal info. The main that required this way of verification are MSN (Microsoft Service Network) and AOL (America Online), even these did not care too much about online privacy as everything was new and unexplored. There had been a change in 1994 as some companies started to deal with issues relate to the online privacy and send weekly emails to their customers. First civil lawsuits regarding this matter were also recorded during this year.

We all know that the internet had become more available in mid 1990s with the introduction of the Windows 95. Computers that were running the Windows 95 were the first to enable their user to connect to the internet without any unnecessary hassle. Internet security had been noticed as a real issue and the combat against illicit sites such as ones that contain child pornography had started. The US Senate had also passed laws which forbid the use of internet to manipulate a person who was considered a minor at the time.

Late 90's had brought even stronger computers which were able to run online games and the internet was developing further every day thus people and the government directed their attention to the problems created by online security. Most of these polices dealt with upgrading children safety when they are browsing the web as children were the most venerable and most of them browsed different unrelated things on the web at that time. COOPA was passed and this law had asked from website to ask for the permission of the parent or the guardian if the website wants to gather data about the child under the age of 13, thus a child would have to ask for the permission of the adult to create an online account. This was one of the first legal codes that tried to protect citizens from the possible misuse of their personal data which were stored on online severs and databases.

The beginning of the twenty-first century was the era of the rapid development of the IT technology and every member of the public both companies and individuals benefited from these events.

It was much different than the 9os as more sites required your personal information and they were more sensitive such as credit card details, address, and the description of your habits. Sites had updated their term and conditions policies so users were introduced to the safe keeping polices that they use to keep the data private. Authorities were more involved with the efforts to let the sites know that they need to respect the privacy of every single user; they had also intensified their combat against cybercrimes.

Mid 2000's brought additional challenges to the aforementioned are as millions of people across the globe were able to connect to the internet and most of them had an ADSL connection or a wireless router. Many people used online shopping sites such as Amazon and EBay thus programmers of certain antivirus software had developed a safe mode which blocks any third party software or an address from connecting to your computer. Just as Facebook, Myspace had required from its user to fill out many personal information along with their pictures. The state of California had passed a law in 2005 which determines on what sort of conditions websites can share your data with third parties.

Description

Web privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Web privacy risks include:

- Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.
- Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.
- Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.
- Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Web privacy violation risks may be minimized, as follows:

- Always use preventative software applications, such as anti-virus, anti-malware, anti-spam and firewalls
- Avoid shopping on unreliable websites
- Avoid exposing personal data on websites with lower security levels
- Clear the browser's cache and browsing history on a consistent basis
- Always use very strong passwords consisting of letters, numerals and special characters

This policy describes the privacy practices on our websites. By "websites" (or "sites") this description refers to groups of pages within the f-secure.com domain. Our online resellers (e.g. Clever bridge AG) have their own privacy policies and are not included in this policy. For our personal data processing practices in general, please see the F-Secure privacy statement. If you are looking for information about how we process your data in a particular service, you may also find our service-specific privacy policies, e.g. that of F-Secure SAFE, relevant to you.

Issues

For years now, Internet privacy is a huge issue. Very few of us opted not to use the Internet and stay in complete anonymity, while the rest of the world chooses to think less about how much of our personal information is out there.

Search engines:

Google the biggest and most used search engine collects a lot of information about its users form basic information like name and birthday to complete history of our browser. The main reason for such features is to create personalized user experience, but at the same time it is quite handy for the company to increase revenue by displaying ads in accordance to person's interests. There's no doubt that this is the dream tool of every salesman in the world. Of course, no one is forced to make a purchase, but knowing that this is the way things work; it makes some of us feel used. It is a matter of trust.

A couple of decades ago when the Internet was created, the decrease of our privacy started. Today we face numerous concerns and there are many ways our private information can be jeopardized.

Identity theft:

Millions of people were victims of identity theft which led to financial loss and even legal problems. Almost every website that asks for registration wants our name and birthdate, which is more than enough for experienced hackers to breach our privacy and create damage. Even secured banking applications suffered breaches. Therefore, should be careful when and where we leave data.

Tracking:

Every website you visit uses cookies. They are now obliged to notify users about it, so we have to click on "Ok" "Accept" or "Agree" in order to continue. Cookies store a certain amount of data specific to a particular client and website. With this information, server can deliver a specially tailored page for the mentioned user.

The smartphones era brought even bigger privacy issues. Smartphones are based on apps and almost every app out there wants access to your entire phone – contacts, texts, emails, notifications, storage etc. Many people don't think about it or consider such information sharing dangerous but as technology continues to advance and becomes inevitable in everyday life, we are becoming less independent and more prone to be either victimized in some way or simply used as a plain consumer to buy stuff.

Facebook recently announced they are now able to trace even non-users. With the help of "Like" buttons, which are now on every website? They will display ads to people that are not

part of this global social network. Using cookies stored in like buttons and other plugins, they can display relevant ads for non-users as well.

Protection:

There's no way to be completely out of it, but there are several things we can do to avoid complete transparency.

- Use 'turn off' options whenever possible, like in Google's activity tracker.
- You can also block ads on your browser and take extra time to actually read privacy policies.
- Next time you wish to install a new application and if you are not ok with it, you can decide not to use it.

- Use more sophisticated methods for protecting your online identity and communications, like
- Protect your password
- Use Anti-virus
- Use Anti-Spyware
- Care to share files
- Be aware not to fall for scams and phishing attacks
- Report SPAM
- Keep sensitive information safely

Results

Online users must seek to protect the information they share with online websites, specifically social media. In today's Web individuals have become the public producers of personal information. We create our own digital trails that hackers and companies alike capture and utilize for a variety of marketing and advertisement targeting. A recent paper claims "privacy is not the opposite of sharing – rather, it is control over sharing." Internet privacy concerns arise from our surrender of personal information to engage in a variety of acts, from transactions to commenting in online forums. Protections against invasions of online privacy will require individuals to make an effort informing and protecting them via existing software solutions, to pay premiums for such protections or require individuals to place greater pressure on governing institutions to enforce privacy laws and regulations regarding consumer and personal information. Over the past few years, internet spam has become an annoying and progressive problem for many consumers. Because internet users are now concerned about having their personal information scattered about, the inclusion of a Privacy Policy on your website has become a very important factor. Internet users are now, more than ever, concerned about who sees their information and how their personal information may be used when they visit your site. They want to ensure that their identifying information will not be sold or used in any marketing efforts that they have not solicited personally. Your personal privacy on the web might be less secure than you think. Web browsing habits are tracked via cookies, search engines routinely change their privacy policies, and there are always challenges to web privacy by both private and public organizations.

My Comments

A good web safety rule of thumb is to avoid filling out forms that require personal information in order to keep anything from being entered into the public, searchable record, aka web results. One of the best ways to get around companies getting your personal information is to use a disposable email account — one that you don't use for personal or professional contacts — and let that be the one that filters things such as contest entries, websites that require registrations, etc.

Think carefully before following links, opening files, or watching videos sent to you by friends or organizations. Watch for signs that these might not be for real: these include misspellings, lack of secure encryption (no HTTPS in the URL), and improper grammar.

Keeping your computer safe from harmful content on the web is simple with a few precautions, such as a firewall, appropriate updates to your existing software programs (this ensures that all security protocols are kept up to date), and antivirus programs. It's also important to know how to properly scan your computer for malware so there isn't something unsafe lurking around in the background as you're having fun on the web.

A privacy policy refers to a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. A privacy policy fulfills a legal requirement to protect a customer or client's privacy. Not only businesses but websites also need to put up a privacy policy so as to leverage its benefits. Hosting providers protect the server your website is on, not the website itself. You can think of the website-host relationship like an apartment building: management provides security for the whole building, but it's up to each occupant to lock their door.

Summary:

Web privacy is a developing worry with kids and the substance they can see. Besides that, numerous worries for the security of email, the powerlessness of web clients to have their web use followed, and the gathering of individual data likewise exist. These worries have started to bring the issues of web protection under the watchful eye of the courts and judges. While the number of web sites using Privacy Policies has definitely increased over the past few years, the problem is that many of these sites simply copy policies found on other websites. In order to reassure your website visitors, you should ensure that your Privacy Policy page is completely unique. You cannot simply borrow words from another site and reassure your visitors. The policies that your website and/or company adhere to are the ones that you want to have listed for your website visitors to see. When you simply copy what another site has posted you may not be accurately depicting the actual policies of your own company. You should also be aware that even when sent data is stripped of personally identifiable information.

References

1. Stein, Web Security: A Step-By-Step Reference Guide (Addison-Wesley, 1998).
2. Rubin, Geer and Ranum, *Web Security Sourcebook: A Complete Guide to Web Security Threats and Solutions* (Wiley, 1997).
3. Howard and LeBlanc, *Writing Secure Code, second edition* (Microsoft Press, 2002).
4. Rubin, White-Hat Security Arsenal.
5. Michal Zalewski (2011) The Tangled Web: A Guide to Securing Modern Web Applications.