edexcel
advancing learning, changing lives

Project Proposal form

Learner Name _____ Learner number _____

Centre Name _____ Centre Number _____

Teacher Assessor _____ Date 20/03/2009

Unit Project

Proposed project title "Will the Internet ever be secure?"

Section One: Title, objective, responsibilities

Title or working title of project (in the form of a question)

For the title of my project, I have selected the question: "Will the Internet ever be secure?".

Project objectives (eg, what is the question you want to answer? What do you want to learn how to do? What do you want to find out?):

The objectives and aims of my project is to better help me learn the practise of research, and how best to go about it (whether asking at libraries), and also to understand the question I have picked in more detail, so I can better cope with Internet security myself.

If it is a group project, what will your responsibilities be?

N/A

Section Two: Reasons for choosing this project

Reasons for choosing the project (eg, links to other subjects you are studying, personal interest, future plans, knowledge/skills you want to improve, why the topic is important):

The reason I chose this question for my project because I have always had a fascination with Internet security, and computer security, and I think the question is very relevant with the modern world, and what has happened with data loss. I think this question will improve my knowledge of security, and the risks involved if you have little or none.

Section Three: Activities and timescales

Activities to be carried out during the project (eg, research, analysis, writing, preparing for the presentation, etc):	How long this will take:
My activity and timescale are located on pages: Time Plan - P.g 1-2 Activity log is after this. All of my activities are located on these pages, so I have	

Milestone one: 20th April

Target date (set by tutor-assessor):

Milestone two: 8th May

Target date (set by tutor-assessor):

Section Four: Resources

What resources will you need for your research, write up and presentation (eg, libraries, books, journals, equipment):
For my research, I will need books that deal with security as well as Internet research and questionnaires that people have filled out.

What your areas of research will cover?
My research will cover Internet security, the history of ciphers (which is part of security) and then questionnaires relating to security.

Comments and agreement from tutor-assessor

Is the learner taking this project as part of the Diploma? (Yes)/No

If yes, which Diploma are they taking? 14-19 Diploma in I.T (Higher)

Comments (optional):

Is project derived from work which has been/will be submitted for another qualification? Yes/(No)

Which qualification (title and unit)? _____

Comments (optional):

I confirm that the project is not work which has been or will be submitted for another qualification and is appropriate.

Agreed: (name) 22nd May 2009 (date)

Comments and agreement from project proposal checker

Comments (optional):

(date) 27/5/9

edexcel
advancing learning, changing lives

Project Activity Log

Learner Name _____ Learner number _____

Centre Name _____ Centre Number _____

Unit Name The Project Unit number Project

Teacher Assessor _____

Proposed project title "Will the internet ever be secure?"

This form should be used to record the process of your project and be submitted as evidence with the final piece of work.
You may want to discuss:

- what you have done (eg, from one week to the next)
- if you are working in a group, what discussions you have had
- any changes that you have or will need to make to your plans
- what resources you have found or hope to find
- what problems you are encountering and how you are solving them
- what you are going to do next

Date	Comments
21st January - 23rd January	I researched questions which I could use as my project, within this time I found 6 questions that I thought would be good enough for my project.
28th January - 1st Febuary	I showed the questions I found and had to choose a question which would be used for my final proposed question. Started an action plan. Carried on with the plan, found some references that could help with my question
4th February - 6th February	Continued with my plan with a better understanding of what was required, added more detail and answering more questions. Finished my final questions ready for the deadline.
11th February - 15th February	Handed in the plan, double checked to make sure it was all correct. Looked on the internet and read some books to help with my research. Made a questionnaire and found out more information for my question.

Date	Comments
20th February - 25th February	Double checked my research in case something was wrong. Handed in my research analysis. Started my essay.
1th April - 20th April	Started my presentation and evaluation of my work
20th April - 8th May	Completed my work and handed it in for the interim. Had my work handed back with what could be improved. Removed the presentation and added some final amendments.
8th May - 21st May	Had more improvements and other things that should be changed, so changed everything accordingly, and added a Project Activity Log.

14-19 Diploma in IT (Higher) – The Project.

To plan what I need to do to evaluate, present and research for my chosen question.

Patrick

2009

Contents Page

Formal Plan:

Date	*Activity*	*Objective*	*Hours spent*	*Comment*
21st January 2009	Research to find the question.	To find an area and questions for the essay.	1.15	Find the unit that will be explored and find questions during the week.
23rd January 2009	Research the questions.	Find questions to do with the area that was chosen.	3	Found 6 questions that I thought would be good and justifiable.
28th January 2009	Show questions and pick one from the list I found.	Clarify questions and decide on one of them.	30 Minutes	Choose a question and decide on what will be my final question.
28th January 2009	Create an action plan of how we're going to research, justify, present and evaluate the question.	Explain what will happen and make a formal plan with dates on how you will conduct research etc.	45 Minutes	Start the plan.
1st February 2009	Create an action plan of how we're going to research, justify, present and evaluate the question.	Carry on with the plan and try to make it as detailed as possible.	2	Carry on with the plan, finding some references that I could use for my question.
4th February 2009	Show moderator what I have done so far with the plan, to clarify my understanding.	Take note of what I did right and wrong and carry on with my plan.	1.15	Continue with plan with a greater understanding of the task, adding more detail and answering more questions.
6th February 2009	Finish action plan.	Finish the final questions that need answering.	2	Finish the final questions ready for the next lesson (deadline).
11th February 2009	Hand in action plan.	Hand in the action plan making some final adjustments.	1.15	Hand in the plan that was made, double checking, making sure that everything was done correctly.
11th February 2009	Research the question.	Start research of the question, using books etc.	1	Look on the internet and read some books.

15th February 2009	Continued research on question.	Continue reading and finding information about the question, and then construct a questionnaire.	2	Constructed the questionnaire and found out some more information.
20th February 2009	Check my research, finding out more information is preferable. Analysis.	Read through everything written down about the research, as well as the questionnaire.	2/3	Double checked all my research
25th February 2009	Hand in research and analysis.	To have had a clear understanding and good level of research.	1.15	Yes.
25th February 2009	Start essay with use of the research. Minimum of 750 words.	Start the essay using research I carried out previously, reference where necessary.	3	Started the essay
10th April 2009	Start presentation and evaluation of my work.	Start my presentation of my work and do the evaluation of what I have done.	1.3	Started evaluation.
20th April 2009	Interim date.	To complete and hand in my work to a satisfactory standard.	1.15	Handed in work to a satisfactory standard
8th May 2009	Amend work	Add any missing work and change layout	1.15	Added a project Activity Log.
12th May 2009	Add work	Add some pages of missing work. I.E the research area	1.0	Added the research area, and changed the look of my research to fit accordingly
22nd May 2009	Final Deadline	Hand in my work by this date		Handed in my work

Plan

Purpose of the question:

The purpose of my question, is to study the possibility of a safe Internet, and to further understand web security and the counter-measures that break it; To evaluate whether or not one will fully overcome the other, and if there are methods already set up to do so.

What do I expect to learn?

I expect to learn about how and why people develop secure web-software, to study how encryption is made and how they help secure the internet, and also study their flaws or how they are broken. To learn about different internet exploits (such as SQL injection) and how they are used and for what purpose, and once these exploits are found how they become publicly available.

Objectives

1. *Main aims/targets/requirements*

To complete this project, a huge deal of research is required, including material from various security books (e.g. Security Engineering by Ross Anderson and Hacking the art of Exploitation by Jon Erikson), as well as web resources, and web pages dedicated to security. A great deal of speculation will have to be necessary, since the question is dealing with future ideas, and thus can only be predicted with both sides of an argument. The aim of this assignment is to help me learn the practise of research and also understanding the question I have picked.

2. *Can they be organised into quantitative/qualitative*

Quantitative involves my questionnaires, which are often used in the essay, this essay will have some points where this will be used, though gathering the information from a wide range of sources is key – seeing as the subject matter is complex without a good understanding of computer security – which might be better explained with numbers and information. So the numbers may be necessary for further understanding, but not paramount to the core of the essay, or the conclusion

3. *How will you know if an objective has been met?*

When the question is justified in a satisfactory way, and that it explains what the question was aimed to do, then the objective will have been met.

4. *What are the inputs, processes and outputs?*

My input is the research, the processes are the thoughts, opinions and ideas, and the output will be the final products.

What skills will you learn?

I will learn skills such as Academic research, collation of data, encryption, exploitation, methods used to prevent hacking and the ingenuity of people designing and programming ways to help security.

What skills do you want to develop?

I want to develop my research and planning skills as well as my knowledge of security.

How will you perform research?

I will perform research by books, internet as well as asking people their opinions via questionnaires.

What resources will you use?

I will use the internet, knowledge of other people and books such as Security Engineering by Ross Anderson.

When will you undertake research?

I will undertake research on my question when I get issued with a dates on when work is due, then, I will do work in accordance to the dates I have to hand work in.

What contingencies have you allowed for? (If things go wrong)

I have a back up of all my work and will make sure that I save my work regularly, as well as having some hand-written work for reference in case of a data loss. I will also have work saved on my email and at the college system, so that I have work in around 5 places in case one goes down.

How will the outcome be presented?

The outcome of what was found will be presented in a formal written report (with a minimum of 750 words), with graphs, as well as a power point presentation. The report should be well written, with good grammar and a clear understanding of the task, the presentation should also contain a clear understanding and be spoken well.

How will you evaluate your outcome?

I will review all of my work, research and methods then separate the good from the bad and ask people what they thought of my work. After I have looked at what I've done in every way possible I will write what I think went well, what could be improved, what was learned and how I did it.

[INTRODUCTION]

Essay Overview

My essay will be taking a look at the question "Will the internet ever be secure?", and in doing so, it will be looking at different aspects of security, from hacking to the preventions made to stop acts of malicious intent. I will aim to answer the question being unbiased, using the information I have gathered from various sources, and coming to the conclusion of the question at the end of my essay.

Introduction - Will the Internet ever be secure?

Since its inception, information security has served but one purpose: to make sure what you relay, doesn't get passed on to others - especially others who might use it to exploit.

Information security has existed before any Von Neumann machine [1], and actually dates back to ancient Rome, where Julius Caesar used it to prevent his battle information from getting in the hands of the enemies. Since the Caesar Cypher [2], security has greatly evolved to the Security mechanisms we use today. Unfortunately, though, so have the methods of breaking such security.

Through the ages, encryption got more complex to counter the advances in decryption technology. For every cypher created through the ages, mechanisms and techniques were made to break them, be it by frequency Analysis methods, Index of Coincidence, Symmetrical Attacks and many others [4]. Though any cypher may be broken at least by using brute force (with the exception of the onetime pad [5]), these methods are often insufficient, since even by their use, long periods of time may be required to break one code. Due to these reasons and more, cryptanalysts are always improving their methods and tools to make breaking a code a more realistic resolution. Both sides of this ongoing battle are always improving their arsenal, so to speak, as to not be caught off guard by the other side.

Upon the invention of computers, even brute forcing for the older cyphers has become something entirely feasible in real time, and due to this, cryptography experience a large advance, seeing the creation of such one sided tools as hashes [6], and private and public keys [7], both methods of asymmetric key cryptography, which allow one side to view the full information, while the other side has no manner of decrypting it through normal means. Later on, even more complex encryption mechanisms such as the DES and AES encryptions [8] were created, the AES considered to be almost unbreakable, and only has been known to be broken once by side-channel attacks. The AES is considered so secure, that the US Government announced that AES may be used to protect even its most classified

information [9]. But even in such cases, counter measures are possible, and even something that is "almost unbreakable", may still be broken.

Computers then became one of the main depositories for personal information around, and as such had to be protected from intruders who could use that information for malicious purposes. For such protection, data classification [10] that requires security clearance in forms of keys or passwords (and sometimes in the form of physical information, such as eye scans or thumbprints), was created, and employed several of the forms of encryption mentioned above. To gather such information, though, malicious users have created such methods as phishing, hacking, and infecting, to better gather information by use of bugs in code or by tricking other users into giving out their data through often ingenious methods. All of these forms often tend to make it easier to obtain data than mere brute force attacks or other complex decryption mechanisms: that is to say, it is always easier to look behind someone's shoulder to read the password directly, than any other method.

This is made easier through the fact that most complex coding contains bugs, and many of these bugs can be exploited. Be it by the popular buffer overflow method [11], or other means of injecting malicious code, access to other computers may be granted, and vital data may be harvested. And when these methods aren't available, fake messages, e-mails, or webpages may be used to trick the user into giving the needed data [12]. Anti-Phishing tools installed into common browsers (such as firefox, and Google Chrome) aid in stopping many of these reported attacks [13]. And anti-viruses try to stop viruses, trojans, and worms from infecting your computer and either destroying, or harvesting your data. The ever-lasting battle between the fields of cryptology and cryptography as detailed above, is what is often called information security.

[*WILL THE INTERNET, EVER BE SECURE?*]

The internet has been adopted as part of our lives, and has had flaws since its beginning. A question has been surrounding the internet since it become part of the public sector, will the internet, ever be secure? This paper will look into this question using research from both qualitative and quantitative sources. Are people aware of the risks using the internet? How are companies developing measures to prevent there being a risk? As software becomes more complex, do the people that break them become even more suited to leaving a hole in internet security? These are some of the questions that have to be asked in order to understand whether or not the internet will ever be secure.

When looking at this question, it gets one to ponder if the internet is insecure, and if it is, what is the biggest flaw surrounding it. With the levels of technology increasing rapidly, the complexity of the technology increases with it[14], this can leave flaws in the technology – others may see this as progress, but the people (engineers) creating the products, have to learn new things, change old things and progress with the technology around them[15].

Over years, hacker has become synonymous with online criminals, or people "stealing" from others, which can be a common misconception, with no help from the media[16], that is not to say that there are not hackers who do use their knowledge for criminal activity, but there are many variations. Without hackers, people wouldn't be able to find the flaws within the technology; "The majority of these people don't have malicious intent and instead help vendors fix their vulnerable software. Without hackers, the vulnerabilities and holes in software would remain undiscovered"[17]. Helping find these flaws, will help patch the holes they found, increasing the security as a whole. Some people would argue a point, that if there were no hackers, then security on the internet would be no problem, although this may be true, it would leave technological advance stagnant, and no progress forward into the unknown [18].

The general public, have only recently been awoken into the realm of internet security, and what dangers it may possess, with information leaking, and identity theft. The media have started to help uncover what may lie beneath, when it comes to a home user browsing the internet, it will often lead lull them into a false sense of security – what can't be seen, can cause no problems – this is often the main problem with security on the internet; awareness and knowledge[19].

Tools are developed for the home user (such as antivirus and firewalls), and often come as standard, or even free packages when they buy computers, but these tools again, lull people into a false sense of security. They don't explain to the user what their purpose is, and what methods the user could take to prevent such things as viruses. Things such as internet browsers, can also play to security strength, and some of the features included, such as the padlock symbol or the HTTPS with a

yellow search frame. But with a lack of knowledge using the browsers, can again lead to their downfall[20].

Confidence can be another major downfall when it comes to security for the internet, if your company is too over-confident with a product, and how secure it is, it can lead to people wanting to figure out a way to break it[21].

Security on the internet will always be a race, with companies developing methods to stop hackers, viruses etc, and then the hackers eventually overcoming the security, forcing the companies to find other ways to stop the new flaws. It will be a continuous cycle, with more and more complexity, with every advancement. This will eventually end, where there can be no more possible advancements, suffice it to say, the internet as we know it today, will never be fully secure.

Developing a new internet, that uses brand new technology, which is unknown to hackers, will restart the internet security race back to the start, but in turn, the hackers will start learning new methods for the new internet and the security race will start all over again, until there are no further steps to take.

The internet will be secure, for a period of time, up until someone breaks the security, so there will always be periods of time where something will not be able to be broken, but better measures need to be in place for the general computer user, to understand how to keep themselves secure, and others when using the internet. In essence, the internet won't ever be secure, because although technology is what's helping making it secure, its technology that is also making it insecure.

[19][20] See questionnaires in appendix 1

[14][15][21][16][17][18] See research appendix 2

[Evaluation]

The question that was asked in the essay brought up some good research, and was a good question relating to how secure one of the most wide-spread pieces of technology is today.

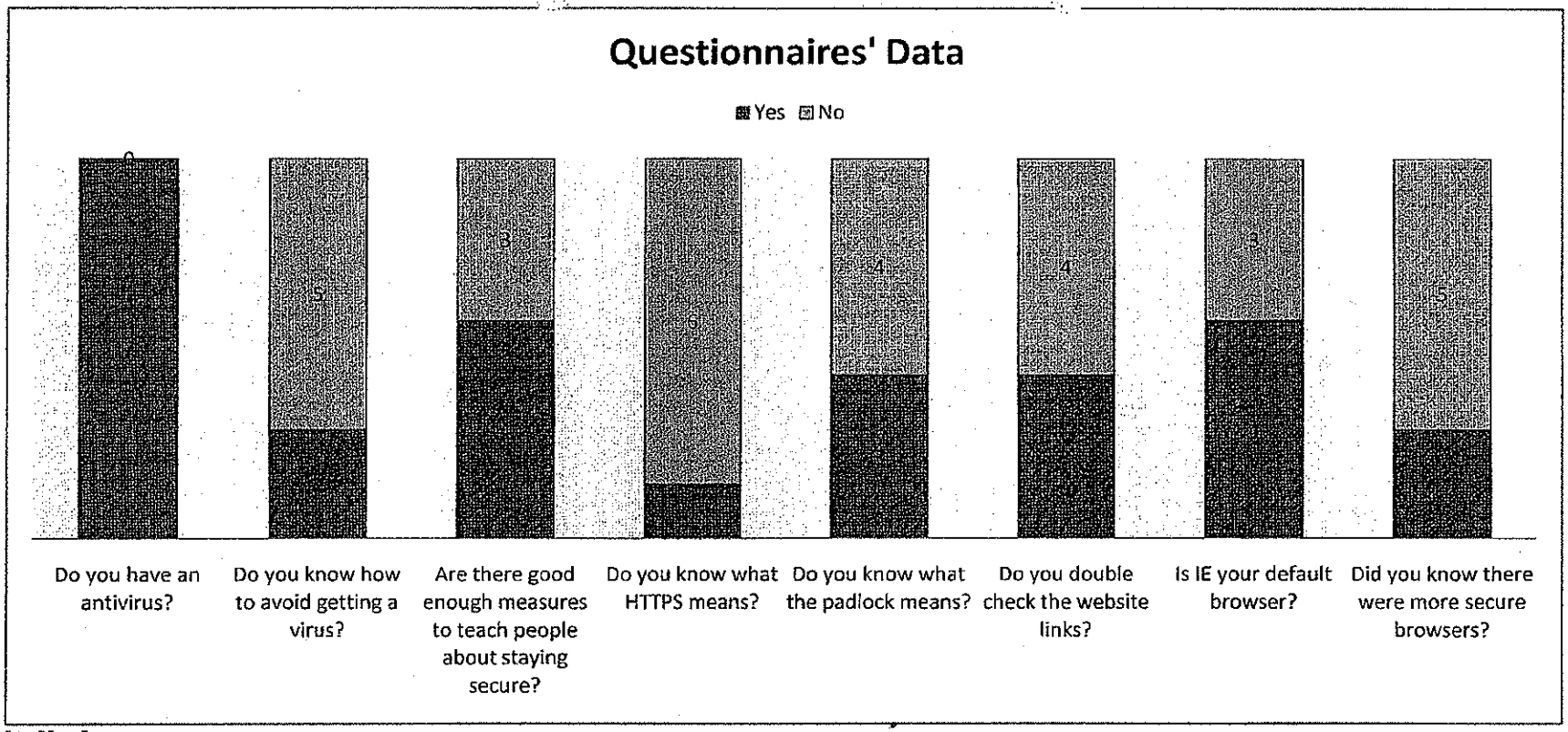
The research was quite hard, because there is a lot of information surrounding the internet in books and online, which made dissecting it quite hard, to find the necessary information that could be used within my essay. I read through some books, which had lots of pages, and extracted the best information that I could use within my essay. Although this was hard work, I feel it gave me some of the best information out of all of my research.

The questionnaires I did were handed out to a variety of people, but some didn't take them seriously and I disregarded the bad ones, which left me with a few good ones. I believe the questionnaires themselves were good, but I could have asked more people to get a wider opinion.

Time management could have gone a bit better, but in the end I had gotten all the work done, and finished to a high quality.

The essay went well, and I feel I put in a lot of good information from the research I had previously carried out. I could have planned my essay, which would have made writing it a lot easier on myself, but, in the end it worked out well and answered the question to a good detail.

[*Research area*]



[19][20]

After I collated all my data into a bar chart, I could see that all of the people I asked had an antivirus; this proves that there is a basic understanding of staying secure when using the internet. After that people generally had no idea how to avoid getting a virus (not visiting weird websites, having script-blockers and email-scanners), which should be basic knowledge, and still a lot of people don't know how, and it should be up to the government to implement adverts or leaflets about staying secure.

The next two questions raised a key point, that 4 out of the 7 people

Research – Will the internet ever be secure?

[14][15][21]

Ten years ago the inhabitants of the different islands in the security archipelago all had huge confidence in their products. The cryptologists believed that certain ciphers couldn't be broken; the smartcard vendors claimed that probing out crypto keys held in their chips was absolutely physically impossible; and the security printing people said holograms couldn't be forged without a physics PhD and $20 m worth of equipment. At the system level, too, there was much misplaced confidence. The banks claimed that their automatic teller machines could not even conceivably make a mistaken debit; the multilevel secure operating systems crowd sold their approach as the solution for all system protection problems; and people assumed that a security evaluation done by a laboratory licensed by a developed country's government would be both honest and competent. These comfortable old certainties have all evaporated. Instead, security has become part of the larger dependability problem. We build better and better tools, and these help the system builders to get a little bit further up the complexity mountain, but in the end they fall off. A proportion of large complex system projects fail, just like in the 1970s; but we build much bigger disasters nowadays.

Complexity is the real enemy of security. The distinction between outsiders and insiders used to simplify the business, but as everything gets connected up it's disappearing fast. Protection used to be predicated on a few big ideas and on propositions that could be stated precisely, while now the subject is much more diverse and includes a lot of inexact heuristic knowledge. The system life-cycle is also changing: in the old days, a closed system was developed in a finite project, while now systems evolve and accumulate features without limit... Economics will continue to ensure that insecure systems get built - and the liability will be dumped on others whenever possible. Governments will try to keep up, but they're too slow and they often can be bought off for awhile. So there will be many regulatory failures now.
The security Engineer of the 21st century will be responsible for systems that evolve constantly and face a changing spectrum of threats. She will have a large and constantly growing toolbox. A significant part of her job will be keeping up to date technically: understanding the latest attacks, learning how to use new tools, and keeping up on the legal and policy fronts. Like any Engineer, she'll need a solid intellectual foundation; she will have to understand the core disciplines such as cryptology, access control, information flow, networking and signal detection.

(Security Engineering Second Edition by Ross Anderson Chapter 27 page 890-891)

[16][17][18]

Hacking tends to be a misunderstood topic, and the media likes to sensationalize, which just exacerbates this condition. Changes in terminology have been mostly ineffective — what's needed is a change in mindset. Hackers are just people with innovative spirits and an in-depth knowledge of technology. Hackers aren't necessarily criminals, though as long as crime has the potential to pay, there will always be some criminals who are hackers. There's nothing wrong with the hacker knowledge itself, despite its potential applications.

Like it or not, vulnerabilities exist in the software and networks that the world depends on from day to day. It's simply an inevitable result of profit-oriented software development. As long as money is connected to technology, there will be vulnerabilities in software and criminals in networks. This is usually a bad combination, but the people finding the vulnerabilities in software are not just profit-driven, malicious criminals. These people are hackers, each with their own motives; some are driven by curiosity, others are paid for their work, still others just like the challenge, and several are, in fact, criminals. The majority of these people don't have malicious intent and instead help vendors fix their vulnerable software. Without hackers, the vulnerabilities and holes in software would remain undiscovered. Unfortunately, the legal system is slow and mostly ignorant with regards to technology, Often, draconian laws are passed and excessive sentences are given to try to scare people away from looking closely. This is childish logic - discouraging hackers from exploring and looking for vulnerabilities doesn't solve anything.

Convincing everyone the emperor is wearing fancy new clothes doesn't change the reality that he is naked. Undiscovered vulnerabilities just lie in wait for someone much more malicious than an average hacker to discover them. The danger of software vulnerabilities is that the payload could be anything. Replicating internet worms are relatively benign when compared to the nightmare terrorism scenarios these laws are so afraid of. Restricting hackers with laws can make the worst case scenarios more likely, since it leaves more undiscovered vulnerabilities to be exploited by those who aren't bound by the law and want to do some damage.

Some would argue that if there weren't hackers, there would be no reason to fix these undiscovered vulnerabilities. That is one perspective, but personally I prefer progress over stagnation. Hackers play a very important role in the co-evolution of technology. Without hackers, there would be little reason for computer security to improve. Besides, as long as the questions "Why?" and "What if?" are asked, hackers will always exist. A world without hackers would be a world without curiosity and innovation.

I hope this book has explained some basic techniques of hacking and perhaps even the spirit of it. Technology is always changing and expanding, so there will always be new hacks. There will always be new vulnerabilities in software, ambiguities in protocol specifications, and a myriad of other oversights. The knowledge gained from this book is just a starting point. It's up to you to expand upon it by continually figuring out how things work, wondering about the possibilities, and thinking of the things that the developers didn't think of. It's up to you to make the best of these discoveries and apply this knowledge however you see fit. Information itself isn't a crime.

(Hacking: the art of exploitation 2nd edition by Jon Erikson, Chapter 8 pages 451 to 452)

[Bibliography]

Bibliography

1. Von Newman Architecture:

http://en.wikipedia.org/wiki/Von_Neumann_architecture

2. Caesar Cypher:

http://starbase.trincoll.edu/~crypto/historical/caesar.html

3. Information security:

http://security.practitioner.com/introduction/

4. One-time pad:

http://en.wikipedia.org/wiki/One-time_pad

5. Cryptanalysis:

http://en.wikipedia.org/wiki/Cryptanalysis

6. Cryptographic hash function:

http://en.wikipedia.org/wiki/Cryptographic_hash_function

7. Public-keys:

http://en.wikipedia.org/wiki/Public-key_cryptography

8. Advance Encryption Methods:

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard john_agiol@hotmail.com;

9. Government view on AES (Advance Encryption Standard):

http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

10. Data classification:

http://en.wikipedia.org/wiki/Classified_information

11. Buffer overflow

http://en.wikipedia.org/wiki/Buffer_overflow

12. Phishing

http://en.wikipedia.org/wiki/Phishing

13. Protection from Phishing on browsers

http://www.mozilla.com/en-US/firefox/phishing-protection/

16, 17, 18Hacking: the art of exploitation 2nd edition by Jon Erikson, Chapter 8 pages 451 to 452

14, 15, 21 Security Engineering Second Edition by Ross Anderson Chapter 27 page 890-891

[*Appendices*]

Write name here MARTIN

Questionnaire

Do you have an antivirus installed on your computer? **Yes [✓] No [ ]**

If yes, is it free or did you pay for the software?

FREE

Do you have a basic idea on how to avoid getting viruses? **Yes [✓] No [ ]**

If yes, how did you come across the information?

INTERNET / WORK

Do you trust using your credit card online? **Yes [✓] No [ ]**

If no, why not?

TRUSTED SITES ONLY

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes [✓] No [ ]**

If not, what measures do you think should be taken?

Do you know what HTTPS means, on your internet browser? **Yes [✓] No [ ]**

Do you know what a padlock on the bottom right of your browser indicates? **Yes [✓] No [ ]**

Do you check website links you are visiting, making sure they are secure? **Yes [✓] No [ ]**

If not, why not?

Do you use Internet Explorer as your default web browser? Yes **[✓] No [ ]**

If yes, did you know there are other browsers, with better security? **Yes [✓] No [ ]**

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

Write name here Laura .....

Questionnaire

Do you have an antivirus installed on your computer? **Yes [ ]** **No [ ]**

If yes, is it free or did you pay for the software?

Free

Do you have a basic idea on how to avoid getting viruses? **Yes [ ]** **No [ ]**

If yes, how did you come across the information?

.....

Do you trust using your credit card online? **Yes [ ]** **No [ ]**

If no, why not?

.....

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes [ ]** **No [ ]**

If not, what measures do you think should be taken?

.....

.....

Do you know what HTTPS means, on your internet browser? Yes [ ] **No [ ]**

Do you know what a padlock on the bottom right of your browser indicates? **Yes [ ]** **No [ ]**

Do you check website links you are visiting, making sure they are secure? **Yes [ ]** **No [ ]**

If not, why not?

too busy

.....

Do you use Internet Explorer as your default web browser? **Yes [ ]** **No [ ]**

If yes, did you know there are other browsers, with better security? **Yes [ ]** **No [ ]**

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

.....

Write name here Sylwia

Questionnaire

Do you have an antivirus installed on your computer? **Yes [✓] No [ ]**

If yes, is it free or did you pay for the software?

I bought it

Do you have a basic idea on how to avoid getting viruses? **Yes [ ] No [✓]**

If yes, how did you come across the information?

Do you trust using your credit card online? **Yes [✓] No [ ]**

If no, why not?

but I am cautious

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes [ ] No [✓]**

If not, what measures do you think should be taken?

I don't know enough to make suggestions

Do you know what HTTPS means, on your internet browser? **Yes [ ] No [✓]**

Do you know what a padlock on the bottom right of your browser indicates? **Yes [ ] No [✓]**

Do you check website links you are visiting, making sure they are secure? **Yes [✓] No [ ]**

If not, why not?

Do you use Internet Explorer as your default web browser? **Yes [ ] No [ ]**

If yes, did you know there are other browsers, with better security? **Yes [ ] No [ ]**

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

I am sorry I don't know enough about my computer to comment

Write name here .....

Questionnaire

Do you have an antivirus installed on your computer? **Yes** [ ] **No** [ ]

If yes, is it free or did you pay for the software?

..... FREE .....

Do you have a basic idea on how to avoid getting viruses? **Yes** [ ] **No** [ ]

If yes, how did you come across the information?

.....

Do you trust using your credit card online? **Yes** [ ] **No** [ ]

If no, why not?

..... I am not trusting enough .....

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes** [ ] **No** [ ]

If not, what measures do you think should be taken?

.....

.....

Do you know what HTTPS means, on your internet browser? **Yes** [ ] **No** [ ]

Do you know what a padlock on the bottom right of your browser indicates? **Yes** [ ] **No** [ ]

Do you check website links you are visiting, making sure they are secure? **Yes** [ ] **No** [ ]

If not, why not?

.....

.....

Do you use Internet Explorer as your default web browser? Yes [ ] **No** [ ]

If yes, did you know there are other browsers, with better security? **Yes** [ ] **No** [ ]

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

.....

Write name here .....

Questionnaire

Do you have an antivirus installed on your computer? **Yes [✓] No [ ]**

If yes, is it free or did you pay for the software?

PAID FOR SOFTWARE

Do you have a basic idea on how to avoid getting viruses? **Yes [✓] No [ ]**

If yes, how did you come across the information?

VIA SERVER'S WEBSITE

Do you trust using your credit card online? **Yes [ ] No [✓]**

If no, why not?

WARNINGS IN THE PRESS (BUT STILL RISK IT!)

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes [✓] No [ ]**

If not, what measures do you think should be taken?

.....

.....

Do you know what HTTPS means, on your internet browser? **Yes [ ] No [✓]**

Do you know what a padlock on the bottom right of your browser indicates? **Yes [✓] No [ ]**

Do you check website links you are visiting, making sure they are secure? **Yes [ ] No [✓]**

If not, why not?

ASSUME THEY ARE SAFE – BUT IF MAKING PAYMENT WILL CHECK FOR 'PADLOCK' SECURITY.

Do you use Internet Explorer as your default web browser? Yes [ ] **No [✓]**

If yes, did you know there are other browsers, with better security? **Yes [✓] No [ ]**

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

.....

Write name here Robin

Questionnaire

Do you have an antivirus installed on your computer? **Yes [✓] No [ ]**

If yes, is it free or did you pay for the software?

Free

Do you have a basic idea on how to avoid getting viruses? **Yes [ ] No [✓]**

If yes, how did you come across the information?

Do you trust using your credit card online? **Yes [ ] No [✓]**

If no, why not?

Too many stories about credit card fraud & have had problems with own.

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes [ ] No [✓]**

If not, what measures do you think should be taken?

Not sure it can ever be foolproof.

Do you know what HTTPS means, on your internet browser? **Yes [ ] No [✓]**

Do you know what a padlock on the bottom right of your browser indicates? **Yes [ ] No [✓]**

Do you check website links you are visiting, making sure they are secure? **Yes [ ] No [✓]**

If not, why not?

Don't know how to.

Do you use Internet Explorer as your default web browser? Yes [✓] **No [ ]**

If yes, did you know there are other browsers, with better security? **Yes [ ] No [✓]**

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

I don't trust computers. I feel there are too many people out there who are fraudulent taking advantage of our computer age. Broadband is safer than dial up. I personally got a £1400 bill as a result of a dial up virus contracted from Spain when my daughter failed to shut the Computer down hence my mistrust!

Write name here Edna [redacted]

Questionnaire

Do you have an antivirus installed on your computer? **Yes** [✓] **No** [ ]

If yes, is it free or did you pay for the software?

PAID

Do you have a basic idea on how to avoid getting viruses? **Yes** [ ] **No** [✓]

If yes, how did you come across the information?

Do you trust using your credit card online? **Yes** [ ] **No** [ ] STILL CAUTIOUS BUT HAVE USED IT

If no, why not?

Do you think there are good enough measures in place for the teaching people about staying secure online? **Yes** [ ] **No** [✓]

If not, what measures do you think should be taken?

LEAFLETS POSTED WITH GOOD HEADINGS AND SIMPLE LANGUAGE

Do you know what HTTPS means, on your internet browser? **Yes** [ ] **No** [✓]

Do you know what a padlock on the bottom right of your browser indicates? **Yes** [ ] **No** [ ]

Do you check website links you are visiting, making sure they are secure? **Yes** [ ] **No** [✓]

If not, why not?

SPARSE USER AND VERY SELECTIVE

Do you use Internet Explorer as your default web browser? Yes [✓] **No** [ ]

If yes, did you know there are other browsers, with better security? **Yes** [ ] **No** [✓]

Thank you for taking part in my questionnaire, if there is anything you would like to add (do not feel obligated), please leave a note below.

AN OAP + USER WHICH HELPS TO EXPLAIN ANSWERS

Informative, unbiased answer

After researching my question I feel I can answer the question without being biased. I have a lot of data present with figures, opinions and facts. My research consisted mainly of professional technical books by experts on computer security, but I have also looked on the internet for figures etc.

In my essay, I shall elaborate about computer security, and its need in computing, as well as whether there will ever be a way to secure a system enough to fully protect against hacking or any other malicious intent.

Everyone that has internet access (or a computer with) is a stakeholder on internet security; ISP's and people who use their services alike are all expected to deal with security as a counter measures, though, the general public seem to have little knowledge of security when it comes to online browsing, as there are not many places they can find out how best to secure themselves.