Fall 2010

Home Computer Security Can Be Improved Using Online Video Streaming Services

Russell Barber
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

<u>Disclaimer</u>

HOME COMPUTER SECURITY CAN BE IMPROVED USING ONLINE VIDEO

STREAMING SERVICES

SUBMITTED ON 30 OF NOVEMBER, 2010

TO THE DEPARTMENT OF COMPUTER SCIENCE

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

INFORMATION ASSURANCE

BY

Russell Barber

APPROVALS
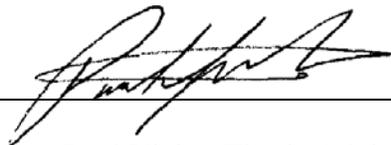
Paul Vieira, Thesis Advisor
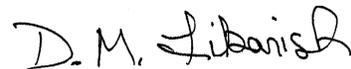
Daniel Likarish

Richard Blumenthal

Abstract

Home computer users face many new computer security threats. The rise of the internet has enabled viruses to spread rapidly. Educating computer users on security issues is one way to combat security threats. Video streaming web sites can provide a simple way to distribute educational videos to computer users. This project investigates the effectiveness of creating and distributing computer security educational videos on video streaming sites.

Acknowledgements

I would like to thank my family for their support during this project. This paper would not have been possible without the support of my wife, Loretta Barber. I would also like to thank my kids for their patience as I completed this paper.

I would also like to thank the Regis University staff for their training and the help I received over the last few years. Finally, I would also like to thank my colleagues and friends for their guidance and support.

Table of Contents

List of Figures

List of Tables

Chapter 1 – Introduction

Almost everyone has a computer in their home today. The most common operating system for home computers is Microsoft Windows XP, which has a history of security vulnerabilities. Microsoft Windows XP accounts for 48.9 percent of all computers on the internet (No Author Given, 2010, OS Platform Statistics). Home computers can have very little computer security protection against threats like viruses and attackers. The growth of the internet and access to broadband services allows these home computer users to be consistently connected to the Internet, offering remote attackers easy access to their systems. Security vulnerabilities can allow viruses and hackers to gain access to home computers and in some cases hijack home computers, forcing them to join forces with dangerous Botnets. Botnets are computer networks designed by hackers to send out spam emails, perform Distributed Denial of Service Attacks (DDOS), store illegal malware and damage files.

1.1 Statement of the Problem

Inexperienced PC users do not understand computer security risks and thus are not inclined to purchase security software to protect their computers. If a computer has been attacked and compromised, in most cases the user many not even know that their computer could host viruses, malware, or backdoors. The infected computer can then spread its infection to multiple computers.

Video based education is one effective way to educate novice users on the problems of computer security. Today, there are very few online videos that focus on computer security awareness available for home users. If such educational or awareness presentations are made available online, home computer security can be improved and the likelihood of future attacks

mitigated. If an educational effort can protect one computer on the Internet, it eliminates the

potential for that computer to become the "weakest link" in the larger IT security picture. In

recent years, businesses have increased their computer security education for employees;

however, home computer users have limited options when it comes to learning how to protect

their personal computer assets and information. Novice users generally do not know what kinds

of computer security they need or how to configure it to protect their computer resources. These

users should be aware of the most common computer security related issues and the appropriate

countermeasures available in their arsenal. Once a user understands what their risks are, they

can seek to protect themselves.

Recently, online video streaming services have become popular. Video streaming

services make distributing video content easy for video authors. Broadband internet connections

can allow high definition video to stream across the internet and users can easily watch videos by

using their internet browser.

There are numerous freeware or open source security applications available; however,

they are not promoted or advertised like most commercial programs. The open source developer

may lack the resources necessary to market their products against commercial products. Finding

free computer security programs to create a complete security solution can require a tremendous

investment of time.

1.2 Statement of Goals and Objectives

The object of this study is to establish the practice of educating users in computer

security through the use of online video streaming services. The study will only include the

evaluation of free or open source security software.   Also, the study will evaluate the

effectiveness of presenting educational videos through video streaming services.

1.3 Relevance, Significance or Need for the Project

Video based educational resources can be very effective at educating users. Videos allow

the user to follow along and complete the actions required to secure their computer. Examples of

areas that could be targeted with such education include, but are not limited to: antivirus

software alternatives and their use, backup policies, password protection and management,

encryption, and various firewall tools. There are commercial computer security training

programs available on the open market; however, they can be expensive and may not address all

the computer security requirements for the home user.

This project will focus on free or open source applications to provide solutions that meet

or exceed commercial products. The target audiences for these educational videos are home

users with limited budgets with little or no computer training. The software was choosing from

reviews and recommendations from multiple sources. Changes to software happen frequently,

this paper contains several distinct sections. Updates to one section can be applied leaving other

sections unaffected.

1.3 Scope of the Research

The study, including all software, background research and questionnaires was limited to

the time between December 2009 and December 2010. The survey was conducted via a free

online service. The users in the survey are anonymous.

Chapter 2 – Review of Literature and Research

This project researches common computer security issues and the ways to mitigate them. The project will also conduct research into video production methods and ways to present various security problems and potential solutions.   It will evaluate different security product solutions and discuss the optimal installation and configuration settings for a given situation. Then finally, this research will evaluate video web streaming technologies as a means to provide Information Security user education.

2.1 Home Computer Security

The focus of the study is the computer security of home computer users. A survey of home computer shows that home computer users are not well educated on security issues. "About 90 percent of those whose computers were infected with spyware didn't know about the infections and didn't know what spyware programs are" (Roberts P., 2010, p.1). We begin by researching computer security, then researching the most common security problems facing home computer security.

2.1.1 Computer Security

Security is defined by the state of being secure or free from danger. Computer security is therefore the state of securing a computer from danger. This means that a *secure* computer is protected from threats against it. These threats can take varies forms, including the users themselves. Software or hardware weaknesses or vulnerabilities can expose your computer and the information on them to these threats. Information security focuses on three main areas:

- Confidentiality – Information should be available only to those who rightfully have

    access to it.

- Integrity – Information should be modified only by those who are authorized to do so.

- Availability – Information should be accessible to those who need it when they need

    it.

These three areas of Information security also apply to home users. Home users wouldn't want a

stranger looking at their important documents. They should also expect that their data on their

hard drive can be retrieved and is available when they need it.

Safeguards and controls are used to protect assets against the impact of threats. An

example of a safeguard is the act of backing up important documents. An example of a control is

the use of password(s) for authentication. Controls are used for: auditing, authentication,

identification, and accountability.

2.1.2 Vulnerabilities and Risks

Vulnerabilities are weaknesses that can be exploited.   "A weakness in a system that can

be exploited to violate the system's intended behavior. There may be security, integrity,

availability and other vulnerabilities. The act of exploiting vulnerabilities represents a threat,

which as an associated risk of being exploited" (System Security Study Committee, 1996, p.

46). Vulnerabilities for home users come from many different areas. First, the most common

operating system for home users is Windows XP, which has had numerous vulnerabilities.

OS Platform Statistics

Windows XP is the most popular operating system. The Windows family counts for almost 90%:

2011	Win7	Vista	Win2003	WinXP	W2000	Linux	Mac
January	31.1%	8.6%	1.0%	45.3%	0.2%	5.0%	7.8%
2010	Win7	Vista	Win2003	WinXP	W2000	Linux	Mac
December	29.1%	8.9%	1.1%	47.2%	0.2%	5.0%	7.3%
November	28.5%	9.5%	1.1%	47.0%	0.2%	5.0%	7.7%
October	26.8%	9.9%	1.1%	48.9%	0.3%	4.7%	7.6%
September	24.3%	10.0%	1.1%	51.7%	0.3%	4.6%	7.2%
August	22.3%	10.5%	1.3%	53.1%	0.4%	4.9%	6.7%
July	20.6%	10.9%	1.3%	54.6%	0.4%	4.8%	6.5%
June	19.8%	11.7%	1.3%	54.6%	0.4%	4.8%	6.8%
May	18.9%	12.4%	1.3%	55.3%	0.4%	4.5%	6.7%
April	16.7%	13.2%	1.3%	56.1%	0.5%	4.5%	7.1%
March	14.7%	13.7%	1.4%	57.8%	0.5%	4.5%	6.9%
February	13.0%	14.4%	1.4%	58.4%	0.6%	4.6%	7.1%
January	11.3%	15.4%	1.4%	59.4%	0.6%	4.6%	6.8%

Figure 1. Operating Systems Statistics

Risks are the likelihood that a vulnerability or threat will be exploited or cause harm. Risk management is the process of identifying, measuring, controlling, and minimizing vulnerabilities.   Additionally, reducing exposure to threats is also part of risk management. These formal risk management techniques can be applied to home computer security.

2.1.3 Threats

Threats are characterized into two different types: intentional threats and unintentional threats. Intentional threats are the worst type. One example is disclosure, which is when someone has access to your information without your knowledge. Hackers that can access a home computer fall under the category of disclosure. Disclosure can come from a number of ways including: viruses, sniffers, trojans, theft, and phishing.

Unintentional threats can also affect your system. Computers are sensitive equipment and be affected by power fluctuations. Electrostatic energy, spikes, surges, brownouts are all power conditions that can cause unintentional threats to computers. Additionally, natural disasters, accidents, and human errors are also unintentional threats.

2.1.4 Managing Risks

Risk management is the process of reducing threats. The first step in risk management is risk assessment which is the process of identifying and understanding the threats. The threats are prioritized according to their severity. Corrective controls are identified that mitigate vulnerabilities.

The following list contains the basic tasks in risk management.

- Identify the assets needing protection.

- Determine the threats against the assets

- Determine the vulnerability to the threats.

- Analyze the current controls and safeguards.

- Select and implement the needed controls.

The second step in risk management is risk mitigation. Risk mitigation is the process of evaluating and implementing controls identified in the risk assessment. Not all threats can be eliminated, but the impact of the threats can be reduced. Risk mitigation is achieved through: assumption, avoidance, limitation, planning, research, acknowledgment, and transference.

Table 1. Risk Mitigation Options

Risk mitigation can be achieved through any of the following risk mitigation options:
• Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

• Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
• Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
• Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
• Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
• Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Each of the prioritized threats is addressed with an appropriate risk mitigation option. The controls are implemented and evaluated; corrections are made to ensure the control is working effectively. In summary, risk management is the process of: identifying, measuring, controlling and minimizing of uncertain events.

2.1.5 Layer Security

The use of multiple forms of security is a recommended technique, whereby multiple layers of security is employed, rather than a "one solution fits all" strategy. "Any single defense may be flawed, and the most certain way to find the flaws is to be compromised by an attack — so a series of different defenses should each be used to cover the gaps in the others' protective capabilities" (Perrin, 2008, p.1). Using different forms of security can be used effectively to provide multiple layers of security against threats. It's possible that one layer may catch the threat, where the other layer wouldn't.

2.1.6 Open Source Software

Open source software is application programs that promote access to the production source materials. Open source applications can be freely used by users as alternatives to

commercial products. To reduce costs for home users, open source solutions will be researched in this study as possible security solutions.

2.2 Computer Security Threats

Research was preformed into the most critical computer security issues facing home computer users. The main areas identified to effectively improve home computer security include antivirus, antimalware and patch management, and backup approaches. For each area, corrective solutions were researched to counter the security threat.

The follow list is an example of actions for home users from the CERT/CC. Numerous other sources have similar recommendations.

Table 2. List of Actions from the CERT/CC

The CERT/CC recommends the following practices to home users:
1. Consult your system support personnel if you work from home
2. Use virus protection software
3. Use a firewall
4. Don't open unknown email attachments
5. Don't run programs of unknown origin
6. Disable hidden filename extensions
7. Keep all applications (including your operating system) patched
8. Turn off your computer or disconnect from the network when not in use
9. Disable Java, JavaScript, and ActiveX if possible

2.2.1 Viruses

This research found that viruses are the main threat to computer users. Viruses have the ability to infect and reproduce themselves and they provide no value to the owner of the

computers. In some cases they can be destructive since viruses spread themselves from computer to computer through networks and removable media.

The best way to prevent viruses is with the use of Antivirus software. Antivirus software uses a scanner to scan files on the hard drive looking for matches against the virus signatory dictionary. Scanning hard drives can be time consuming so it is best to schedule scanning times at times with the computer is not being used. Once a scan has completed, the antivirus software will display the results of the scan.

Removable media allows viruses to spread directly from computer to computer. Removable media is typically used when transferring data between computers or sharing data with others. Most users trust removable media and wouldn't imagine it contained harmful viruses. Removable media also allows viruses to bypasses typical virus network firewall controls. Removable media can even allow viruses to infect computers in closed networks. Furthermore, easily versions of the Windows operating system by default automatically execute the autorun.inf file on removable media, allowing viruses to automatically be executed.

Viruses can impact the user computers in various ways. First, viruses will slow down computers as they reproduce and distribute themselves. Viruses will also consume computer resources like hard drive space and network bandwidth. Viruses can also affect the integrity of the hard drive by modifying, corrupting or even deleting files.

2.2.2 Malware

Malware was found to be the second threat to home computer users. Malware includes a number of threats against a computer user including, Adware, Spyware, Trojans, and Root Kits. Like viruses, malware run on a computer without the users' knowledge.

Malware is a real threat against computer users because they can spy on users' activities including: capturing keystrokes, taking screenshots, capturing passwords and accessing personal information stored on the computer. Malware can also provide a back door allowing remote users to access the computer remotely and slow down or interrupt a computer.

Recently malware has been used to target individual companies. Attackers embed malware into email and send them to employees at the target company. This type of focused attacked is called spear phishing. The attack can trick employees into revealing usernames, passwords, pins, and account numbers.

Malware scanners are the best way to detect and remove malware. Using a malware signatory file, a scanner scans the hard drive looking for matches. Malware scanners can also scan the windows registry file for possible infections. Knowing the sources of downloaded software and ensuring they are reputable sources is another way to prevent malware.

2.2.3 Updates and Patches

The study found that through the use of updates and patches computer users can lower the threats against them. Updates are improvements to software the user already has installed. Updates can add new functionality or fix security issues. Patches are fixes to existing software which may be installed on the user's computer.

Both updates and patches were found to be easy ways to correct possible security related issues. Because there is no industry standard for updating or patches, multiple methods were researched. Microsoft Windows provides the "Windows Update" feature which can identify and update Microsoft products including the operating system. The "Windows Update" feature can automatically download and install patches. Other software products commonly include a

"update" feature which allows the software to check for updates. Finally, there are new update

tools which will scan and identify installed application and compare against a database of known

versions. This last type of updater is powerful because it spans across multiple vendors.

2.2.3 Firewalls

Firewalls were found to also lower the threats against computer users. Firewalls block or

limit connections between the computer and remote computers. Firewalls effectively act as a

barrier between computers. Firewalls can block malicious applications like viruses or malware

that tries to connect to remote computers or remote computers connecting to back doors.

Firewalls can be configured using rules to allow application access to network features.

Rules can allow or block applications from access. Any new application requesting network

access will prompt the user to allow or block the application. This allows the user to control

what applications can engage the network.

Many home computer users now deploy routers in their homes to create small networks.

A router connects two networks and forwards data from one network to the other. Routers track

which local computer requests information so that it can route the data return back to the

requesting computer. If the router receives data, but it wasn't requested, the router will ignore

the data. This ignoring of unexpected data can protect home computers from malicious attacks.

In this case the router is acting as a hardware firewall.

2.2.4 Backups

The research showed that backups allow the user to recover critical data in case of loss.

Backups are part of a planned disaster recovery in case of data loss. It was discovered that two

different types of backups exist for the home computer users. The first type is a file backup,

were the individual files or folder are copied to a second location as a backup. The second type

of a backup is a drive backup. This backup is created at a hard drive level where the hard drive

contents are copied to a second location; typically these types of backups are larger than file

backups.

The file backup is a very easy and quick way to backup files. Backups should be copied

to a secondary drive. If the hard drive fails and the data is no longer available, the backup files

can easily be used. The file backup is stored in normal file system making recovery very easy.

The drive backup allows you to easily recover from a hard drive failure by recreating

your entire hard drive, include operating system. A drive backup is stored as an image; the only

way to view the files in the image is by doing a hard drive recovery.

Another possible backup strategy which was researched is internet backups. Using

commercial software, files can be identified for backup; those files are then compressed then

copied across the internet to a remote centralized location for storage. Using a remote location

for backups can prevent data loss in disasters, like fires where all data at a location can be lost.

2.2.5 Common Sense Security Issues

The research also identified some common sense security issues. The common sense

security areas cover the normal use a computer that any user should know. These common sense

security areas have been group together because there is no software solution that covers these

issues.

2.2.5.1 Passwords

Passwords provide authentication for many features on a computer as well as for online services. Creating strong passwords is important for good security. Many users use no or weak passwords. Other weak patterns are used like keyboard patterns and double words. Passwords should be controlled by a user and never allowed to be discovered or shared.

A strong password can be creating using 6 or more characters using; upper, lower, and special characters. A strong password will not contain a word that can be found in a dictionary. The Good Password Practices table covers 7 simple practices which will allow a user to create strong passwords.

Table 3. Good Password Practices

The following list of password practices create secure passwords:
1. Don't write your password down
2. Don't tell anyone your password
3. Change your password often
4. Password contains 6 or more characters
5. Password contains a mix or upper and lower characters
6. Password contains special characters
7. Password contains alphanumeric characters

A strong password is one that cannot be easily guessed or found using a brute force attack. A brute force attack is an attack that systematically tries all possible password combinations for a user. Each additional character in the password causes a brute force attack to increase the number of combinations exponentially. Using a long password with at least 6 characters, including special characters can create 782 billion possible combinations. The large number of combinations can deter attacks.

2.2.5.2 Wireless Access Points

Wireless access points allow users to easily connect computers together in a network or access the internet while traveling. They provide an easy way to wirelessly share resources or connect to the internet. Early wireless access points provided very little security to wireless users. Most wireless access points default to use not or little security. The lack of security on wireless access points can expose them to intruders.

Intruders can consume network bandwidth or access local shared resources including shared folders. Wireless access owners can be held responsible for the actions that intruders cause while accessing the internet through the wireless access point. Enabling encryption is an effective way to reduce intruders from accessing the wireless access point.

Table 4. Steps to Secure your Wireless Router

Steps to Secure you Wireless Router:
1. Change the administrator password 2. Change the default name of the SSID 3. Don't broadcast your SSID 4. Use WPA encryption instead of WEP 5. WEP security is better than no security 6. Use MAC filtering for access control

Recent manufactured wireless access points now enable encryption by default. This one feature forces owners into securing their wireless access points. Following the steps in Table 3 owners can easily secure the wireless access points.

2.2.5.3 Phishing

      Phishing is the attempt by criminals to acquire personal info by posing as a trusted source. Phishing can be done through emails or web pages claiming to be someone other than who they are. For example, a user may be emailed to login and check their bank account, when the user clicks on the link, they see a web site exactly like their banks so they enter their username and password.

2.3 Studio Equipment

      To create professional video content, the proper equipment is required. For this study, the following suggested equipment was used to create professional videos.

Table 5. Studio Equipment

Equipment	Cost
HDTV Camera Canon Vixia HF11	$800.00
Wireless Microphone, Samson SR-33	$120.00
Green Screen, 10X30 Feet	$80.00
Lighting, 2 Umbrella Lights, 2 Spot Lights	$100.00
Video Prompter, Wood and Glass	$35.00
Podium	$80.00
Video Camera Tripod	$40.00
Screen Capture Software, CamStudio Open Source	$0.00
Sony Vegas, Trial Version	$0.00
Total	$1255.00

2.3.1 HDTV Camera

For this study a high definition video camera was required to capture the highest possible resolution of the video presentations.   A Canon HD Vixia HF11 video camera was selected because it digitally stores all video which directly allows the video content to be uploaded to computer for editing.   The video camera also has a microphone input jack to receive audio from the wireless receiver.

2.3.2 Wireless Microphone

Capturing clear audio is important to being able to understand the instructions from the speaker. Numerous methods of audio capture were tried during the research, the final version used a professional wireless lapel microphone. The lapel microphone accomplishes two things: it clearly captures the voice audio, and centralizes the audio to the lapel microphone. The Samson SR-33 receiver is a professional two channel wireless receiver that receives audio from the lapel wireless transmitter. The receiver then retransmits the audio straight into the camera thru the microphone in jack providing very clear audio.

2.3.3 Lighting

Proper studio lighting is essential to allowing the video camera to capture the best available picture. A common lighting technique called three-point lighting was used in this study. The main illumination is created by the key light placed at 45 degrees in front of the subject. A second light, called the fill light, is placed at 90 degrees to the key light in front of the camera. The last light, called the rim light, backlights the subject and is positioned behind the

subject opposite the subject. Dual rim lights were used in this study to brighten the green screen

background.
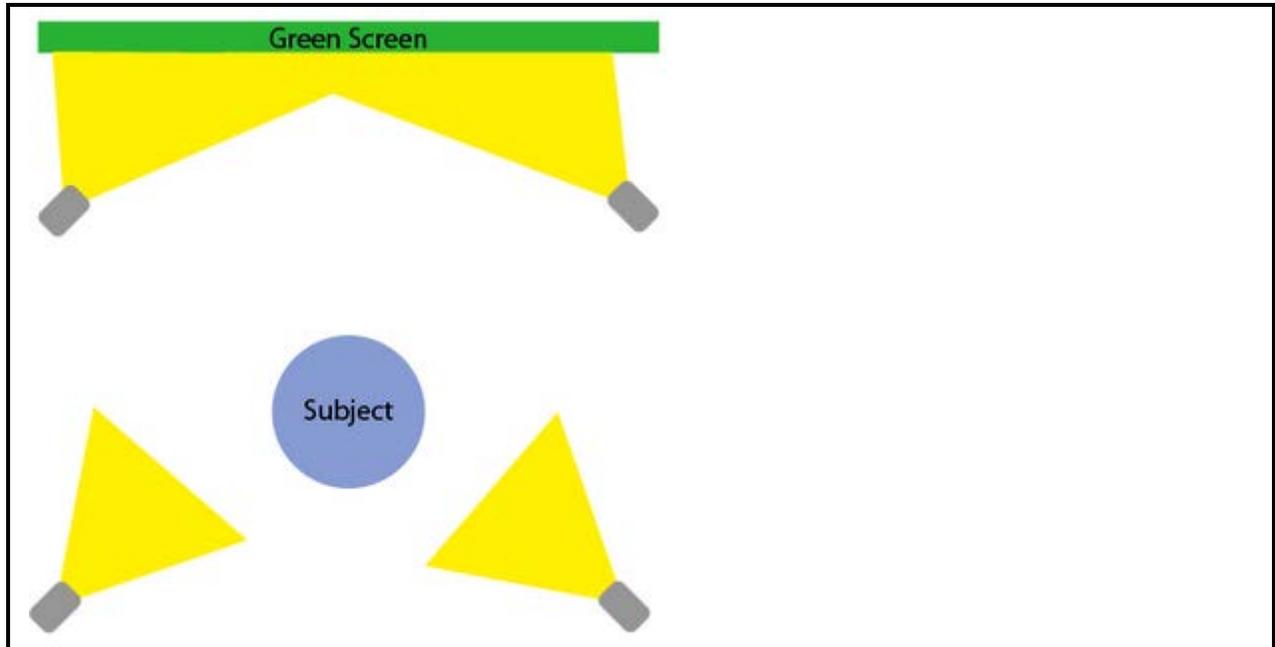
Figure 2. Three-Point Lighting

2.3.4 Green Screen

The use of a green screen allows video editing software to remove the background in post

editing. This technique is commonly called "blue screen" because of the initial use of blue

screens. However, the use of blue background screens has been replaced with green screens

because blue is a more commonly use color then green and you don't want the subject to have

the same color as the background color.

The video editing software uses chroma keying to combine the two images. The first

image contains the speaker and all non-green screen content. The green screen becomes

transparent allowing the second video to show through. A background animation was used as

the second video.
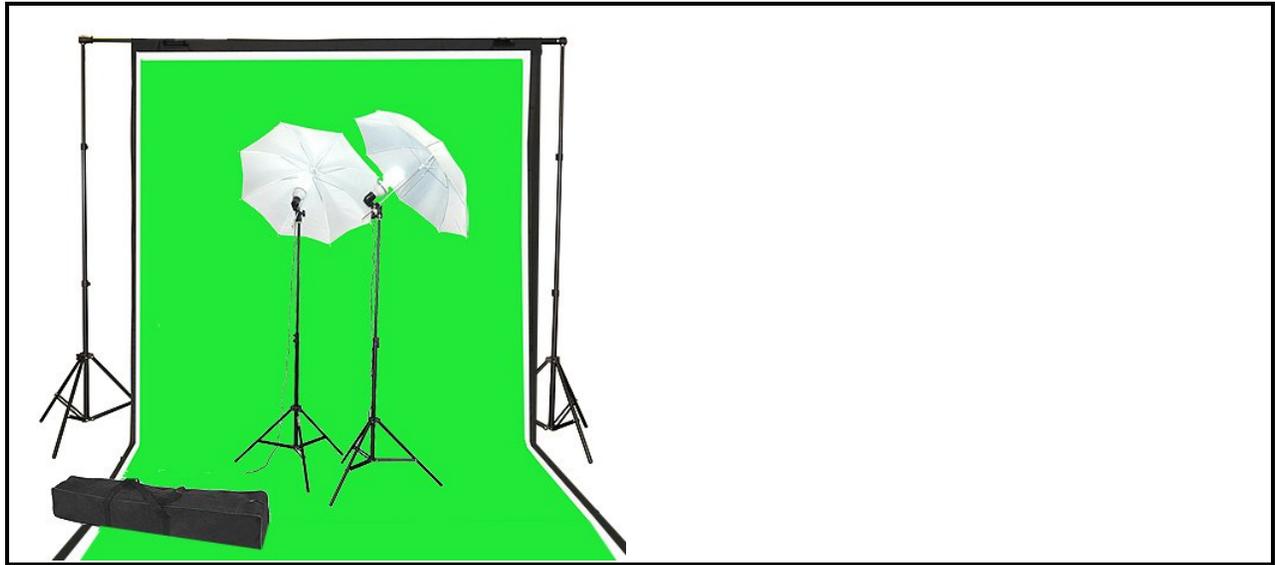
Figure 3. Green Screen

For this study it was necessary to adjust the lighting to improve the green screen keying. Dual lights were used to brighten the green screen behind the subject to provide a cleaner key color for the video editing software.

Figure 4. Green Screen Shadows

Additionally, it was necessary to move the green screen further behind the subject to

prevent shadows from the subject being cast on the green screen.

Figure 5. Correct Green Screen

2.3.5 Teleprompter

A teleprompter helps a speaker deliver a prewritten speech. A teleprompter uses a one

way mirror to reflex an image of the speech directly to the user. The camera looks thru the one

way mirror and the subject looks directly at the mirror and camera. The speaker views the text

as a reflection that scrolls as the speaker speaks. This allows the speaker to look directly at the

camera and give their speech.

During this study a teleprompter was constructed to aid in the presentation of the content. The teleprompter was constructed from; wood, glass, and a LCD monitor. The teleprompter plans were available online and free teleprompting software was used to display the text.

2.3.6 Video Editing Software

Video editing software is used to sequence and encode the individual video clips into a single finished presentation. First, the raw video from the video camera is copied to the editing computer's hard drive. Next, the raw video can be imported then edited in the video editing software. Using the built-in video filters, the green screen was chroma keyed out of the presentation. The editing software was used to create presentation titles.

Once the raw video has been sequenced and edited, the video edition software then renders the final video. The rendering process is a very slow process. The finished videos were encoding using the MPEG-4 AVI format. This universal target format was the recommended compression codec for many video streaming web sites.

2.3.7 Presentation Script writing

Each security presentation required writing two different types of dialog scripts. First, each presentation begins with the speaker directly addressing the camera. Next, using screen capturing software, video is captured of the software installation and configuration procedures. A total of 256 PowerPoint slides were created for 6 different presentations. Appendix A shows an example PowerPoint presentation that was created for the virus presentation video.

2.3.8 Screen Capture Software

Screen capture software is used to capture computer screens directly into videos. Audio dictation was captured as actions are performed. For this study screen capture software was used to capture installation and configuration procedures. Microsoft Powerpoint was used for video presentations.

2.4 Video Streaming Services

The videos created from this research will be distributed via an online video streaming service. Some video streaming sites provide a free way to stream videos to people via a web interface. Video steaming services have recently become a major player in internet entertainment. Netflix, a video streaming service now accounts for 20 percent of all internet traffic and YouTube accounts for 10 percent of all internet traffic (Schonfeld, 2010, p.1).

Video steaming services allow users to upload videos through a web browser. The videos are converted into a format that can be streamed to an internet browser using the providers' embeddable player. Many common browsers use Flash to render the videos. Users only have to view the web page and the embedded player or Flash will play the uploaded video.

Chapter 3 – Methodology

This study involves the creation and the distribution of educational videos. The project

was managed using a common development life cycle model. The study will also collect the

following data for analysis: anonymous reviews, surveys, counters, and user feedback on the

effectiveness of the videos.

3.1 Development Life Cycle

The author used a standard software development methodology in the creation of the

content used in this course. The Software Development Life Cycle (SDLC) is an engineering

model used in the creation process of software applications. The SDLC is commonly used in

software development because it is effective at creating computer systems. The SDLC model

was used because the author was familiar with the model. The common stages in a SDLC are;

planning, analysis, design, implementation, testing, release and maintenance. Typically once a

stage has been completed you move to the next stage. During the development process, earlier

stages had to be repeated in an iterative process. Previous stages were repeated because of

lessons learned during one stage forced a redesign or a reshoot.

3.1.1 Planning Stage

The planning stage began with the author identifying the high level goals of the project.

The main goal of the project is to create educational material for computer security. The target

audience for the course is home based users with minimal security training. The video quality

should be high quality and give the users a sense of professionalism. The project should have

educational content for each security threat that is found to commonly affect home computer

users. The educational material should be easy install to install or access. The course should

focus on free or open source software solutions.

3.1.2 Analysis Stage

During the analysis stage the outputs and deliverables of the project were determined.

The main security threats were researched and determined. Security software products were

evaluated that mitigated the threat. CBT courses were reviewed for common features and

functionality. Video streaming services were researched for features and video quality. Finally,

video production methods were researched and applied.

3.1.3 Design Stage

During the design stage, the content of each of the video presentations was written. Story

boards and then video scripts were created for each presentation. The length of each video

presentation was targeted to last ten minutes. Microsoft Powerpoint was used for presenting the

main points of each section. The video studio was equipped and prepared for shooting

presentations.   The studio setup consisted of setting up the green screen, video camera,

teleprompter, lighting, wireless microphone and podium. The design stage was the longest stage

of the project.

3.1.4 Implementation Stage

The implementation stage contained many activities including; video production and

video postproduction. The scripts were uploaded to the teleprompter and then each video was

captured. Each video presentation was captured numerous times. Each video was reviewed and

the best version was selected for postproduction. The security software selection and installation

video presentations were captured. Finally, the postproduction included edited and rendering

individual videos into a final presentation.

3.1.5 Testing Stage

The testing was performed by reviewing the videos after postproduction. Some changes

were necessary because of video glitches. Some common video glitches that were observed

were due to the green screen and scene transitions. The changes were made in postproduction

video editing software and did not require shooting new video.

3.1.6 Releasing Stage

During the final stage the videos were release to the general public. Youtube.com was

selected as the video streaming provider for this project. A user account was needed in order to

upload videos to YouTube.com. Each video presentation was uploaded as a separate video.

Each video was required to be less than 10 minutes. YouTube.com provides view counter on

how many times has been viewed.

3.1.7 Summary

The project included video production steps which are not normally done with SDLC.

Some of the activities during video production don't match exactly to a SDLC stage. The author

tried to match a video production task to the appropriate SDLC stage.

3.2.1 Data Collection

In this study two online questionnaires were created to capture information from anonymous users before and after reviewing the video presentations. The questions centered on the usefulness of the videos. The questions in the survey were kept brief to ensure users complete the task.

The data was obtained using a questionnaire, video ratings, personal interviews and observations. The online survey targets anonymous internet users. The video ratings were obtained from YouTube video rating system. The personal interviews were collected from work colleges.

3.2.2 Data Analysis

Graphical methods have been used because of the understandability. Microsoft Excel spreadsheet has been used in the data analysis.

Chapter 4 – Results

The evaluation of the results of this research has been used to draw conclusions on

efficiency of the content and the delivery method.

4.1. Security Solutions

For each presentation a number of security software solutions were researched. Based on

the features, usability, and other factors a product was selected. Each security software solution

was tested and then configured to ideal conditions.

4.1.1 Antivirus Software

The research determined that a number of useable free open source antivirus solutions

were acceptable. The Avira AntiVir software product was selected because it provides a

scheduler for automated scanning and it was very easy to understand and use. It also received

high marks for its detection rates as determined by independent tests from www.av-

comparatives.org.

Table 7. Antivirus Software

Software	Avira AntiVir Personal	AVG Anti-Virus Free Edition	Avast Home Edition
Scheduler	Yes	Yes	Yes
Easy to use	Yes	Yes	Yes
Detection Rate	Advanced+	Advanced	Advanced+
False Positives	Few	Many	Few
Scan Speed	Fast	Average	Fast

4.1.2 Antimalware Software

This study found a number of open source antimalware solutions. Unlike antivirus

software, in which multiple antivirus program installed on one computer can cause issues,

multiple antimalware products can improve security. Two products were selected for their

performance, *Ad-Aware* Free AntiMalware and Spybot Seek and Destroy.

Ad-Aware Free AntiMalware was selected for its fast scanner, its antimalware protection

and its ability to detect root kits. And finally, the product is well maintained and is updated

often.

Spybot Seek and Destroy was also selected because of its detection abilities which

include detection of over 1000 different types of malware, includes anti-root kit functionality and

possesses a real-time malware detection capability.

Table 8. Antimalware Software

Software	Ad-Aware Free Anti-Malware 8.3.1	Spybot Seek and Destroy	Malwarebytes Anti-Malware
Ease of Use	Yes	Yes	Yes
Features	Many	Many	Most
Scheduling	No	No	No
Updates	Yes	Yes, often	Yes, often
Detection	Excellent	Excellent	Excellent
Real-time Protection	Yes	Yes	No

4.1.3 Updating and Patches

A number of procedures and software tools were found to aid users to update or patch

their computers. Microsoft Windows XP contains a built in mechanism to update and patch

Microsoft products. The research also found a free software tool called FileHippo Update

Checker. The final feature that was found is embedded in many products, commonly called the

"Check for Updates" functionality.

4.1.4 Backup Software

The research discovered two different types of backups. The first backup is a file backup and the second type of backup is a drive backup. A number of backup products were evaluated and the results were determined. Both a file backup and drive backup product was selected and covered.

Table 9. Backup Software

Software	SyncBack Freeware 3.2.21	Macrium Reflect Free 4.2	FBackup	Windows Backup and Restore
Easy of Use	Yes	Yes	Yes	Yes
Features	Yes	Yes	No	No
Scheduling	Yes	Yes	Yes	Yes
File Backups	Yes	No	Yes	Yes
Drive Backup	No	Yes	No	No
Boot CD	No	Yes	No	No
Compressed	Yes	Yes	Yes	No

4.2 Video Distribution

Youtube.com was found to the best the web streaming service available. YouTube makes uploading videos a simple process. After a video is uploaded it requires about an hour before it is ready to be streamed. Videos are located through the use of keyword searches, whereby users enter words into a search textbox, and as a result matching videos are returned.

The finished security presentation video was approximately one hour long. The finished video had to be cut into smaller pieces to fit within the 15 minute limitations of each YouTube video.

Table 10. Video Streaming Sites

Video Streaming Sites	YouTube	Vimeo	Metacafe
Ease of Use	Yes	Yes	Yes
Features	Yes	No	Yes

Popularity	Yes	Yes	No
Length of Videos	15 minutes	60 minutes	10 minutes
Cost	Free	10 a month	Free
Quality	Good	Good	Low

4.2.1 Video Views

YouTube.com provides a view counter for each video. Table 11 shows the view metrics for each video in the course. The first video in the series contain more views than latter videos in the course. It possible that user found and reviewed the first video then either could not navigate to the next video or lost interest in continuing the course.

Table 11. Video Views

Video Section	Views
Overview -Viruses	68
Malware	15
Updates and Patches	9
Firewalls	9
Backups	7
General Security (Passwords, WAP, Email, and browsers)	15

4.3 Online Survey

SurveyMonkey was selected for anonymous surveys. SurveyMonkey offers free surveys that users can access through a web based browser. This research used a pre-video and post-video survey to collect user experiences. The use of a dual survey allowed for the comparative evaluation of the videos effectiveness.

The questions on the survey include:

- How would you rate yourself with computer security?

- Do you think your computer is infected with a virus or spyware?

- Do you think your computer is safe against viruses or hackers?

- Do you understand the security threats against your computer?

- Do you use any security software on your computer?

The following table contains the results of the survey. The total number of survey replies was very low. The limited number of survey results makes drawing conclusions difficult. However, the percentage of people understanding and using security software was higher after the post-video survey then the pre-video survey. Finally, the overall opinion on if the video was of benefit shows that they did provide a benefit to the viewers whom submitted to the survey.

Table 12. Survey Results

Survey Question	Before (7 total)	After (5 total)
How would you rate yourself with computer security?	No knowledge(3) Some (4)	No knowledge(2) Some (3)
Do you think your computer is infected with a virus or spyware?	No (3) Yes (4)	
Was your computer infected with a virus or spyware?		No (2) Yes (3)
Do you think your computer is safe against viruses or hackers?	No (4) Yes (3)	
Is your computer more safe against viruses or hackers?		No (2) Yes (3)
Do you understand the security threats against your computer?	No (3) Yes (4)	No (1) Yes (4)
Do you use any security software on your computer?	No (2) Yes (5)	No (0) Yes (5)
Was the video of benefit to you?		No (0) Yes (5)

Table 13. Survey Comments

Survey Comments (3 total)
Thanks, it helped me understand more about my computer
Thanks!!
Very professional, nice work

Additionally, the Post-Video survey contained a free form box allowing the user to enter any comments. Table 13 contains the comments that were received in the survey. Overall, the feedback was positive.

Chapter 5 – Conclusions

Video education presentations can be created using high grade consumer video equipment. A complete security solution for home users can be created using open source or free software. Video streaming sites provide an easy way to deliver videos to users. The creation of the dialog scripts is the first and the longest stage of the video production process.

5.1 Recommendations

During the course of the research a number of recommendations were discovered. The studio equipment recommendations were found through a process of trial and error. The analysis of the available open source applications provided the necessary material for software products. Finally, reviews of the available features from various video streaming sites were conducted.

5.1.1 Studio Equipment

The use of good video equipment is necessary when making quality presentations. A lot of time was wasted initially because of poor quality studio equipment. Capturing video is only a small part of the process, so focusing on video quality and using the best possible camera which can be afforded will prevent poorly captured or lost video.

5.1.2 Open Source Software

The results of this research showed that a complete security solution can be created using open source products. The research found that multiple products from different vendors could provide a free software security solution and most vendors offered a free version of their

software to attract home users; the vendors subsequently offer an enhanced product with full/enhanced features for a fee or suite purchase.   This research shows that open source applications can provide effective security solutions without purchasing commercial products.

5.1.3 Video Streaming Sites

YouTube is currently used by millions of people for entertainment. The results of this research show that this capability is falling short as an educational resource. One feature that would enable educational videos to be better presented is video chaining. Video chaining is the ability to create an ordered playlist of videos. Because videos are limited in length, finding the next video in a presentation can be challenging. Video chaining would allow entire presentations to be seamless shown from start to end.

5.2 Effectiveness of the Video Presentations

Based on the survey results it is possible to suggest that the video presentations presented enough educational material that users were able to start to secure their home computers. The format of the video presentations was very formal and educational. The majority of videos on YouTube.com are user create and non-formal. The videos might be more effective on a video streaming service that contained more educational type videos. The educational format of the videos may prevent some inexperienced users from fully utilizing them because they are in a formal format they are not familiar with.

5.3 Lessons Learned

The streaming technology at YouTube.com can provide high quality videos in real time. The features offered at YouTube.com are limited and do not provide the capabilities of a traditional software based training course. The lack of page customization and navigation between videos prevents using YouTube.com as complete educational solution. A web site with embedded YouTube.com videos would allow more flexibility and customizations needed to provide a complete educational course. While developing quality videos for distribution is possible; making the users aware of the educational videos is a problem.

5.4 What would you have done differently

One change that the author would have done differently is changing the location of the final hosting location. The author would have used a traditional web site to host the CBT course. This would allow more features which were not possible using only a video streaming service. The video presentations would still be hosted by YouTube.com. The YouTube.com video player object would be embedding inside web pages. This would allow other content to be present. Using web pages allows the ability to create a richer environment and provide better video to video navigation.

References

Creswell, J. W. (2003). Research Design: Qualitative, Quantitative, and Mixed Methods

    Approaches (2nd ed.). Thousand Oaks, CA: Sage Publications.

Leedy, P. D., & Ormrod, J. E. (2005). Practical Research: Planning and Design (8th ed.). Upper

    Saddle River, NJ: Pearson Education.

Yin, R. K. (2003). Case Study Research: Design and Methods (3rd ed.). Thousand Oaks, CA:

    Sage Publications.

Abell, J. C. (2010). Netflix Instant Accounts For 20 Percent of Peak U.S. Bandwidth Use.

    Retrieved from http://www.wired.com/epicenter/2010/10/netflix-instant-accounts-for-20-

    percent-of-peak-u-s-bandwith-use/

Schonfeld, E. (2010). Web Video Hogs Up 37 Percent of Internet Traffic During Peak TV

    Hours. Retrieved December 12, 2010, from http://techcrunch.com/2010/11/19/web-

    video-37-percent-internet-traffic/

No Author Given. (2010). OS Platform Statistics. Retrieved on December 12, 2010, from

    http://www.w3schools.com/browsers/browsers_os.asp

Kay. K. (2010). Weekend Project: DIY Teleprompter. Retrieved on November 2, 2010 from

    http://www.youtube.com/watch?v=3hNhIEDMm9o

No Author Given. (2010). Anti-Virus Comparative, On-demand Detection of Malicious

    Software. (Revision 5 October 2010). Retrieved on November 2, 2010 from

    http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf

Bavis, P. & Lewis B. (1996).Computer Security for Dummies. (1st ed.). Foster City, CA: IDG

    Books Worldwide, Inc.

Roberts P. (2010). Your PC May Be Less Secure Than You Think. Retrieved on Feburary 27,

 2011, from

 http://www.pcworld.com/article/118311/your_pc_may_be_less_secure_than_you_think.h

 tml

System Security Study Committee (1996). Computers at Risk: Safe Computing In the

 Information Age. (2st ed.). National Academy Press.

No Author Given. Open Source. Retrieved on Feburary 27, 2010 from

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

No Author Given. (2010). OS Platform Statistics. Retrieved on Feburary 27, 2011, from

 http://www.w3schools.com/browsers/browsers_os.asp

Perrin C. (2008). Understanding layered security and defense in depth. Retrieved on Feburary

 27, 2011, from http://www.techrepublic.com/blog/security/understanding-layered-

 security-and-defense-in-depth/703

Stoneburner G. & Goguen A. & Feringa A. (2008). Risk Management Guide for Information

 Technology Systems. Retrieved on May 15, 2011, from

 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Appendix A – Sample PowerPoint Slides

Virus Scripts

Viruses and Antivirus software

Barber, Russell CISSP

Viruses

- Viruses are applications that reproduce themselves and spread themselves to other computers
- They spread via computer networks(Internet or local networks) and removable media(USB drives, CD/DVD)
- They do nothing for the owners of the computers, other then waste computer resources.

How you can be infected

- Computer networks
- Removable media
- Email
- Internet Browsers
- Running applications that are infected with viruses

How to prevent viruses

- Antivirus software
- Not executing software from a questionable sources.
- Latest updates or patches installed (discussed later)
- Firewalls (discussed later)

Components of Antivirus Software

- Virus scanner
  - Scans memory and file system for viruses
- Virus signature file
  - Stores fingerprints of all know viruses
- Resident scanner
  - Watches computer processes in real-time
  - Scans files before they are opened or created

Popular Antivirus Products

- Avira AntiVir Personal - Free Antivirus*
- AVG Anti-Virus Free Edition
- Avast Free Antivirus
- PC Tools AntiVirus Free Edition 7.0
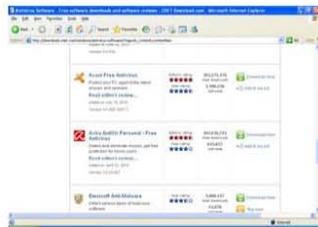- Microsoft Security Essentials

Virus Scripts

Avira AntiVir Personal - Free Antivirus

- Really high virus detection rates
- AutoUpdate
- Scheduler
- Guard (Resident scanner)

Avira AntiVir Personal - Free Antivirus

- Download Software
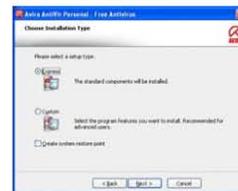 - Download.com
  - Search for "AntiVir"

Download.com
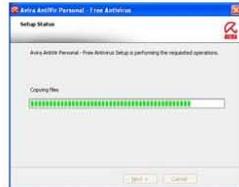
Save file

Welcome

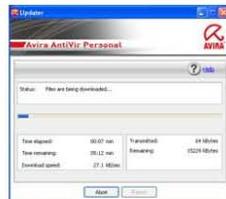### Install Type

Virus Scripts

Setup Status

Installation Complete

Auto Update

Main Screen

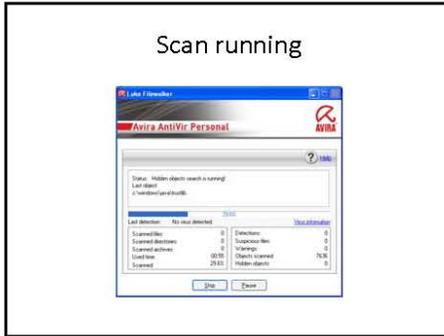Updater

Scheduler

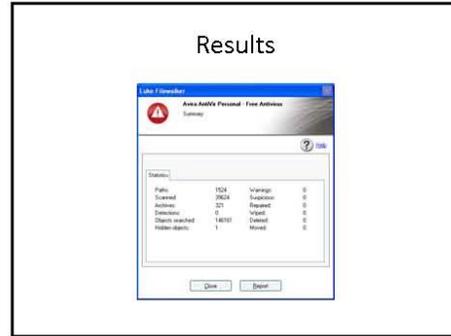Virus Scripts

Auto Updates
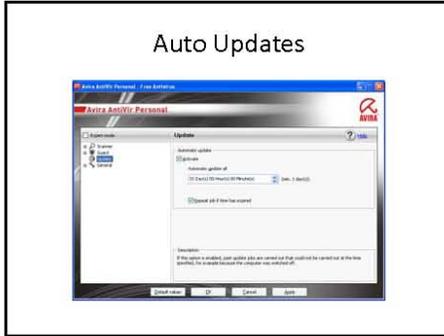
Scan system now
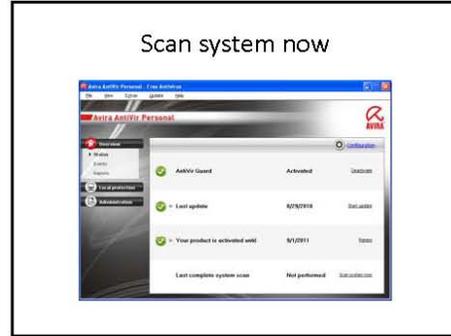
Scan running

Results

Nag Screen

Finished

Virus Scripts

Review

- You need Antivirus Software
- Create a schedule for scanning
- Update your Virus signature file before scanning or use autoupdate

Appendix B – YouTube Videos

Viruses

http://www.youtube.com/watch?v=O0tb2EcdL3I

Malware

http://www.youtube.com/watch?v=753oOp5Tzn8

Updates and Patches

http://www.youtube.com/watch?v=NaOKUAltTFo

Firewalls

http://www.youtube.com/watch?v=8IggN60Ckcc

Backups

http://www.youtube.com/watch?v=ffhYcBvkWJY

Basic Security

http://www.youtube.com/watch?v=TD8X3W8Rz6g