5-5-2012

Java Applet Awareness Impacting User Web Browsing Behavior

Norilyz Figueroa
University of Massachusetts Boston

Java Applet Awareness Impacting User Web Browsing Behavior

Honors Thesis

Norilyz Figueroa
May 5, 2012
University of Massachusetts Boston
Advisor: Ramakrishna Ayyagari
Professor: Jeffrey Keisler

Abstract:

The purpose of this study is to investigate the web browsing behaviors of computer users and how awareness about threats impacts their behaviors. This research focused on how users behave towards web browser alerts which prompt users to install Java Applets. Applets have become common tools for enhancing user experience. However, installing these features overrides security mechanisms inherent in browsers and provides complete access to users' computing resources. A survey was administered to two separate groups of students from the University of Massachusetts Boston to collect data. The first group took the survey after being given a few details about the study. The same survey was then given to a second set of students after they watched a video. The video educated participants on the dangers of installing Java Applets. Results showed that after watching the video participants had increased Java Applet Security Awareness and Information Security Awareness. This study can inform management on effective training procedures to improve compliance with security.

Table of Contents

Introduction

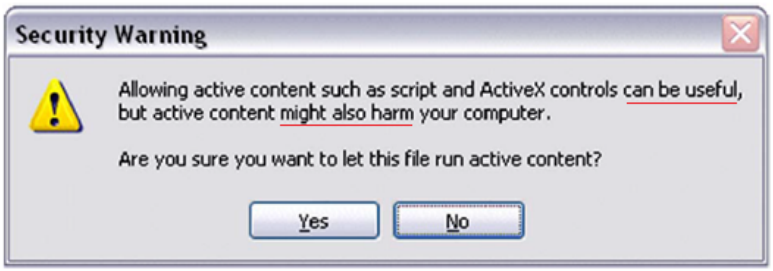
Privacy and security of information is a major area of concern for computer users. This research will focus exclusively on home users of computer systems. Home users make decisions on their computing practices and can decide whether or not to install protective software on their computer, what content to browse on the Internet, which emails to open, and how complex to make passwords. The goal for this study is to understand the behaviors of home users in respect to their web browsing behavior and how their behaviors may impact their privacy.

This study will focus specifically on how users behave towards Java Applets. A ***Java Applet*** is a program written in Java Programing Language which is transferred to a system and then executed by a web browser (Oracle, 2010). While browsing the Internet many users will encounter these Applets and allow them to run on their machine, being unaware of the serious risk they pose.

Java Applets are a well-known example of mobile codes. ***Mobile code*** is software that is transferred between systems, which can execute automatically (Microsoft, 2012). Mobile codes have become common tools for enhancing user web browsing experience. Other common mobile codes are ActiveX controls and Plugins. ActiveX controls and Plugins also pose similar security related issues as Java Applets. For instance, once a user downloads a malicious ActiveX control it has gained full access of the computer and will endanger user privacy (Schneier, 2004). Plug-ins pose a greater threat because they are automatically trusted by web browsers (Schneier, 2007).

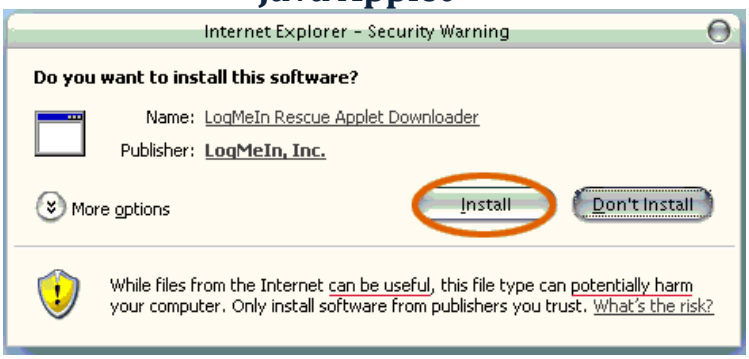
Some users can be confused by message alerts and browser recommendations. For example, an ActiveX control security warning displays the following message: (see image below)

ActiveX Control



The warning message tells the users that Active content can be useful but at the same time it might also harm their computer. The same confusion can occur with a Java Applet security warning. The Java Applet warning informs a user that while files from the Internet can be useful the file can be potentially harmful (see image below).

Java Applet



In both cases the user is left to make a security related decision based on the given information from the security warnings.

Java Applets

While users are exposed to numerous risk while browsing the Internet, this research will strictly focus on the risks associated with Java Applets. Java Applets will run on a variety of platforms and browsers, unlike ActiveX controls that will only run on Microsoft applications and

platforms (Microsoft, 2012). Java Applets are supported by Windows, Linux, Mac and Unix platforms. The variety of browsers and platforms Java Applets are allowed access makes this research essential. While browsing the Internet users can encounter two different types of Java Applet warning security messages. Users can encounter an Applet with a *digital signature verified.* A user can also come across an Applet with a *digital signature that cannot be verified*. If the signature is verified it is coming from a trusted source, and if the Applet is executed it will have greater access over users computing resources to execute its process (Oracle, 2012). On the other hand, if the signature cannot be verified then the Applet has originating from an untrusted source. If this Applet is downloaded, by default it is given less access to users computing resources in order to execute its process. "Signed Applets do not have the security restrictions that are imposed on unsigned applets and can run outside the security sandbox" (Oracle, 2012). It is important to keep in mind that when an Applet cannot be verified it does not mean that it is malicious. Users can be easily confused when deciding to run an Applet if they are not clearly informed in the distinction between Signed vs. Unsigned Applets.

If a user mistakenly allows a malicious Applet to run on their computer, their privacy is at risk. Once the Applet is installed it has full control over the users computing resources. A malicious Applet has the ability to capture images of users computing environment. It can also capture keystrokes which can compromise users sensitive information (i.e. passwords). They are also capable of executing new programs onto a user computer. These are just a few examples of how Java Apples can pose a security risk. (Microsoft, 2012)

User Behaviors Impacting Privacy

To explore research theories and methods, background literature includes research that is targeted to the behaviors of home computer users in respect to privacy and security. Anderson and Agarwal (2010) conduct a study to examine the security behavioral intentions of home computer users to secure their computer and their intentions to secure the Internet infrastructure. Dinev and Qing (2007) are interested in investigating the behavioral intentions of home computer users to use protective technologies. While Park, Sharman, Rao and Upadhyay (2007) examine the behaviors of home computer users who receive spam email.

"With over one billion people with access to the Internet, individual home computer users represent a significant point of weakness in achieving the security of cyber infrastructure" (Anderson and Agarwal, 2010, pg. 613) . The main purpose of the research conducted by Anderson and Agarwal was to understand the drivers that motivate home users to practice security-related behavior on their computers. Behavioral habits can affect the privacy of their personal data and can "potentially compromise the safety of the Internet infrastructure" (Anderson and Agarwal, 2010, pg. 614). They build and extend to the Protection Motivation Theory model, "which predicts individual response when faced with a threat" (2010, pg. 615). Both a survey and an experiment were conducted for this research. This study was focused to home users of computers with access to the Internet. A total of 594 undergraduate students and subscribers of a locally based internet service provider were surveyed. A lab was used for the experiment and 101 subjects were asked to review a website. They attempted to influence user's security attitude and norm, by using self-view and message frame manipulations (2010).

Results showed that a user's attitude for practicing security-related behavior is effected by "concern regarding security threats, perceived citizen effectiveness, and self-efficacy" (2010, pg. 628). While "attitude, social norms, and psychological ownership" are factors that influence user's to protect both the Internet and their own computer (2010, pg. 628).

Dinev and Qing (2007) examine the factors that influence user's intentions to use protective technologies and focus on attitudes and behaviors of individual computer users. Protective technologies are "information technologies that protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware, and others" (Dinev & Qing, 2007, Pg. 386). They focus on spyware because it endangers privacy since it is not created to destroy a computer, but rather to work undetected for long a period of time. The Theory of Planned Behavior (TPB) is used as a framework for the research and is extended and refined by technology acceptance model (TAM) and technology acceptance (TA) model. The Theory of Planed Behavior states "that a person's behavior is determined by her intention to perform the behavior of interest" (2007, pg. 389). To conduct this study a survey was administered to IS professionals and undergraduate students at a large university. The most significant result found that awareness of threats was the strongest predictor of user behavioral intention towards the use of protective technologies (2007).

Park, Sharman, Rao and Upadhyay conduct research to "examine the effect of privacy concerns on users behaviors after they have been exposed to spam e-mail" (2007, pg. 39). In this study users are categorized as either exhibiting usage-oriented or protection-oriented behaviors. Usage-oriented behavior describes "a behavior that relates to avoiding or reducing

e-mail use" (2007, pg. 43). On the other hand, protection-oriented behavior describes a "more active response which may include reporting spam to the email provider and applying protection filters" (2007, Pg. 43). The study for this research used data surveyed by the Pew Internet Research Center. 2,279 out of 4,000 survey responses were filtered out for this study because they were e-mail users. Logistic regression analysis was used to test each hypothesis. The most insightful finding in this study was that concern of privacy is important in explaining user's dual behavior, when they exhibit both usage-oriented and protection-oriented behaviors (2007).

There were similar approaches to the research conducted by Anderson and Agarwal (2010) and Dinev and Qing (2007). They both drew upon behavioral theories from psychology, sociology, and other disciplines to get better understanding of how individuals exhibit behavior. In respect to better understanding users behaviors, Anderson and Agarwal's (2010) research was better suited because of the experiment they conducted attempting to influence users behaviors. However, Anderson and Agarwal (2010) were concerned about both user's security and the security of the Internet. However, this current study only be addresses how user's security is impacted by their behavior.

Park, Sharman, Rao and Upadhyay aim to understand the behaviors of home computer users in respect to privacy. Their study only concentrates on user behaviors after the receipt of spam. The study conducted predetermines users behaviors to being usage-oriented, protection-oriented or both. For this research we investigated what behaviors may impact privacy and at

the same time not predetermine what those behaviors might be. A drawback from their research is that it uses secondary data that was not originally intended for their study.

Dinev and Qing (2007) examine the behaviors of home users and narrow down to a specific computing practice, the use of protection technologies. For this research user behaviors are also examined. In particular, how they respond to Java Applet warnings while browsing the Internet. This study will allow a better understanding of how users behave towards these warnings. It will also allow for recommendations to be made so that users are better protected from these threats.

Related Work

The purpose of my research is to explore the Internet browsing behaviors of home users and examine how these behaviors may impact their privacy. This study in particular will concentrate on how users respond to Java Applet alerts. Therefore, related work on where research focused on user web browsing behaviors was reviewed.

To practice safe web browsing individuals must be aware of how to configure their security settings and understand web browser alerts. Web browsers may alert users if they are trying to access a website that is a known phishing website, has a security issue, or is trying to install a Java Applet. Some prior studies have focused their research on the interaction between users and the Internet. Experiments have also been conducted to understand what actions users take when they are asked to make security related decisions.

Flinn and Lumsden (2005) conducted an online survey to get a more in depth understanding of home users "awareness and knowledge of specific technologies that relate to their security and privacy when using a Web browser to access the Internet" (pg. 13). Over a four month period 237 individuals participated in the study and completed an online questionnaire. The study focused on how aware and knowledgeable individuals were using web browsers. The questionnaire was specifically interested in addressing how familiar users were with "secure Web sites, browser cookies, Web site privacy policies, and trust marks (Flinn and Lumsden, 2005, Pg. 2). An important finding from their research was that users tried to educate themselves with online security and privacy practices, but were not as successful in doing so. There were also many different interpretations of the term "secure Web site" which caused users to have different levels of trust with sites. It was also found that browser cookies were confused with other types of data, which misrepresented their level of risk (2005).

Internet users are customizing their web browser experience through the use of third party web extensions (Martin, Smith, Brittain, Fetch, and Wu, 2001). However, these browser extensions can monitor and report user's Internet browsing behavior (Martin, Smith, Brittain, Fetch, and Wu, 2001). Martin, Smith, Brittain, Fetch, and Wu performed research to "report on the privacy practices of some common internet explorer extensions" (2001, Pg. 1). For this study they downloaded 16 internet explorer browser extensions and observed how they functioned. They found extensions that respected and endangered user privacy.

One main threat that home users face while browsing the internet is phishing. Phishing is a scam that clones trusted websites and attempts to acquire personal information from

individuals. Egelman, Cranor, and Hong (2008) research how users respond to phishing alerts while they are browsing the internet. They conduct an experiment where phishing emails were sent to participants, and observations were recorded (2008). Participants believed that they were going to be observed on their online shopping behavior. Participants were told it was a "think out-loud" experiment and they had to speak about what was happening and the choices they were making. Once participants made a purchase they were sent email confirmations, which were simulated phished emails. After, they would either receive passive or active phishing alerts. Results showed that active warnings stopped 79% of the participants from entering personal information, whereas passive warnings only stopped 13% of participants from doing so.

Jagatic, Johnson, Jakobsson, and Menczer (2007) conducted an experiment to understand the impact social context would have on a simulated phishing attack. The simulated phishing attack was administered to college students in Indiana University. Using information that was publicly available, through social networking sites, they were able determine relationships between students. Students would receive spoofed emails from who they believe where their friends. If students clicked on the email they received and entered their university email and password, the phishing attack was successful. The results showed that the phishing success rate in a social network context was 72%, higher than was expected (2007).

Many applications allow users to configure the security features allowing them a safer web browsing experience. Furnell, Jusoh, and Katsabas (2006) perform a study which determines if users understand how to configure the security features of certain applications. A

survey was administered to over 340 people to determine how well they understood the security features in Windows XP and in specifically 3 popular applications Internet Explorer, Outlook Express, and Microsoft Word (2006). The questionnaire included screenshots of these applications and asked questions to determine how comfortable participants were in configuring the settings. Findings show that users are having problems with both basic and advanced security options (2006).

"Users often do not understand enough about the impact of a security decision to make an informed choice" (Zurko, Kaufman, Spanbauer, 2002, Pg. 1). Zurko, Kaufman, Spanbauer, and Bassett try to understand what users would do when faced with a security decision by an application. A 500-person organization participated in this study. It reports on the security of each user's Lotus Client, after the default security setting on active content protection was changed from *open* to *secured* (2002). A Lotus Client is a "platform for distributed applications, of which email and discussion forums are examples" (2002, pg. 2). Lotus Notes security can protect from potentially dangerous active content. Active content languages supported by Lotus Notes include LotusScript and @ formulas, Java, and Javascript. Results showed that after the change in security settings, 59% of the respondents choose to allow unsigned active content to run on their Lotus Client.

Awareness

Java Applets are an area of concern due to the risks posed by malicious Applets and the contradictory messages Applets show when users are prompted to install them. User behavior

is a big factor for understanding why users are downloading malicious Java Applets. The drivers that influence users to make these decisions can lead to recommendations to prevent these downloads. Previous security related studies have concentrated on Awareness and Technology Awareness constructs. Technology Awareness (Dinev and Qing, 2007) and Information Security Awareness (Bulgurcu, Cavusoglu, & Benbasat, 2010) have proven to be a significant. Dinev and Qing (2007) adopted the concept of technological issues and individual awareness to develop the term *"technology awareness"*. *Technology awareness* is defined "as a user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (Dinev & Qing, 2007, Pg. 391). ***Information Security Awareness (ISA)*** is defined as a person's understanding and general knowledge about information security (Bulgurcu, Cavusoglu, & Benbasat, 2010). For purposes of this study ***Java Applet Security Awareness (JASA)*** has been developed and defined as a user's increased cognizance and understanding about Java Applets security. This study will incorporate both ISA and JASA constructs to examine user awareness.

The following research questions have been proposed for this research:

1. What kind of behaviors do users exhibit when they encounter Java Applet warnings?
2. Will increased awareness about the risks associated with downloading Java Applets impact user web browsing behaviors?

Hypotheses

The 2010 study on employee compliance and Information Security Policies found a significant correlation between *Information Security Awareness* and Information Security Policies (Bulgurcu, Cavusoglu, & Benbasat). This previous finding was adapted to fit the criteria

for this current study with Java Applets. When users are more aware of Java Applet Security they will also feel they have gained new knowledge, which will in turn increase their *Information Security Awareness*. To test this theory the following hypothesis is proposed:

> ***Hypothesis 1***: Users with training in Java Applet risk will have increased *Java Applet Security Awareness* and increased *Information Security Awareness*.

For proper testing this study will also provide the null hypothesis (1_o) which states that no significant differences between the groups will be found:

> ***Hypothesis 1_o:*** There is no significance relationship between users that receive training and J*ava Applet Security Awareness* and *Information Security Awareness*.

Previous studies have shown awareness to be a key factor in how users behave towards security related issues. In a study on employee compliance on Information Security Policies, *Information Security Awareness* showed to influence an employee's attitude to comply (Bulgurcu, Cavusoglu, & Benbasat, 2010).

This current study is focused on how users Java Applet Security Awareness will influence a user's attitudes and as a result influence their behavior. Users that are more aware of the security risk and threats that malicious Java Applets pose should be least likely to run them. Thus, the following hypothesis has been developed:

> ***Hypothesis 2***: Users with increased *Java Applet Security Awareness* are least likely to run them.

For proper testing this study will also provide the null hypothesis (2_o) which states that no significant differences will be found:

> ***Hypothesis 2_o:*** There is no significance between users with increased *Java Applet Security Awareness* and their likelihood of running them.

"One's awareness of Information Security may be built from direct life experiences, such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations, or it can be based on information obtained from external sources, such as newspapers, professional journals, organizational policy documents, and/or organizational workshops" (Bulgurcu, Cavusoglu, & Benbasat, 2010, pg. 533). Bulgurcu, Cavusoglu, & Benbasat found a significant positive relationship between an employee's Information System Awareness and Vulnerability of Resources (2010). ***Vulnerability of Resources*** is defined as "an employee's perception that information and technology resources at work are exposed to security-related risks and threats as a consequence of noncompliance with the ISP" (Bulgurcu, Cavusoglu, & Benbasat,2010, pg. 532). This current study will test if this hypothesis holds true with the relationship between Information System Awareness and Vulnerability of Resources constructs.

> ***Hypothesis 3***: A users Information System Awareness is positively associated with Vulnerability of Resources.

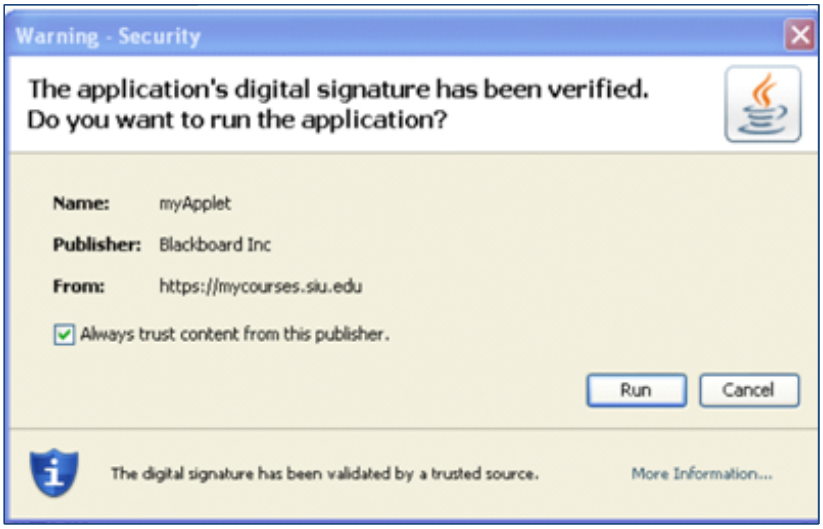
For proper testing this study will also provide the null hypothesis (3_o) which states that no significant differences in the relationship will be found:

> ***Hypothesis 3_o:*** There is no significance in the relationship between Information System Awareness and Vulnerability of Resources.

Method

Surveys were used to collect data for this research and test the hypotheses. The survey population consisted of 141 undergraduate students from the University of Massachusetts Boston. Participants were Management students who were enrolled in either introductory business or information technology courses. Management professors at UMASS Boston were asked if they would allow the survey to be administered during class time. There was no incentive for students to complete the survey and participation was strictly voluntary.

Surveys were administered by paper and contained questions which could be measured on a 5 point Likert scale. The survey contained a captured image of a Java Applet (shown below)



and participants were asked questions based on the image. The survey had a total of 22 questions and was designed to capture six main constructs: 1. Information Security Awareness, 2. Java Applet Security Awareness, 3. Attitude, 4. Self-Efficacy, 5. Vulnerability of Resources, and 6. Behavioral Intention. The survey also asked participants questions such as age, gender,

and years of Internet browsing experience. This survey was designed with the collaboration of thesis advisor to ensure that the survey was structured properly.

The survey was used to determine users awareness of Java Applet Security threats and how they responded towards threats. In order to capture awareness the survey was administered to two separate groups. Group A consisted of 65 students and Group B contained 76 students. Both of the groups took the same exact survey, however; Group B took the survey after watching a video. Complete survey can be found in Appendix A.

The three minute video demonstrated the risks associated with downloading Java Applets. The video started by demonstrating a user on a Google homepage being prompted to install a Java Applet. It then shows the user accepting the Java Applet and allowing it to run. Then the video shifts the view from the user to the attacker. The ***attacker*** is the person who intentionally installed a malicious Java Applet on the user computer to gain control of the users computing resources. The attacker then executes query which allows him to capture screen shots of the user computer. The video also shows the attacker remotely executing a calculator program onto the user computer. The attacker was able to see what the user was doing on his computer and at the same time control his computer by making programs start. This video was intended stimulate awareness and educate Group B on Java Applet security risk. After Group B watched the video they were then asked to complete the survey.

Analyzing Data

The survey was designed in such a way so that questions could be valued on a 5 point Likert scale. When a participant answered a Likert question they are specifying their level of

agreement or disagreement from a five point scale. Respondents were able to choose from strongly disagree, disagree, neither, agree, or strongly agree.

Surveys were collected, coded and separated into two groups. Group A did not watch the video while Group B did, and both groups took the same survey. Survey responses were first recorded into Microsoft Excel. The Excel data was then imported into IBM SPSS statistical software. Once the data was imported missing values of survey responses were calculated using series mean. The survey had a total of 22 questions and 19 of them aimed to capture 6 constructs. The following chart below shows how many questions were originally created to capture each construct.

	Construct	Number of Questions
ATT	Attitude	4
ISA	Information Security Awareness	2
APA	Java Applet Security Awareness	2
SE	Self-Efficacy	3
BI	Behavioral Intention	3
VURE	Vulnerability of Resources	5

Using SPSS software, the mean of each construct was then calculated. For instance, ATT (Attitude) which originally consisted of four questions would return the mean of four questions and classify them as AVE_ATT (average Attitude). This step was repeated for the remaining constructs. Computing construct means was an essential process for hypotheses testing.

Results

Hypothesis1 suggests that users with training of the risks associated with Java Applets will gain knowledge and have increased awareness of *Applet Security* and *Information Security*. In order to test this, a survey was administered to two separate groups. Group A took a survey

and Group B took the same survey after watching the video. The video was used as a training to increase *Java Applet Security Awareness*. This Hypothesis was tested by comparing the means of two independent samples with a T-Test. This test revealed if there were any significant differences between the Group A and Group B. This test indicated if there were any differences between the groups in terms of Attitute (ATT), Information System Awareness (ISA), Java Applet Awareness (APA), Self-Efficacy (SE), Behavioral Intention (BI), and Vulnerability of Resources (VURE). The two tables below display the output. The table labeled "Group Statistics" displays each construct and the statistics for the group who watch the video and the group who didn't. Video was coded as either being 0 or 1, 0 being participants did not watch the video (Group A) and 1 being participants did watch the video (Group B). The table labeled "Independent Samples Test" is where significance for each construct is tested. There is considered to be significance if sig<.05.

Group Statistics

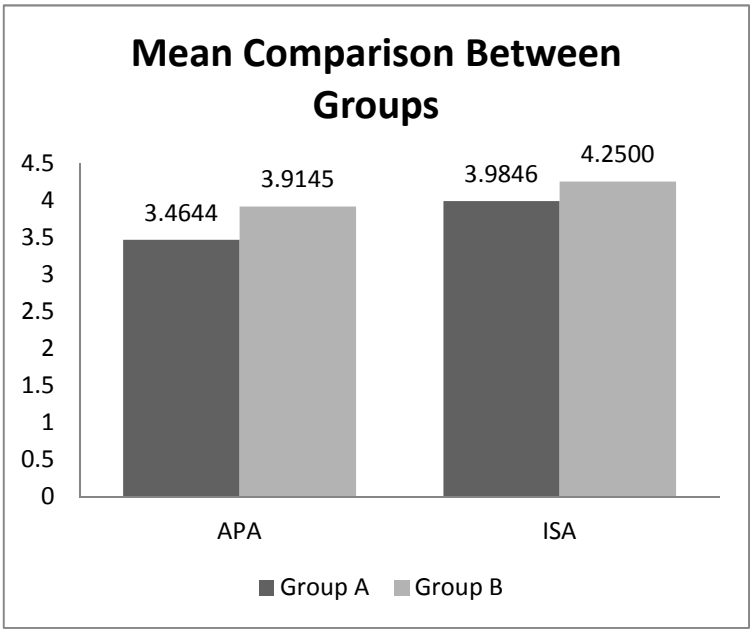
	VIDEO	N	Mean	Std. Deviation	Std. Error Mean
AVE_ATT	0	65	3.3980	1.17741	.14604
	1	76	3.6604	1.07722	.12357
AVE_ISA	0	65	3.9846	.75503	.09365
	1	76	4.2500	.78951	.09056
AVE_APA	0	65	3.4644	.94215	.11686
	1	76	3.9145	.91793	.10529
AVE_SE	0	65	3.2351	.97867	.12139
	1	76	3.6667	.92212	.10577
AVE_BI	0	65	3.6341	.88410	.10966
	1	76	3.8114	.79131	.09077
AVE_VURE	0	65	3.5236	.79236	.09828
	1	76	3.7771	.87620	.10051

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
AVE_ATT	Equal variances assumed	.581	.447	-1.381	139	.169	-.26239	.18997	-.63800	.11322
	Equal variances not assumed			-1.372	131.100	.173	-.26239	.19130	-.64083	.11605
AVE_ISA	Equal variances assumed	4.164	**.043***	-2.030	139	.044	-.26538	.13073	-.52387	-.00690
	Equal variances not assumed			-2.037	137.248	**.044***	-.26538	.13028	-.52299	-.00777
AVE_APA	Equal variances assumed	.013	.908	-2.867	139	**.005 ***	-.45011	.15698	-.76048	-.13974
	Equal variances not assumed			-2.862	134.469	.005	-.45011	.15730	-.76121	-.13901
AVE_SE	Equal variances assumed	.310	.579	-2.693	139	**.008***	-.43160	.16026	-.74846	-.11475
	Equal variances not assumed			-2.681	132.769	.008	-.43160	.16101	-.75008	-.11313
AVE_BI	Equal variances assumed	.053	.818	-1.257	139	.211	-.17734	.14112	-.45636	.10169
	Equal variances not assumed			-1.246	129.763	.215	-.17734	.14235	-.45897	.10430
AVE_VURE	Equal variances assumed	.849	.358	-1.789	139	**.076****	-.25352	.14168	-.53365	.02662
	Equal variances not assumed			-1.803	138.551	.073	-.25352	.14057	-.53146	.02443

The "Independent Samples Test" table reveals that there are significant differences between the group in terms of Information System Awareness (Sig 0.44*), Java Applet Awareness (0.005*) and Self- Efficacy (0.008*). There was also a marginal significance found for Vulnerability of Resources (0.076**).

The T-Test of Independent samples supports Hypothesis 1 because significance was found for both Java Applet Awareness and Information Security Awareness. Mean comparison shows that the Group B (participants who watched the video) responded significantly higher than Group A (participants who did not watched the video).



Results prove that after watching the video participants had increased APA and ISA. Thus, the following null hypothesis can be rejected:

> ***Hypothesis 1_o:*** There is no significance difference for users that receive training in terms of J*ava Applet Security Awareness* and *Information Security Awareness*.

Hypothesis 2 proposed that users with increased awareness of Java Applet Security (APA) would be least likely to run them. In order to test this hypothesis we used the T-test of two Independent samples to compare means, the same test previously used for Hypothesis 1. No significant differences between the groups were found in terms of *Behavioral Intention* (sig. .211). The following null hypothesis in this case is not rejected. The discussion portion of this paper will provide some details on why this unexpected result may have occurred.

> ***Hypothesis 2_o:*** There is no significance between users with increased *Java Applet Security Awareness* and their likelihood of running them.

The final hypothesis was derived from a previous study conducted that found a strong correlation between Information System Awareness and Vulnerability of Resources (Bulgurcu, Cavusoglu, & Benbasat, pg. 532). A user belief that their computing resources are at risk is dependent on their awareness of information security. From this case Information Security has been drawn from life experiences and effects Vulnerability of Resources. In order to test this hypothesis, we needed to get a sense of the overall Information security Awareness of the sample who participated in the study. A linear regression analysis was conducted having ISA as the dependent variable and Vulnerability of Resources, Attitude, and Self - Efficacy as the independent variables. No separation of the groups was necessary in this case. The following output resulted from the regression:

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24.691	3	8.230	18.481	.000[b]
	Residual	61.011	137	.445		
	Total	85.702	140			

a. Dependent Variable: AVE_ISA
b. Predictors: (Constant), AVE_ATT, AVE_VURE, AVE_SE

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.230	.293		7.611	.000
	AVE_SE	.351	.064	.435	5.485	**.000***
	AVE_VURE	.165	.072	.178	2.275	**.024***
	AVE_ATT	.022	.054	.031	.405	.686

a. **Dependent Variable: AVE_ISA**

The 'ANOVA' table shows sig. 0.000 meaning their sufficient significances found and the 'Coefficients' table shows the results of where those significances pertain. There does show to be significant relationship with ISA and VURE (sig. 024*). Therefore, the following null hypothesis is rejected:

Hypothesis 3_o: There is no significance in the relationship between Information System Awareness and Vulnerability of Resources

There was also a strong significant difference found between ISA and Self- Efficacy (sig. 0.000*). A further discussion on all hypotheses will be provided in the next section. See the table below for a summary of hypothesis testing results.

Summary of Hypotheses Results

H1	Supported	*$H1_o$ null*	Rejected
H2	Rejected	*$H2_o$ null*	Supported
H3	Supported	*$H3_o$ null*	Rejected

Age/ Years of Internet Browsing Experience/ Gender

To test the validity of the data retrieved from both groups test were conducted to ensure that age, years of internet browsing experience, and gender were not significantly different across Group A and Group B.

Regardless of age, we expected that awareness would change between the two groups. However, the age of the participants was not expected to affect the way they were influenced by the Java Applet video. The age range for participants in Group A was between 17-42 years

old and average age was 21 (21.433 was rounded). The age range for Group B participants was 22- 31 years and average age was 23 (22.75 was rounded).

Years of Internet browsing experience were also not expected to be effect results. We expected that such factor would be relatively similar across undergraduate students being surveyed in freshman course levels. Browsing the Internet was assumed to be similar and was not expected to have an impact on the current study. The range for years of Internet browsing experience for participants in Group A was between 4-20 years and average was 9 (9.43 was rounded). The range for Group B participants was 12- 26 years and average was 11 (10.55 was rounded).

Both participant age and years of Internet browsing experience were tested for validity by a T-Test of two Independent samples to compare means. Below is the output of the results:

Group Statistics

	VIDEO	N	Mean	Std. Deviation	Std. Error Mean
AGE	0	60	21.43	4.706	.608
	1	72	22.75	5.054	.596
YIBE	0	56	9.438	3.0823	.4119
	1	70	10.557	3.3390	.3991

***Note:** 'Group Statistics' table shows N (number of respondents) to be inconsistent for Age and years of Internet browsing experience. However, this is only the case because missing values were not calculated for these two instances. There were cases were respondents listed their age and but omitted years of browsing experience and vice versa. Refer to Appendix B for a full summary of calculated missing values.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
AGE	Equal variances assumed	.016	.900	-1.537	130	**.127**	-1.317	.856	-3.011	.378
	Equal variances not assumed			-1.548	128.371	.124	-1.317	.851	-3.000	.367
YIBE	Equal variances assumed	.040	.842	-1.935	124	**.055**	-1.1196	.5787	-2.2650	.0257
	Equal variances not assumed			-1.952	121.433	.053	-1.1196	.5735	-2.2550	.0157

This study did not expect to find differences between female and males in terms of how they respond to the Java Applet Awareness training video. We expected that regardless of gender, after respondents watched the video they would become more aware of Java Applet Security. Group A has a total of 60 participants, with 28 female and 32 male. Group B had a total of 71 participants, 12 being female and 59 male. Some participants did not indicate gender in the survey. Both Group A and Group B had 5 participants that did not indicate their gender.

Gender across groups

	Group A	Group B
Female	47%	17%
Male	53%	83%

The table above summarizes the percentage of females and males per group. There are slight differences in percentage of females and males across groups. Group A participants were 47% female and 17% of Group B participants were female. Group A had 53% of participants male and Group B had 83% male.

Discussion

The training video demonstrating the risk associated Java Applets did prove to stimulate awareness, with the rejection of null hypothesis 1_o. Testing showed that Group B participants responded to survey questions with higher averages than those of Group A. The group that watched the video (Group B) were more aware of Information Security and Java Applets. In terms of Information Security, Group B felt they were more aware of possible security threats and the risks that they posed in general. When it came to Java Applets, Group B felt that they understood the Java Applet alerts. They also felt they were more aware of the options available when prompted to install an Applet.

There were also a significant difference found between the groups for Self-Efficacy. Survey questions wanted to get a sense of how comfortable and confident respondents felt in making decisions in respect to Java Applets. The responses for the group that did not watch the video (Group A) averaged closer to the 'neither' selection of the Liker scale. The responses for Group B showed increase in the means. This indicated that after watching the video participants felt more confident in making decisions relating to Applets, such as feeling more comfortable in preventing their harmful installation.

A marginal significance was found for Vulnerability of Resources construct. Although marginal, it is important to mention because it does show that Group B respondents did respond slightly higher than Group A respondents. Vulnerability of Resources survey questions were designed to get a sense of how at risk respondents thought their computing resources

would be if they did not comply with Java Applet Alerts. Group B responded higher in thinking their resources would be more at risk, more vulnerable, exploited, misused and compromised.

When measuring to find differences between groups Behavioral Intention, no statistically significant differences were in fact found. As a result null Hypothesis 2_o was not rejected. Behavioral Intention survey questions tried to capture participants future behavior in respect to Java Applets. Participants were asked if they intended to comply with the recommendations of the Applet and intend to protect their computer in accordance to the alert. There were no significant differences in the responses to these questions by Group A and Group B. This does show to be worrisome, that participants could demonstrate increased Awareness, confidence (Self-Efficacy), and Resource Vulnerability but are not showing a reaction to behave differently. A training video was enough to increase their awareness on Java Applet security risk, but not enticing enough to change their habits.

A previous study found that Information Security Awareness had a positive relationship with Resource Vulnerability. In this case we ungrouped participants to capture their overall Information Security Awareness. We found that participant awareness of Information Security will affect how Vulnerable their Resources will become. In testing we also found a strong significance in Self-Efficacy. Therefore, participant awareness of Information Security will also affect how confident they feel in making decisions in respect to Java Applets.

Limitations and Future Research

This current study does have some limitations which could be addressed in future studies. Participants of this study were all undergraduate students at the University of Massachusetts Boston. Participants were all students enrolled in freshman level courses. There also resulted to be differences in gender amongst the groups. Group A had 47% female and 53% male and Group B had 17% female and 83% male respondents. The Group that took the survey after watching the video (Group B) had more male respondents. This occurred by chance, we were only informed by professors how many students they had in their classes. Estimated amount of students was important to try and capture beforehand so that Group A (65 participants) and Group B (76 participants) could be as close as possible in size.

Future research should further investigate behavioral intention. In this study, respondent awareness did not stimulate participant behaviors. The training video did impact awareness, participant confidence, and resource vulnerability but failed to impact their behavior. Further research could be done to test participant behavior, possibly with an experiment. After awareness is stimulated, participants could be observed on how they behave towards Applets. A previous study by Egelman, Cranor, and Hong (2008) observed how users respond to phishing alerts while they are browsing the Internet through an experiment. A similar tactic could be used to observe the way users behave while they come across Java Applet alerts while browsing the web.

Conclusion

This study can be effective for organizations interested in securing their computing resources. It is essential that employees are appropriately trained in areas of Information Security. With Internet usage in the workplace and employees constantly browsing the Internet, it is important that managers know how to effectively train employees.

Managers training employees on Information Security and Mobile Code security would only increase employee awareness of risk if they show a training video to employees. This study shows that users intentions to behave differently as a result of the video did not work. This is alarming with training videos being popular form of employee training. Further research needs to be done to determine how behavior can be influenced.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613-A15.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality – Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523-548.

Dinev, T., & Qing, H. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386-408.

Egelman, S., Cranor, L. F., & Hong, J. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* (CHI '08). ACM, 1065-1074.

Flinn, Scott & Lumsden, Joanna. (2005). User Perceptions of Privacy and Security on the Web. (NPArC) NRC Publications Archive.

Furnell, S. M., Jusoh, A. A., & Katsabas, D. D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications Of The ACM*, *50*(10), 94-100.

Martin Jr., D. M., Smith, R. M., Brittain, M., Fetch, I., & Wu, H. (2001). The Privacy Practices of Web Browser Extensions. *Communications Of The ACM*, *44*(2), 45-50.

Microsoft. (2011). Per-Site ActiveX Controls. Retrieved December 2, 2011 from "http://msdn.microsoft.com/en-us/library/dd433050(v=vs.85).aspx"

Microsoft. (2012). Managing Mobile Code with Microsoft Technologies. Retrieved March 3, 2012 from “http://technet.microsoft.com/en-us/library/cc750862.aspx”.

Oracle. (2010). Code Samples and Apps: Applets. Retrieved April 3, 2012 from “http://java.sun.com/applets/”

Oracle. (2012). What Applets Can and Cannot Do. Retrieved April 4, 2012 from “http://docs.oracle.com/javase/tutorial/deployment/applet/security.html”.

Park, I., Sharman, R., Rao, H. R., & Upadhyaya, S. (2007), The Effect of Spam and Privacy Concerns on Email Users’ Behavior , *Journal of Information System Security*, Volume 3, Number 1, pp 39-62.

Schneier, Bruce. (2004). Secrets & Lies: Digital Security in a Networked World. Wiley Publishing, Inc.

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). "Did You Ever Have To Make Up Your Mind? What Notes Users Do When Faced With A Security Decision. *ACSAC*, pp.371, 18th Annual Computer Security Applications Conference.

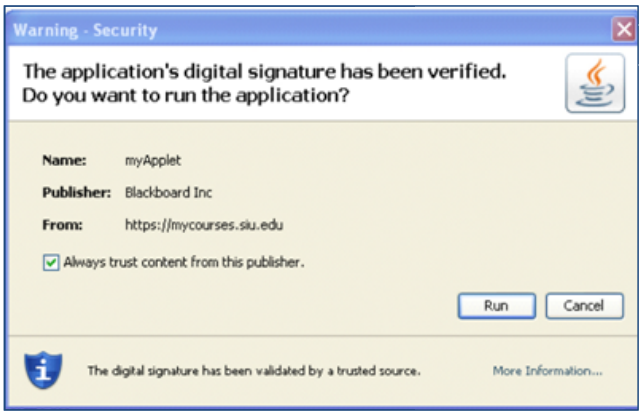
Appendix A

Java Applets, plug-ins, and active-x controls enhance user browsing experience. Common browsers (Firefox, Internet Explorer, Safari etc.) provide warning messages when using these additions (example picture is provided below). The following survey will focus on 'java applet' warning messages.

Note: The information you provide is confidential and we are not collecting any identifying information. There is no right or wrong answer – we just need your opinion.

Refer to the figure below to answer the following questions.

To me, proceeding with the recommendations of the browser alert would be:



1.	Unnecessary	☐	☐	☐	☐	☐	Necessary
2.	Unbeneficial	☐	☐	☐	☐	☐	Beneficial
3.	Unimportant	☐	☐	☐	☐	☐	Important
4.	Unclear	☐	☐	☐	☐	☐	Clear

When surfing the Internet on a web browser:	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
5. I am aware of possible security threats and their negative effects.	☐	☐	☐	☐	☐
6. I understand the concerns of information security and the risks they pose in general.	☐	☐	☐	☐	☐

Web Browsers will alert users to install Applets when visiting certain websites.

7. I understand the alert I receive when attempting to download Applets.	☐	☐	☐	☐	☐
8. I am aware of my options when attempting to download Applets.	☐	☐	☐	☐	☐
9. I feel comfortable making decisions with respect to installing Applets.	☐	☐	☐	☐	☐
10. I am confident in my ability to determine if an Applet is useful or harmful.	☐	☐	☐	☐	☐
11. I am confident I can prevent the installation of harmful Applets.	☐	☐	☐	☐	☐
12. I intent to comply with the recommendations of the Applet alert in the future.	☐	☐	☐	☐	☐
13. I intent to protect my computer according to the recommendations of the Applet alert in the future.	☐	☐	☐	☐	☐
14. I intend to follow the recommended action of the Applet alert message in the future.	☐	☐	☐	☐	☐

If I don't comply with the recommendations of the Applet alert, my computing resources _____

15. Will be at risk	☐	☐	☐	☐	☐
16. Will be vulnerable	☐	☐	☐	☐	☐
17. Can be exploited	☐	☐	☐	☐	☐
18. Can be misused	☐	☐	☐	☐	☐
19. Can be compromised	☐	☐	☐	☐	☐

20. Gender: _____

21. Age: _____

22. Years of Internet Browsing experience: _____

Appendix B

Result Variables

	Result Variable	N of Replaced Missing Values	Case Number of Non-Missing Values		N of Valid Cases	Creating Function
			First	Last		
1	ATT1_1	9	1	141	141	SMEAN(ATT1)
2	ATT2_1	12	1	141	141	SMEAN(ATT2)
3	ATT3_1	15	1	141	141	SMEAN(ATT3)
4	ATT4_1	15	1	141	141	SMEAN(ATT4)
5	ISA1_1	0	1	141	141	SMEAN(ISA1)
6	ISA2_1	0	1	141	141	SMEAN(ISA2)
7	APA1_1	0	1	141	141	SMEAN(APA1)
8	APA2_1	2	1	141	141	SMEAN(APA2)
9	SE1_1	1	1	141	141	SMEAN(SE1)
10	SE2_1	2	1	141	141	SMEAN(SE2)
11	SE3_1	1	1	141	141	SMEAN(SE3)
12	BI1_1	1	1	141	141	SMEAN(BI1)
13	BI2_1	0	1	141	141	SMEAN(BI2)
14	BI3_1	0	1	141	141	SMEAN(BI3)
15	VURE1_1	4	1	141	141	SMEAN(VURE1)
16	VURE2_1	3	1	141	141	SMEAN(VURE2)
17	VURE3_1	4	1	141	141	SMEAN(VURE3)
18	VURE4_1	2	1	141	141	SMEAN(VURE4)
19	VURE5_1	3	1	141	141	SMEAN(VURE5)