Installing Software Through Scareware

By Tyler Holland

CSC 300: Professional Responsibilities

Section 01-02

Dr. Clark Turner

April 11, 2012

Abstract

Scareware is software that the user is "scared" into installing through misleading advertisements. In 2009 over 40 million people fell victim to scareware, resulting in un-needed software being installed on their computers [3]. Scareware can be malicious and steal credit card information, or it can be software that doesn't do what it is advertised to do. This has become increasingly relevant on the Android OS, where ads are appearing that alert the user that "they need to upgrade their device's battery", but the software the user installs after following the ad does not actually help the battery [16]. While these advertisements may seem purely malicious, scareware vendor Marc D'Souza was able to create a profitable business model on this fake software [7]. D'Souza sold 1 million copies of his 40 dollar software through scareware advertising, deceiving users into thinking their computer was infected with a virus that D'Souza's software could fix [7]. Although it may be a profitable business for some, the "Software Engineering Code of Ethics" suggests scareware advertising is unethical because the advertiser is acting only in their best interest and does not think of the user at all [1].

Contents

1 Facts

In 2008 Marc and Maurice D'Souza began selling software through scareware under the company names Innovative Marketing and ByteHosting Internet Services [7]. They sold over 1 million software products for $39.95, under names such as WinFixer, Drive Cleaner and Antivirus XP [7]. Users were sold the software under the premise that "scans had detected viruses, spyware and illegal pornography" on their computers [7]. In 2011, the FTC fined the D'Souza's for $8.2 million dollars for multiple violations, including "unfair or deceptive marketing" and "mispresentations in connection with computer security software" [5].

WinFixer has no license agreement or prompts during installation [17]. It also claims to have found "Severe System Threats" on the user's computer, and launches automatically every time the user's computer is rebooted [17].

A study at North Carolina State University led by David Sharek and Cameron Swofford "shows that most internet users are unable to distinguish genuine popup warnings messages from false ones" [19]. "The study examined the responses of undergraduate students to real and fake warning messages while they did a series of search tasks on a personal computer connected to the Internet" [19]. The creators of the study pointed out that "The physical differences between the real and the fake messages were subtle, and most participants did not discern them" [19]. The results showed that 63% of users would click the OK box, even when knowing that the popup could be fake [19]. "Safer options, such as simply closing the message box, were infrequently chosen." [19].

In-app ads for both the iOS and Android smartphone operating systems have had links to malicious scareware apps that would install malware [16]. In 2011, malware specifically targeting Android increased 76% from the previous quarter [16]. Malicious software is not the only result of scareware on Android. Android developers can pay ad brokers such as "Green Fin Media" $1 to $3 per install of their app, so the advertiser's goal becomes "to get you to install that app by any means possible" [16].

Scareware has been advertised in many other ways as well. In 2008 advertisers would cold call people pretending to be from "support-onclick.com", and "frighten people into buying software that has little or no value or utility" [9]. The callers would claim there was something wrong with the user's computer, and attempt to sell software that would solve the fake problem [9]. Scareware advertisers have also used pop-ups on personal computers claiming that the computer is "damaged and corrupted", and then persuades the users to buy the scareware to fix the non-existant issue [9].

2 Research Question

Is it ethical to use "scareware" advertising to get users to install software, such as WinFixer?[7][16] This question is relevant to future software platforms. As Android has risen in popularity, scareware that tar-

gets that platform has begun to emerge[16]. There are many ads that will pressure you into downloading software that will "improve your battery life", when in reality they will either install malware or do nothing at all [16]. The answer to this question will assist future software developers in deciding how to or how not to advertise their software.

3 Extant arguments

3.1 Arguments that scareware software installation is ethical

3.1.1 FAKEAV and similarity to SEO

FAKEAV is a piece of scareware that has been very persistant. Roland Dela Paz, Threat Response Engineer at Trend Micro calls FAKEAV a "good example of a social engineering 'success story'" [14]. He explains, "by leveraging human weakness, FAKEAV effectively utilizes social engineering techniques" similar to SEO to "trick users" [14].

3.1.2 Lack of internet security training

Bill Mullins, Tech Thoughts blogger also takes a pro scareware stance. "If you get a malware infection; it's virtually certain it's your fault" [11]. Mullins believes that with proper internet security training, scareware wouldn't be an issue. "If users followed advice posted here, and advice from other security pros, and high level users, the Internet could be a vastly different experience for many" [11].

3.1.3 Users are easily tricked

North Carolina State University conducted a study to see "what visual design cues, if any, would alert people to the illegitimacy of fake popup warning windows while browsing the internet" [19]. The result of the test (63% of users clicking OK even when the popup window could be fake) prompted discussion at NCSU [19]. Study co-author Dr. Michael S. Wogalter says, "I don't know if you could develop a legitimate message that could not be duplicated and used illegitimately" [19]. He goes on to warn users to "be suspicious when things pop up" and to not "click ok, close the box instead" [19]. Wolter also says "The ways people responded could potentially open them up to malevolent software, such as spyware or a computer virus" [19].

3.2 Arguments that scareware software installation is unethical

3.2.1 Paying for software they don't need

Both Microsoft and Washington State's Attorney General are strongly against scareware. In 2008, they filed lawsuits against a large number of known scareware "scam artists" [15]. Attorney General Rob McKenna describes scareware to be a "blatant rip-off of consumers", and that users are "duped into downloading a fake scan and then duped into paying for software they don't need" [15]. He continues by saying that they "won't tolerate the use of alarmist warnings or deceptive 'free scans' to trick consumers into buying software to fix a problem that doesn't even exist" [15]. McKenna has had success in lawsuits against "inter-

net companies that prey on consumers' anxieties", and is confident in having this lawsuit go through.[15]

3.2.2 FTC Case

The Federal Trade Commission has brought a "temporary halt" to a large scareware scheme [4]. The scareware that the FTC is focused on is one that "falsely claimed that scans had detected viruses, spyware, and illegal pornography on consumers' computers" [4]. This version of scareware has been installed by over one million users, costing each user $39.95 [7]. The FTC also noted that the scareware "used an elaborate ruse that duped Internet advertising networks and popular web sites into carrying their advertisements" [4]. With this court case, the FTC is aiming to "permanently bar the defendants from engaging in 'scareware' marketing", and "provide monetary redress" to the users it has affected [4].

3.3 Summary:

The pro-scareware side thinks of scareware as just another social engineering technique. Scareware is compared to SEO in the way it "tricks users"[14]. The anti-scareware side sees scareware as false advertising and a "blatant rip-off of consumers" [15].

4 Application of Software Engineering Code

In the dictionary, a software engineer is "a person who designs and writes and tests computer programs" [6]. Scareware and the software it is advertising are both computer programs, so the definition fits [3]. The SE Code does apply to this ethical question, as the designers and developers of the scareware are then software engineers by definition, because they are creating computer programs [1][3]. There are also a few sections of the SE Code that directly apply to the ethics regarding this question.

Section 1.02 "moderate the interests of the software engineer, the employer, the client and the users with the public good" [1]. It is important to determine if the creation and distribution of scareware is working in the interests of the public good.

Section 3.08 ensure the software is well documented and "satisfy the users' requirements" [1]. Does scareware satisfy any of the users' requirements or expectations?

Section 4.04 "not engage in deceptive financial practices" [1]. Is the way scareware is advertised, by definition, a deceptive financial practice?

5 Analysis

The Association of Computing Machinery (ACM) has created a code of ethics for software engineers. It details the ethical responsibilites of software engineers working in the field. As described earlier in this document, the scareware makers and the corresponding software developers are by definition software engineers. In the next few sections, I will use the SE Code of Ethics to determine if "WinFixer" was installed on user's devices ethically.

5.1 SE Code 1.02: Moderating Interests

SE Code section 1.02 states that software engineers should "Moderate the interests of the software engineer, the employer, the client, and the users with the public good"[1]. "Moderate", as defined by the dictionary, means "to reduce the excessiveness of; make less violent, severe, intense, or rigorous" [6]. This definition means that SE Code section 1.02 is instructing software engineers to make sure the none of the interests of any one of these groups become excessive when compared to the other groups. "Interest", as defined by the dictionary, means "concern; importance" [6]. To simplify even further, this definition means that software engineers should make sure all groups affected by the software in question should have their concerns and important matters balanced to a fair level. In the next few sections, I will define what each groups' interests are.

5.1.1 Interests of the Software Engineer

The Software Engineering Code of Ethics states that software engineers should "act consistently with the public interest" and "act in a manner that is in the best interests of their client and employer consistent with the public interest"[1]. As defined above, the "interest" of these groups is anything that concerns or is important to them. The SE Code also states that "software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest" [1]. The interest of the software engineer is based on balancing the interests of all of the other groups mentioned in SE Code section 1.02. If all of the other groups interests are fulfilled, the software engineer's will be too, because they will be acting ethically. For this analysis, I will not directly involve the interests of the software engineer in my calculation, as it is fulfilled only if the other groups interests are balanced.

5.1.2 Interests of the Employer

In this example, the employer for the piece of software "WinFixer" is Marc D'Souza[7]. An employer, as defined by the dictionary, is "a person or business that employs one or more people, especially for wages or salary" [6]. The main concern of the employer is to be able to employ one or more people, by definition. The optimal team size for developing software is 5, as shown by research[2]. Additionally, the average salary of a software engineer is between 40,000 and 100,000 dollars a year, according to PayScale[13]. In order for Mr. D'Souza to fulfill his interests as an employer and hire a team of 5 software engineers, plus his own salary, the software he sells needs to bring in at least $600,000 a year[13].

The sales of "WinFixer" is over 1/3 of a million units sold at $39.95 each [7]. This comes out to over $13 million dollars from selling the software. 13 million is much greater than the needed 600,000 to pay salaries for himself and his team. As an employer, the sale of this software fulfills Mr. D'Souza's interests.

5.1.3 Interests of the Client

The clients in this example are the scareware advertisers. An example of a scareware

advertisement is a pop-up on a user's computer that says "CRITICAL ERROR MESSAGE! - REGISTRY DAMAGED AND CORRUPTED"[15]. Messages like these "scare" users into downloading the software it is advertising. As defined in the dictionary, to advertise is "to offer goods for sale or rent, solicit funds, etc., by means of advertisements"[6]. By definition, the interest of the client in this case is to offer their goods ("WinFixer") for sale.

As stated in the previous section on the interests of the employer, "WinFixer" sold over 1/3 million units combined [7]. The scareware advertisers were able to sell their goods, which fulfills their interests.

5.1.4 Interests of the Users

The users are the ones receiving the client's advertisements. It is in the interest of the user to have a working piece of software that acts as advertised [3]. In this example, the software was advertised as a registry error scanner that would solve the problems the scareware showed[15].

"WinFixer" was a "fake scan" as reported by the BBC [15]. The installed program was "software that corrects the non-existent issue by offering fake security fixes" [15]. To the users, the software they installed did not act as advertised. They expected to purchase a registry scanner to solve the problem the scareware was reporting, but in reality the software did not do any registry scanning[15]. The interests of the users were not fulfilled in this case.

5.1.5 Interests of the Public Good

For the public good, I will be using the ethical system of act utilitarianism. Act Utilitarianism states that "it is the value of the consequences of the particular act that counts when determining whether the act is right"[12]. The "value" that is mentioned is calculated by utilitarian principles. Utilitarianism is defined as "the ethical doctrine that virtue is based on utility, and that conduct should be directed toward promoting the greatest happiness of the greatest number of persons"[6]. In order for the interests of the public good to be served, the act of selling the scareware must provide the most happiness to the most number of people.

Based on the above sections dealing with the employer, client, and users, I will do a simple calculation of utility to determine if the public good's interests were fulfilled.

Group	Interests Fulfilled?	Utility
Employer	Yes	+1
Client	Yes	+3
Users	No	-333,000
Net Utility:		-332,996

Overall: Far greater negative utility than positive, this action is not ethical based on act utilitarianism. The public good's interests were not fulfilled.

5.1.6 Conclusion

In order for the installation of "WinFixer" to be ethical, the interests of the above groups must be balanced and fair as a result of moderation by the software engineer. As seen by the above calculation, the interests of the

two largest groups, the users and the public good, were not fulfilled.

Based on Section 1.02 of the SE Code, using scareware advertising to install this software is **unethical**.

5.2 SE Code 3.08: Satisfying Requirements

SE Code section 3.08 states that software engineers should "Ensure that specifications for software on which they work have been well documented, satisfy the users requirements and have the appropriate approvals." [1]. In order to determine if it is ethical to use scareware to install software on users' computers, I will use the example of Marc D'Souza's WinFixer program. In the following subsections, I will substitute parts of SE Code section 3.08 with relevant details about WinFixer. There are 3 parts to substitute that are referencing the software's specifications: "well documented", "satisfy the users' requirements", and "have the appropriate approvals".

5.2.1 Well Documented Specifications

According to the dictionary, "documented" is defined as "to furnish with references, citations, etc., in support of statements made" [6]. Additionally, "well" is defined as "in a good or satisfactory manner" [6]. "Specifications" is referencing the requirements document described in SE Code. Combining these definitions I will replace "have been well documented" in the SE Code with "have been satisfactorily referenced and cited".

5.2.2 Satisfy the Users' Requirements

As described earlier in the SE Code section 1.02 analysis, the "users' requirements" are having a working piece of software that works as advertised [3]. WinFixer is advertised as:

> "The ultimate solution that safeguards your system by cleaning the Windows registry, fixing damaged files, running disk cleanup and detecting hard drive errors. Winfixer protects your system against potential damages and problems, ensuring its optimal performance" [17].

For this part of the SE Code substitution, "satisfy the users' requirements" will be replaced with "satisfy the need for cleaning the Windows registry, fixing damaged files, running disk cleanup and detecting hard drive errors", as that is what the user requires from WinFixer as it is currently advertised.

5.2.3 Have the Appropriate Approvals

"Appropriate" is defined in the dictionary as "suitable or fitting for a particular purpose" [6]. "Approval" is defined in the dictionary as "formal permission or sanction" [6]. Using these definitions, I will substitute "have the appropriate approvals" in the SE Code with "have the suitable formal permissions".

5.2.4 Analysis and Conclusion

Combining these three substitutions together, the SE Code section 3.08 becomes:

> "Ensure that specifications for software on which the work have been satisfactorily referenced and cited, satisfy the need for cleaning the Windows registry, fixing damaged files, running disk cleanup and detecting hard drive errors, and have the suitable formal permissions".

In order to determine if WinFixer's specifications were satisfactorily referenced and cited, the requirements document must be inspected. After 10 internet search engine queries on WinFixer's requirements, there were no results that yielded an actual requirements document. However, one search result was a webpage dedicated to listing all known information about WinFixer [17]. According to this webpage, WinFixer has not published any information about itself [17]. This means that WinFixer published no public formal requirements document, which makes it impossible for the users to see. Due to the complete lack of a formal requirements document, WinFixer does not fulfill this section of the SE Code.

5.3 SE Code 4.04: Deceptive Practices

SE Code section 4.04 states that software engineers should "Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices" [1]. In order for WinFixer to have been involved in "deceptive financial practices", it needs to have engaged in "financial practices" in the first place. As described earlier in this paper, WinFixer sold over 333,000 units at $39.95 each [7]. Financial is defined as "pertaining to monetary receipts and expenditures", so because WinFixer received money for its software, it is dealing with financial practices [6]. In order to determine if WinFixer violated this section of the SE Code or not, I will examine each of the described financial practices to see if WinFixer violated one or more of them.

5.3.1 Bribery

A "bribe" is defined as "anything given or serving to persuade or induce" [6]. WinFixer was sold using "scareware" advertising techniques [3]. To sell the software, the scareware advertisers tricked computer users "into clicking on pop-up alerts that claim their device is 'damaged and corrupted'", even when there is no such problem on the user's machine [15]. WinFixer went even further with its persuasion, and alerted the user that it had detected hundreds of "Severe System Threats on your computer" and if the user did not install WinFixer, more problems would occur if not fixed immediately [18][10]. These problems included "lost documents and profile settings, physical data loss, system not starting up, and system slowdowns, crashes, and freezes" [18][10]. All of these messages are used in an attempt to persuade the user into buying the scareware, which in this case is WinFixer. The user is being persuaded into purchasing the software, because of a perceived problem on their computer that the scareware software can solve [3] [15]. This proves WinFixer guilty for using bribery, and failing this part of this SE Code section. It is worth continuing on to the other sections in order to gain a better grasp of the other deceptive financial practices, if any,

that WinFixer is guilty of.

5.3.2 Double Billing

Double Billing is defined as "to bill different accounts for the same charge" [6]. From all of the users that bought WinFixer, double billing has not been a complaint [15] [5]. What WinFixer does with the user's credit card information after the software is purchased is close to being considered double billing, but will be covered in the next subsection for a more detailed analysis.

5.3.3 Other Improper Financial Practices

This section will describe additional issues with WinFixer's financial practices that do not fit in to the categories of "bribery" or "double billing".

Right from the start of the scareware advertising, there are deceptive practices being used to trick the user into buying WinFixer [15]. The BBC reports that users were "duped into downloading a fake scan (of the computer) and then duped into paying for software they don't need" [15]. As described above, the users were "bribed" into paying for and installing the software because of what the user perceived as "threats to their computer" [18][10]. The BBC goes on further to describe the selling of WinFixer as a "scare and scam" that is "all about getting money out of the user" [15].

A study from North Carolina State University showed that "most internet users are unable to tell the difference between genuine and fake pop-up messages", such as those used in scareware [15]. Given a pop-up window, 63% of users would hit the OK button even knowing that there was a chance that the window was fake [15]. WinFixer's scareware advertisers used this to their advantage in another deceptive financial practice. Once the user started to install WinFixer, there would be no further pop-ups or prompts during installation [17]. This means that the user was never shown the license agreement, and was also never given an opportunity to stop the installation once it had started [17]. Not being shown the license agreement is classified as a deceptive financial practice, because the user is not aware of how they are or are not allowed to use and share the software [17].

The FTC has also identified a number of deceptive financial practices that Marc D'Souza undertook while selling WinFixer. This includes:

- "Installing advertising Software on consumers' computers in a deceptive or unfair manner" [5]
- "Misrepresenting ... the total cost to purchase, receive, or use ... any goods or services that are subject to the sales offer"[5] ...
- "Misrepresenting ... any material aspect of the nature or terms of a refund, cancellation, exchange, or repurchase policy"[5]

5.3.4 Examples in other Scareware

In addition to WinFixer, there have been over 250 other instances of software being in-

stalled through scareware [3]. In 2009 alone, over 40 million people had installed software solely because of scareware advertising [3]. In order to answer the larger question of "Is it ethical to use "scareware" advertising to get users to install software", it is important to observe the other examples. This section will be a brief look at some other possible problems related to scareware and deceptive financial practices.

Some scareware advertisements have been made to look exactly like products from large companies like Microsoft or other software providers [3]. This tricks users into thinking they can trust the software they are downloading, but in reality they are downloading completely different software. Software sold through scareware has also contributed to identity theft by installing trojans and viruses[3].

5.3.5 Conclusion

The selling of WinFixer through scareware advertising has involved using bribery along with other deceptive financial practices, such as imitating other software for the purpose of tricking the user [15] [5] [17]. This causes the selling of WinFixer to violate section 4.04 of the SE Code.

5.4 Conclusion:

Based on utilitarian principles and violations of the Software Engineering Code of Ethics, "Scareware" is not an ethical way to advertise software. Scareware benefits the advertiser, but at the cost of happiness for all of the users of the scareware. The only ones benefiting from the scareware are the advertisers and the employer, as the users are most likely tricked or scared into installing the software. Scareware advertising also violates sections 1.02, 3.08, and 4.04 of the Software Engineering Code of Ethics [1]. Scareware is not made in the interest of the public good, as it is only for the benefit of the advertiser. The user is also in most cases deceived into thinking the software will do something that it does not. Scareware is also a deceptive financial practice in some cases, such as when the software installed is actually malware and the software steals the credit card info of the user [3].

References

[1] "Software engineering code of ethics and professional practice," 1999. [Online]. Available: http://www.acm.org/about/se-code#full

The Software Engineering Code of Ethics used for many of the arguments.

[2] J. Appelo, "The optimal team size is five." [Online]. Available: http://www.noop.nl/2009/04/the-optimal-team-size-is-five.html

Optimal team size research done by an agile development researcher. Finds that optimal team size is 5.

[3] BBC, "Millions tricked by 'scareware'," October 2009. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/8313678.stm

Story of the 40 million scareware victims. Details how scareware is made to look like a legitimate warning, as well as many examples of the deceptive practices scareware uses.

[4] F. T. Commission, "Court halts bogus computer scans," December 2008. [Online]. Available: http://www.ftc.gov/opa/2008/12/winsoftware.shtm

FTC Court case ruling against scareware. This scareware falsely claimed a computer had a virus, then tricked the user into installing anti-virus software that they did not need.

[5] ——, "Stipulated final order for permanent injunction and monetary judgment as to marc d'souza and maurice d'souza," January 2011. [Online]. Available: http://ftc.gov/os/caselist/0723137/110127innovativemktgorder.pdf

The legal document fining the D'Souza's for their scareware scheme. This is mainly a negative, as it shows that this type of scareware does have legal repercussions

[6] Dictionary.com. [Online]. Available: http://dictionary.reference.com/

The dictionary. This is used to define software engineer and moderate.

[7] G. Gross, "Alleged 'scareware' vendors to pay $8.2 million to ftc," January 2011. [Online]. Available: http://www.pcworld.com/businesscenter/article/217987/alleged_scareware_vendors_to_pay_82_million_to_ftc.html

Pro argument for scareware. Man sold 1 million copies of software for 40 dollars a piece, only fined 8.2 million

[8] J. Hipolito, "Air france flight 447 search results lead to rogue antivirus," June 2009. [Online]. Available: http://blog.trendmicro.com/search-results-for-air-france-flight-447-lead-to-rogue-antivirus/

Scareware hijacking links related to top news stories through SEO and installing software. This was a new way of getting scareware out to people, through "SEO Poisoning".

[9] J. Leyden, "Scareware scammers adopt cold call tactics," April 2009. [Online]. Available: http://www.theregister.co.uk/2009/04/10/supportonclick_scareware_scam/

Scareware being promoted through cold telephone calls. People would get phone calls saying their computer was infected, and given instructions on how to install scareware.

[10] McAfee. [Online]. Available: http://vil.mcafeesecurity.com/vil/content/v_135733.htm

McAfee's page on WinFixer and the dangers it brings along with it. Describes in detail what WinFixer is.

[11] B. Mullins, "Scareware is everywhere - as mac users just found out," May 2011. [Online]. Available: http://billmullins.wordpress.com/2011/05/28/scareware-is-everywhere-as-mac-users-just-found-out/

Pro scareware article. Goes through the steps of preventing scareware, and comes to the conclusion that it is the users' fault if any malware is installed.

[12] T. P. D. of Philosophy, "Act-utilitarianism." [Online]. Available: http://www.utilitarianism.com/actutil.htm

Definition of Act Utilitarianism. Used in analysis.

[13] PayScale, "Salary for software engineer/developer/programmer jobs." [Online]. Available: http://www.payscale.com/research/US/Job=Software_Engineer_%2F_Developer_%2F_Programmer/Salary

Average Software Engineering salaries. The average is between 40k to 100k a year.

[14] R. D. Paz, "The persistence of fakeav," August 2010. [Online]. Available: http://blog.trendmicro.com/the-persistence-of-fakeav/

Pro scareware article. It deems FAKEAV a "social engineering success story" that leverages on human weakness.

[15] M. Shiels, “Fighting the scourge of scareware,” October 2008. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/7645420.stm

Microsoft’s lawsuit against scareware in the personal computer segment. Specifically, the lawsuit was against James Reed McCreary IV and his company that ”sent incessant pop-ups resembling system warnings to consumers’ personal computers”.

[16] T. Spring, “Sleazy ads on android devices push bogus ’battery upgrade’ warnings,” October 2011. [Online]. Available: http://www.pcworld.com/article/241967/sleazy_ads_on_android_devices_push_bogus_battery_upgrade_warnings.html

Examples of scareware on the Android side. In-app ads saying that your phone’s battery needed upgrading, then installing scareware when you download the recommended software.

[17] StopBadware.

[18] Symantec, “Winfixer.” [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2005-120121-2151-99&tabid=2

Symantec’s page on WinFixer and how to remove it. Describes in detail what WinFixer is.

[19] N. C. S. University.