# Internet science-Creating better browser warnings

Sepideh Mesbah
Advisor: Dr. Heiko Niedermayer
Seminar Future Internet WS1415
Chair for Network Architectures and Services
Department of Informatics, Technical University of Munich
Email:sepideh.mesbah@tum.de

## ABSTRACT

The number of internet users is increasing everyday, the number of security threats is growing as well. Browser warnings try to avoid users from being defrauded. They warn the users about the possibility of a threat, but it is always up to the user to decide whether to heed or ignore the warning. One main issue is the overwhelming amount of security warnings that each user might face, which makes it hard for the user to distinguish between serious or trivial threats. Better warnings can be created by considering items such as: how to design the display of warnings that affects the user's attention; how to involve social psychological factors in designing the warnings to have an impact on the user's decision; or realizing when to present a warning message and etc. The aim of this seminar paper is to first present the reasons why the users ignore a browser warning or turn it off and afterwards to discuss some recommendations for creating more effective warnings.

## Keywords

Warnings, Malware, Social, Psychology, Behaviorism, Security, Phishing

## 1. INTRODUCTION

While surfing the internet, the user might visit an infectious website. Browsers like Google Chrome and Firefox will try to stop the user by showing a warning message, but it is always up to the user to proceed or return to a previous page. This indicates that the role of the user should not be ignored by security practitioners.

There are three kinds of browser warnings: **malware** warning which appears when a website intends to damage a computer or steal information, **phishing** happens when the user is sent to a fake website instead of the real one and **SSL** warning pop ups when an invalid security certificate is identified.

Every day internet users are targeted by viruses, malwares, worms, phishing, etc. Users who do not pay attention to the warnings might believe that they are able to distinguish a real threat from a fake one. They extremely trust their ability or might think they have nothing to lose and are less susceptible. Stealing is not always about money, it can be the user′s information. The victims do not consider the ability of the scammers who can steal their information [14]. The scammers can use the victims personal information and create a bank account, buy or rent a property, etc.

In May and June 2013, a study[1] analyzed more than 25 million warning screens in Google chrome and Firefox to find the percentage of users which heed web browser security warnings. Users faced a by-passable browser warning given the option to click trough the warning by 'choosing proceed anyway' in Google chrome or 'understood the risk' in Firefox. The authors implemented some metrics in browsers to count the number of times that users saw a warning but clicked through without paying attention to it.

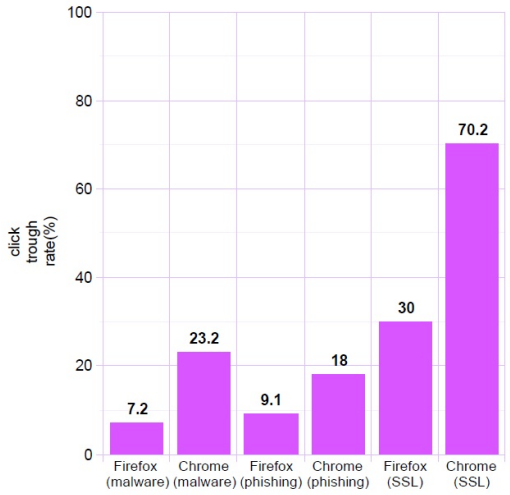


**Figure 1: Click through rate (number of ignored to number of shown warnings) for Firefox and Google chrome malware, phishing and SSL warnings**

As the results are shown in Figure 1, user behavior changes across different warning mechanism designs, hence more effective security warnings can be created in practice.

In this paper our main research is about how to create less but effective warnings that can attract the users attention. The paper is organized as follows: first, we present some reasons why the users ignore the warnings. Next, we focus on how to create more effective warning and will present several approaches which will be followed by a conclusion.

## 2. REASONS FOR TURNING OFF BROWSER WARNINGS


doi: 10.2313/NET-2015-03-1_06

In order to create better warnings, the reasons for ignoring or turning off the security warnings have to be discovered. Some individuals will ignore a warning in any way without any reason. They generally click through the security warning without looking through it. Some others think that warnings are just related to windows users and other operating system users can feel safe.

In this section we want to discuss several possible reasons for turning off browser warnings. Figure 2 is an example of a malware warning in Google Chrome.

## 2.1 Trust in automation

Automation has its own problems. Some users do not trust automated systems, they can not rely on it and would rather make their own decision. On the other hand some individuals trust automated systems incorrectly. For example they extremely trust their anti virus applications and think that the application can protect them from all kind of malwares, thus will download whatever they want.

The association between the users and automation can be defined with words misuse and disuse. Misuse means that people trust an automated system inappropriately which may lead them to fail. Disuse means that individuals do not trust an automated system and will ignore its ability[5]. In both situations the users do not have enough knowledge about the automated systems and may lead them to make wrong decisions.

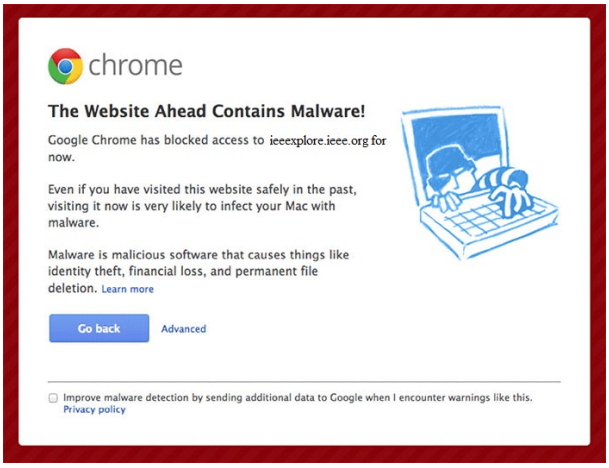


**Figure 2: Example of a malware warning in Google Chrome**

## 2.2 Not understand

Not understanding the meaning of a security warning is another reason for ignoring it. Individuals who do not understand the concept of the warning will ignore it easily. For example when users do not have enough information about the words SSL or Phishing, they will ignore it without considering the negative consequences[3].

## 2.3 Habituation

When the user observes a warning multiple times she might get used to it. After several times perceiving the same warning, the user gets confused with the similar looks and can not distinguish the serious alarms. User's attention decreases, thus ignores the exception message without even reading it once.

## 2.4 False positives

It is always difficult for the users to distinguish between a real and serious security warning from a trivial one. Analysis in [6] showed that various users didn't heed the warnings since they previously faced several false alarms. This means that they saw a warning message which tried to stop the user's operation, but when they ignored it, it later appeared to pose no threat. In this case, the users think they can identify the security risks on their own. For example browsers might give a false SSL alarm about expired security certificate of a website. This kind of alarms can be meaningless like if the computer's clock is set incorrectly, which makes the security certificate look expired.

## 2.5 Hassle

Some individuals are lazy and think heeding to the warning is waste of time, so will ignore it quickly. Another view is economic perspective. Herley [8] described that the likelihood of a serious attack happening is relatively low, compared to the cost of effort of reading a warning message, checking the URL for detecting phishing threats, spending time to choose strong passwords, etc.

## 2.6 Trusting high-reputation websites

Users might heed warnings about the websites they visit for the first time, but they won't pay attention to the warnings that appear for a safe high reputation website which the user visited before[7].

A recent study [7] analyzed around four million different Chrome malware warning effects. As it is shown in Figure 3, the users are twice as likely to ignore a visited website which was stored in their browser's history. Individuals trust high-reputation websites, thus will not heed to the warnings.

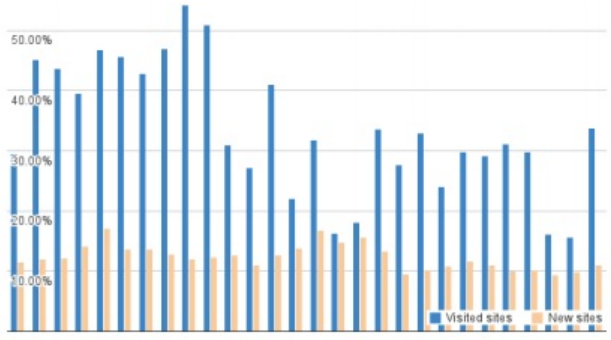


**Figure 3: Y indicates the click through rate, for visited web sites (blue), or new sites (red). Each point in x axis is a day. 28 days in January 2014 [7].**

# 3. CREATING EFFECTIVE WARNINGS

When a user visits a suspicious website, the browser will present a warning message to the user. Although the last decision is always made by the user, effective warnings can


doi: 10.2313/NET-2015-03-1_06

be designed in a way that can prevent the user from being in a hazardous situation. In this section first we will discuss when a warning should be used. Next the focus will be on the presentation of warnings, afterwards the social psychological factors will be discussed which showed to have a great impact on creating effective warnings.

## 3.1 When should a browser warning be used

As mentioned in [15], one of the main issues in security warnings is the habituation. The user will try to ignore the messages she has seen several times without reading it. Being aware about when a browser warning should be shown is important. Figure 4 shows a graph for risk assessment. Risk can have two features: The impact it may have and the probability that it might occur.
Three different zones are presented in Figure 4. The first zone indicates that the impact of the risk is low, so in this case it is better to not bother the user, and it is not necessary to send a security warning. In the second zone, the impact of risk is high thus the browser should block the user's action without sending any warnings. Only in the third zone it is required to ask the user to make a decision. When the impact of the risk is neither low nor high, based on the probability of risk occurrence, a warning message should be shown to the user and ask her to choose between ignoring or heeding to the alarm[15].

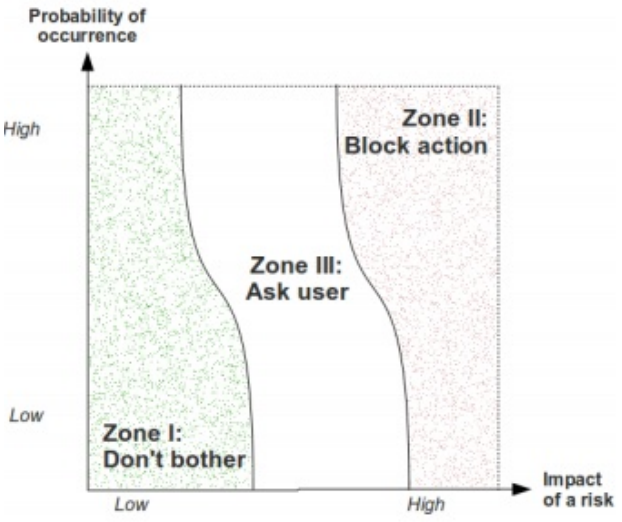


**Figure 4: Risk assesment [15]**

## 3.2 Active warnings

A good step towards creating effective warning is the usage of active warnings. New browsers use active indicators instead of the passive one and force interaction with the user. The warning gives the user choices and recommends the best option, but it is always up to the user to either heed or ignore the suggestion.

A laboratory study [2] was conducted to examine the effectiveness of active warnings. The authors used the Communication Human Information Processing Model (C-HIP) of Wogalter[1] to determine the reasons an indicator is ineffective. The C-HIP model delivers a warning message to the receiver, the receiver verifies five processing steps and the goal is to identify if the warning can change the user behavior. 60 users participated in the study. They were asked to make a purchase from Ebay or Amazon. After finishing the payment they had to check email for purchase confirmation which was a phishing message sent by the examiner. During the whole process the users were asked to think loudly, and after the experiment they had to fill out a survey.

### *3.2.1 Results*

The reaction of the users was recorded as shown in the Figure 5.

| Condition Name | Sample Size | Saw Warning | Read Warning | Recognized Warning | Understood Meaning | Understood Choices |
|---|---|---|---|---|---|---|
| Firefox | 20 | 20 | 13 | 4 | 17 | 19 |
| Active IE | 20 | 19 | 10 | 10 | 10 | 12 |
| Passive IE | 10 | 8 | 3 | 5 | 3 | 5 |

**Figure 5: The number of participants for different conditions [2]**

79% of participants heeded the active warnings, but for passive warnings only one user payed attention to the warning. The results of the processing steps of the (C-HIP) are as follows:

**Attention Switch and Maintenance**: Active warnings interrupt the user's task and forces her to notice the indicators, but due to keystrokes users may never notice passive warnings. Warnings should be effective in a way that it can get the user's attention. Around 55% of the participant claimed to read at least one of the phishing messages completely. 19 participants stated they recognized the message. The users assumed the message is not serious since they had seen it before for trusted websites, thus ignored the message.

**Comprehension/Memory:** This part is to find out if user understands the meaning of the indicators. As shown in Figure 5, most Firefox users claimed they understood the meaning

**Attitudes/Beliefs:** The authors [2] asked the users about their attitudes and belief and how it affected their perception. The answers proved that there is a strong correlation between trust and obeying the warnings. Most of the users stated that since it gave them the option of still proceeding to the website, they thought it couldn't be that serious. Another significant correlation was between knowing the meaning of phishing and paying attention to the message. Having information about phishing made the users obey warnings.

**Motivation**: Overall 31 participants heeded the warning message. The motivation of the participants behavior was that they thought about the risks they might face and they wanted to feel safe. But the rest were unaware about the risks.

### 3.2.2 *Suggestions*

The authors of [2] presented the following suggestions:

- Interrupt users primary task and force her to notice the warning and take an action by active warnings
- Recommend a clear option which is the best choice for the user.
- If an indicator is not read by the users, then the warning should take the recommended action. This means in active warnings if the users close the message without reading it it should prevent the user from visiting the website.
- Indicators must prevent habituation. The more serious warnings should be designed different from less serious ones. In this instance, the users won't recognize and thus will pay attention to the message.
- The warning should be designed in a way that can draw inappropriate trust away from the user, so that the user won't trust for example their anti virus and heed the warning.

## 3.3 Warning design guidelines

Based on the work of [15] some general guidelines for the design of warnings will be discussed in this section.

**Describe the risk clearly:** An indicator should be designed to protect the user from being in an unsafe situation. Every warning should clarify the risk the user might face, the consequences of not heeding to it, and options for avoiding the risk.

**Be concise and accurate:** A warning should be brief but accurate. It should avoid long, technical and offensive text. Technical terms should be replaced with words that are easy to understand for users. At the same time the warning should include enough information that the user can perceive the risk in simple words without being oblivious to it.

**Offer meaningful options:** Indicators should contain two or more choices and it should suggest the best option for the user. Moreover, instead of using options like 'Ok' or 'Cancel' for disregarding the warnings, it is better to use a clear option like 'ignore this warning'. Over and above that, the location of the recommended option must be above all the other choices.

**Follow a consistent layout:** Figure 6 shows a suggested layout for warning messages.

- As shown in Figure 6 critical warnings should not have a close button at the upper right corner of the message, to force the user to read the content.
- The indicator should contain an icon for showing the seriousness of the warning message.
- The primary text of the warning should be a clear single sentence that can convey the importance of the message

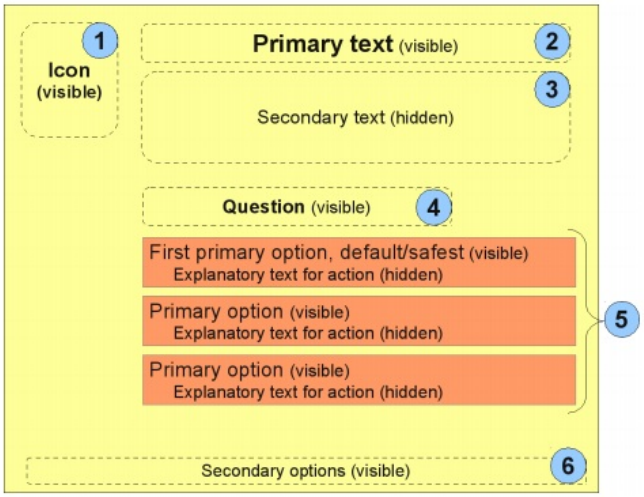


**Figure 6: Warning design guideline [15]**

- The warning should include secondary text for giving more information to the user but it is better to be hidden and be presented if the users clicks the more information option.
- A question should be asked about the action the user wants to take.
- Several options should be provided, and the recommended option should be the first one.
- It is good to use secondary option at the bottom of the message like 'help' which does not respond directly to the question asked from the user

In previous sections the presentation of warnings was discussed. The next section will focus on some social psychological factors used by scammers.

## 3.4 Social psychological factors

The goal is to create less but more effective warnings in order to improve risk communication. The social psychological factors discussed in [3] are: influence of authority, social influence, concrete threats and vague threats, which will be defined as follows:

### 3.4.1 *Influence of authority:*

Scammers are able to defraud users using the influence of authority. The scammers will act in the role of a trusted authority figure. Victims will trust requests from these scammers, since individuals tend to agree to request from authority figures. For example Murphy [9] showed that when the users trust the tax authorities, their willingness to pay taxes will increase. Another example [11] would be that when individuals receive emails from an ostensible doctor which suggests some drugs, they will trust the suggestion since they believe in doctors generally. In this instance, better warning can be created using influence of authority, which leads the users to heed to the warnings presented by a trusted authority figure.


doi: 10.2313/NET-2015-03-1_06

### 3.4.2 Social influence:

Social influence is another factor in social psychology, and it happens when individual thoughts and actions are affected by other people in the society. Being susceptible to social influence is one of the main features of peoples. Design and fashion in a community is a clear picture of social influence[12]. In marketing, the costumer will buy the item that the seller has suggested to her, even if is not her preferred item[13]. A person tends to commit more crimes if she finds out that the other members of the community also comply with committing crimes [10]. In this case, social influence can be considered for creating better warnings. The individuals which are more susceptible to social influence will comply to the request from other people from the society, for example Facebook friends, and will heed or ignore warnings.

### 3.4.3 Concrete and vague threats:

[16] showed that individuals which had already an information about the fraud, or individuals who tried to probe the request sent by the scammer, were less likely to be scammed. Individuals are likely to feel safe and be away from risky situations. Warning messages should be created in a way that present clear information about the negative consequences. Using concrete threats compared to vague ones, helps the individuals to gain more information about the frauds, thus will lead them to pay attention to the warnings.

### 3.4.4 Study:

500 users participated in the survey recruited via Amazon Turk. Five different conditions (warning) were presented to the user shown in Figure 7.

| Condition | Text |
|---|---|
| Control | Control text has been taken from Google Chrome anti-malware warning as of June 2013.[a] |
| Authority | The site you were about to visit has been reported and confirmed by our security team to contain malware. We strongly encourage you to avoid visiting this page. |
| Social Influence | The site you were about to visit contains software that can damage your computer. The scammers operating this site have been known to operate on individuals from your local area. Some of your friends might have already been scammed. Please, do not continue to this site. |
| Concrete Threat | The site you are about to visit has been confirmed to contain software that poses a significant risk to you, with no tangible benefit. It would try to infect your computer with malware designed to steal your bank account and credit card details in order to defraud you. |
| Vague Threats | We have blocked your access to this page. It is possible that it might contain software that might harm your computer. Please close this tab and continue elsewhere. |

**Figure 7: Five different warning texts [3]**

### 3.4.5 Result:

The research [3] showed that concrete threats had the most significant effect on users behavior. In general when users get a clear understanding about the threat and risky situation they can decide better and will heed to the warning. Appeal to authority was another factor which had influenced the users decision. When individuals receive the message from a trusted authority figure they will accept it easier, thus will pay attention to it. Another factor that had an impact on users was social influence. Individuals would click through a warning if their friends told them it is safe.

## 4. CONCLUSION

In this paper first several reasons were presented why the users turned off the browser warnings. Mistrust or trust in automation led the users to make wrong decisions in different situations. Misunderstanding the concept of the warning made the users to ignore or turn off the warnings. Receiving bunch of false positive warnings which later appeared to pose no threat, was another reason for users to don't heed to warning. Some other users think heeding to the warning is waste of time. Also, users won't pay attention to the warnings that appear for a safe high reputation website which user visited before.

For creating less but effective warnings several suggestions were presented. Taking into account the design guidelines given by[15], can help to design an appropriate warning which will have a great impact on users decision. Creating active warnings was another suggestion studied by[2]. Active warnings showed to have a better effect compared to passive indicators since they interrupt the user's primary task and force her to notice the warning and take an action.

Beside focusing just on warning's presentation, other items such as social psychological factors like appeal to authority, social influence, concrete and vague threat can also have a great impact on user's behavior. Scammers used the mentioned items to fraud the victims by introducing themself as an authority figure and by gaining the users trust. The authors [3] mentioned it is best to create concrete warnings. This means that instead of using just a phrase like "'this site might harm your computer"', it is better to use phrases like "' This site wants to steal your bank account details"'. The user needs to get a clear illustration about the consequences of ignoring the warning.
Trusted authority figure was another factor presented in [3] which showed to have a great impact on users behavior. The individuals trusted the warnings that came from a trusted authority.

However, at the end every person has to decide whether she wants to pay attention to the alarms or not. Warning designers should be more accurate in creating indicators. Warnings should be more intelligent and should avoid interrupting the user with useless SSL warnings which are mostly false alarms,. On the other hand they should block the user's action when it is a serious dangerous situation . Beside that people need to increase their knowledge and have got to be carefully taught about security threats. The information about the existing frauds has to be spread very soon through the society.

## 5. REFERENCES

[1] Akhawe, D., Felt, A. P. : *Alice in Warningland: A Large-Scale Field Study of Browser Security Warning*

*Effectiveness*, Paper presented at the USENIX Security Symposium, Washington, D.C, 2013

[2] Egelman, S., Cranor, L. F., Hong, J: *You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings*, New York: Assoc Computing Machinery, 2008

[3] Modic, David and Anderson, Ross J: *Reading this May Harm Your Computer: The Psychology of Malware Warnings*, Available at SSRN: http://ssrn.com/abstract=2374379 or http://dx.doi.org/10.2139/ssrn.2374379,January 3, 2014

[4] Egelman, S., Schechter, S: *The Importance of Being Earnest [in Security Warnings]*,Paper presented at the Financial Cryptography and Data Security 2013, Okinawa, Japan.

[5] Lee, J. D., See, K. A: *Trust in automation: Designing for appropriate reliance. Human Factors*, 2004

[6] Krol, K., Moroz, M., Sasse, M. A: *Don't work. Can't work? Why it's time to rethink security warnings*, Paper presented at the Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on.

[7] Almuhimedi, Hazim, et al: *Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning.*, Symposium on Usable Privacy and Security (SOUPS).,2014.

[8] Herley, C: *So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users.*, Paper presented at the NSPW '09 Proceedings of the 2009 workshop on New security paradigms Oxford, UK

[9] Murphy, K: *The Role of Trust in Nurturing Compliance: A Study of Accused Tax Avoiders*, Law and Human Behavior, 28(2), 187-209. 2004

[10] Kahan, D.M: *Social Influence, Social Meaning, and Deterrence*,Virginia Law Review, 83(2), 349-395 1997

[11] Modic, D., Lea, S. E. G : *Scam Compliance and the Psychology of Persuasion*, Journal of Applied Social Psychology. 2013

[12] Bikhchandani, S., Hirshleifer, D., Welch, I : *A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades*, The Journal of Political Economy, 100(5), 992-1026.1992

[13] Bearden, W.O., Netemeyer, R.G., Teel, J.E : *Measurement of Consumer Susceptibility to Interpersonal Influence*, Journal of Consumer Research, 15(4), 473- 481.1989

[14] *http://fraudavengers.org/scams/*

[15] Bauer, L., Bravo-Lillo, C., Cranor, L., Fragkaki, E. : *Warning Design Guidelines (C. S. Laboratory, Trans.)*, Pittsburgh, PA: Carnegie Mellon University.2013

[16] Titus, R. M., Dover, A. R : *Personal Fraud: The Victims and the Scams*, Crime Prevention Studies, 12, 133-151.2001