# Warning Design Guidelines[*]

Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki
{lbauer,cbravo,lorrie,elli}@cmu.edu
Carnegie Mellon University

February 5, 2013

## 1 Executive summary

This document contains a set of guidelines aimed at helping software designers and developers in designing more effective warning dialogs. These guidelines were compiled from available literature on usable security and warnings research and from Human Interface Guidelines for three broadly used operating systems: Windows, MacOS, and Linux.

A brief description of the guidelines follows:

1. **Describe the risk comprehensively:** Warnings are meant to alert the user of an impending risk to her information or her identity. Whenever a warning is used, the risk that motivates the usage of a warning should be identified and presented clearly.

2. **Be concise and accurate:** Warnings always interrupt the user. If too long, overly technical, inaccurate, or ambiguous, a warning will simply be discarded and its purpose will be lost.

3. **Offer meaningful options:** Warnings should present understandable choices, and enough information to decide between them.

4. **Present relevant contextual information:** In most contexts that require a warning to be shown, a computer or software system cannot make a decision on behalf of the user. Warnings should present relevant contextual information that allows the user to make an informed decision.

5. **Present relevant auditing information:** In some contexts, actions have been performed in the past that may help a user understand the risks associated with the choice she needs to make. In such cases, relevant auditing information should be presented.

6. **Follow a consistent layout:** Warnings that follow a common visual layout can be recognized faster. We suggest a common layout based on the Human Interface Guidelines (HIG) of the most broadly used operating systems.

Section 2 defines and discusses the purpose of warnings, and when a warning should and should not be presented. Section 3 presents each of the previous guidelines in detail, along with comments and examples. Section 4 applies these guidelines to critique a set of deployed warning dialogs.

[*] This work was supported in part by a grant awarded to the University Corporation for Advanced Internet Development (Internet2) under the sponsorship of the U.S. Department of Commerce, National Institute of Standards and Technology; and by NSF grants CNS0831428, CNS1116934, and DGE0903659.

# 2 Introduction

## 2.1 Purpose of this document

This document describes six warning design guidelines based on current literature. The purpose of these guidelines is to help software designers in designing effective warning dialogs to be shown in a computer system. Section 2.2 describes what is understood by a warning in the context of this document.

These guidelines should be applied as part of a systematic effort to design out or minimize the risks to user's safety and privacy, like the "Human Threat Identification and Mitigation Process" described by Cranor [7]. The first four guidelines are general, and should be applicable in any situation wherein a warning is needed. The last two guidelines may help improve warnings in more specific situations.

## 2.2 Warnings definition and purpose

Warnings are communications designed to prevent people from hurting themselves or others [11]. Warnings should serve only as a third-line defense against hazards, in a well-accepted hierarchy known as "hazard control hierarchy" [11]:

1. **Design out the hazard**: eliminate or minimize the hazard if possible.
2. **Guard against the hazard**: limit the contact or interaction between people and the hazard.
3. **Warn about the hazard**.

When designing out a hazard is infeasible or impractical, some guards should be implemented to limit the contact between the person and the hazard. Only when this second step proves infeasible or impractical should a warning be used. For example, if it were possible to replace a dangerous chemical by another that is safer, and that has comparable levels of cost and effectiveness, this should be the preferred solution over other alternatives [11].

However, some hazards are inherent to certain tasks, and cannot be completely eliminated without loss of functionality. For example, using knives and scissors will always involve some level of risk due to their sharp edges. Eliminating completely the sharp edges would render these tools useless.

In computer systems, we understand a warning as a communication that alerts users to take immediate action to avoid a hazard [7]. Five different resources are typically used for this purpose: warning dialogs, notices, status indicators, training material, and policy communications [7]. Warning dialogs signal a hazardous situation where two or more courses of action are available, a decision has to be made by the user, and the designer of the software cannot be certain about which option is less harmful for the user. Notices provide users with information to enable them to make decisions about potentially hazardous situations. Status indicators are passive messages that inform the user about a risk condition, without necessarily asking the user to acknowledge that condition. Neither notices nor status indicators are necessarily meant to interrupt the user [7]. There is evidence that cognitive bottlenecks exist in human visual information processing [4]; there is also evidence that whenever a notice is provided for a threat that does not come to be realized, the perceived reliability of the system decreases, and the tendency to dismiss future signals as unreliable or inaccurate increases [6]. These two pieces of evidence suggest that users' attention should be considered a scarce resource, and should be allocated only when absolutely necessary.

Consent dialogs are a type of warning wherein users are asked to make a binary decision: either consenting or not to a specific course of action, which is assumed to be potentially hazardous. As such, the guidelines contained in this document are also applicable to consent dialogs.

This document assumes that a warning dialog is used as a last resource in a systematic attempt to mitigate the risk before requiring the user to make a decision. The next section describes a systematic approach to determine when the user should be asked to make a decision.

## 2.3 When should a warning be used

There is some evidence [9, 11] that warnings may produce habituation very quickly. When a warning is disregarded before it can be read, it becomes completely useless. A criteria to decide whether it is worth showing a warning is needed.

A risk may be characterized by two features: its probability of occurrence and its impact. The former is more objective (depends mostly of external factors) but often unknown, whereas the latter is subjective (always relative to the user). In an ideal case, a system should be able to estimate both quantities to determine the position of the risk in the graph shown in Figure 1.

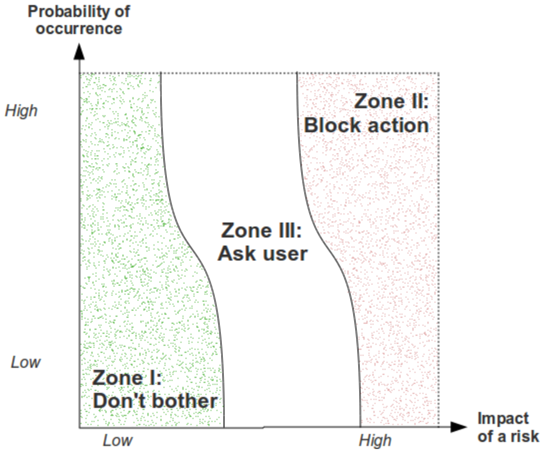


Figure 1: Ideal automatic risk-assessment graph.

In this graph (intended only as a way to depict a concept), three zones are presented. In the first ("Don't bother"), the impact of a risk is so low that it is not worth showing a warning even to let the user know about the risk. In the second, the impact is so high that the action should not be allowed, and thus again the user does not need to be asked. In the third and last zone, the risk is neither high nor low, so depending on the probability of occurrence, the user might be asked what to do.

What can often be estimated by a system (even if only based in expert knowledge embedded in the system) is the probability of occurrence of a risk. Unlike the probability, the impact of the risk is very hard to estimate by a system. Thus, a warning dialog should always be interpreted as an implicit question to the user: "how bad it would be if...?"

The previous notions should be used as part of a process that takes place **before** designing a warning. The main question that should be answered in this process is "should a warning be used in this context?" Along with characterizing the risk, some specifics about computer users' mental models should be considered. The next section summarizes some of these considerations.

## 2.4 Users' mental models of computer warnings

Bravo-Lillo et al. [5] performed a qualitative study wherein a number of experts and lay users were interviewed and asked about their perceptions on computer warnings in several contexts. Figure 2 shows a simplified mental model of the activities performed by computer users when faced with a warning dialog. The model contains three sets of tasks that a user performs immediately after the dialog pops up. In the first set, a user observes and considers several **variables** — factors and events — to try to understand the message communicated by the warning ("Observe and consider..."). Next, the user attempts to **diagnose** what is the problem she perceives she is dealing with ("Diagnose the problem..."). Whether the perceived problem matches the real problem depends on the person's knowledge and experience, as well as other factors. As a consequence of the perceived problem, one or more **actions** are taken ("User reacts"), which finally leads to a situation where either the problem has been solved, or one or more new problems have occurred. The user might or might not be aware of this new problem.

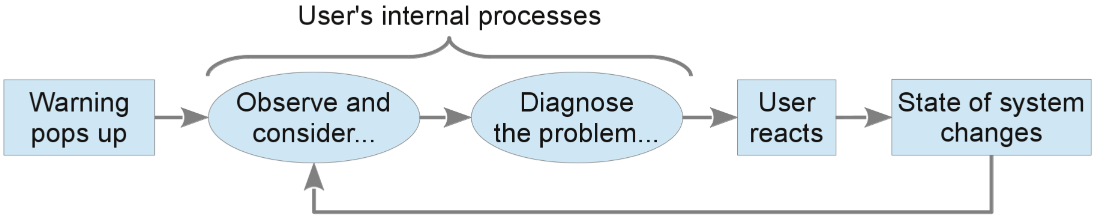


Figure 2: Simplified mental model, showing the sequence of activities performed by users (adapted from [5]).

Examples of variables that a user may consider in the first stage: antivirus software status, origin of the information presented by the warning, and recent activity. Examples of users' judgments in the diagnose stage are: "The computer is infected or has been cracked", "My email has malware on it", and "This might be a phishing website." Examples of actions performed by users, with both positive and negative consequences: use secure connections tools, stop surfing, disable security mechanisms, and contact someone trusted with more experience.

Table 1 summarizes the main conclusions of the study, along with possible ways to counteract the negative consequences of each conclusion.

| # | **Observation** | **Possible correction** |
|---|---|---|
| 1 | Users usually do not read warning messages, unless they do not visually recognize the warning or they do not know how to respond to it. | Egelman et al. reported on several techniques to capture user's attention in warnings presented within a browser [8]. These techniques are presented in the guidelines later in this document. |
| 2 | Novice users usually do not consider many of the variables that advanced users do. | Present the variables that might be relevant to the novice user. |
| 3 | Novice users usually consider variables in the wrong order. | Present the information in a meaningful order. |
| 4 | Novice users often consider the wrong variables. | Tell the user about the options she should not consider.<br>Present the possibly offending application in a distorted fashion, for example, shaded. |
| 5 | Novice users do not keep in mind a dynamic image of the state of their computers. | Keep a detailed log of all security relevant operations performed by applications and by all the users of the system. Present part of this information whenever relevant for the user.<br>Offer information about the status (Running? When last updated?) of the security software installed in the system. |
| 6 | Novice users don't look for vulnerabilities in public expert forums (on the Internet) that may aid them in dealing with common problems. | Since it's not realistic to ask novice users to check expert forums, this information should be gathered and presented when most appropriate.<br>Include a link to the official software support site, maintained by the software vendor. |
| 7 | Novice users are usually not aware of the consequences of their actions. | Offer a brief explanation of the consequences of every option. |
| 8 | Novice users usually assess the safety of an action **after** engaging on it, while advanced users do so before. | If an option is not safe for the user, offer a brief explanation of the reason right next to the option. |
| 9 | When the information they have gathered for their decision is insufficient, novice users usually do not gather more information; instead, they discard the information and decide they have no problems. | Present all available information to the user in a progressive fashion, and convey the seriousness of the hazard through an adequate combination of color and words. |
| 10 | Novice users do not understand many common technical terms, and often become confused and frustrated when they are presented with them. | Offer a brief definition or explanation of the technical term, based on a trusted source. |
| 11 | All users try to understand the options being presented to them before reading the description of the warning. As a result, they might misunderstand a warning if the labels of the options are not clear. | Offer longer and meaningful explanations for the options, if possible. |
| 12 | Novice users often feel discouraged to read a warning dialog when the message is long. | Make the text useful, understandable, and engaging. |

Table 1: Summary of conclusions from study on warnings [5]

# 3 Guidelines

## Guideline 1: Describe the risk comprehensively

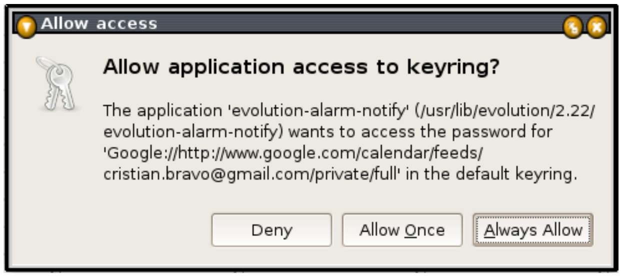
| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 1.a | A warning message must clearly specify the underlying risk. | [8, 11] |
| 1.b | A warning message should clearly describe the consequences of not complying with the intended course-of-action. | [8, 11] |
| 1.c | A warning message should include instructions on how to avoid the risk, unless these instructions are obvious in the statement of the risk. | [8, 11] |

**Comments:**

Every warning should be designed to protect the user from a risk. This risk should be stated clearly, along with instructions for avoiding it and the consequences of not avoiding it. The warning should be displayed when the user can still take a preventive action.

If the user is not aware of the risk or does not understand the risk, she might simply dismiss the warning and believe it has no importance. If the user is aware of the risk but doesn't know how to comply after reading the warning, she might feel frustrated with this particular message. If she understands the risk, understands how to comply with the warning, but believes that the consequences of not complying are not important, the user might not comply since she might perceive that complying is not worth the effort.

**Examples:**



**Allow application access to keyring?**

The application 'evolution-alarm-notify' (/usr/lib/evolution/2.22/evolution-alarm-notify) wants to access the password for 'Google://http://www.google.com/calendar/feeds/cristian.bravo@gmail.com/private/full' in the default keyring.

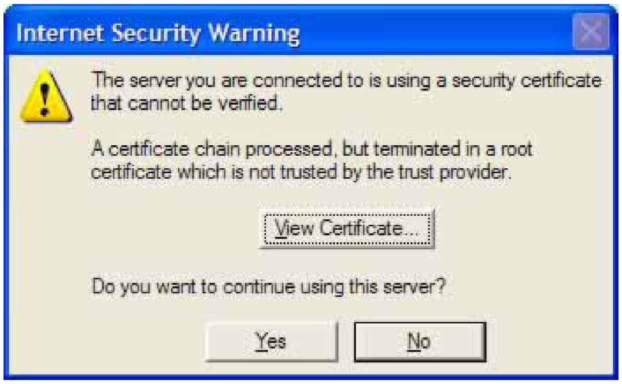
An Ubuntu 10.04 warning dialog triggered by the Gmail plugin[a] for the Evolution application suite v2.22[b].

[a] https://help.ubuntu.com/community/GoogleCalendarWithEvolution

[b] https://help.ubuntu.com/community/Evolution

In this dialog, the risk is not stated at all; the consequences of user's actions are not indicated, and there are no instructions on how to comply except for the labels on the buttons. A better design would include:

1. A statement about the risk (e.g., "You might be disclosing private information to this application"),
2. Instructions on how to comply (e.g., "If you were expecting this application to access your password, click on..."),
3. Consequences of not complying (e.g., "This application will have complete access to your calendars and appointments").



Internet Security Warning

The server you are connected to is using a security certificate that cannot be verfied.

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Do you want to continue using this server?

A Windows XP dialog triggered both by Outlook 2010 and the Office 2007 suite.

In this dialog, the risk can be understood only by an expert user. The problem is described from the software's viewpoint instead of the user's. There is no statement about the consequences of not complying, nor there are instructions about how to comply. A better design would include:

1. A statement about the risk (e.g., "This server might not be who it claims to be"),
2. Consequences of not complying (e.g., "A possibly unknown third-party will have access to the information you create or share with this application"),
3. Instructions on how to comply (e.g., "Check the certificate and decide if you want to trust this site...").

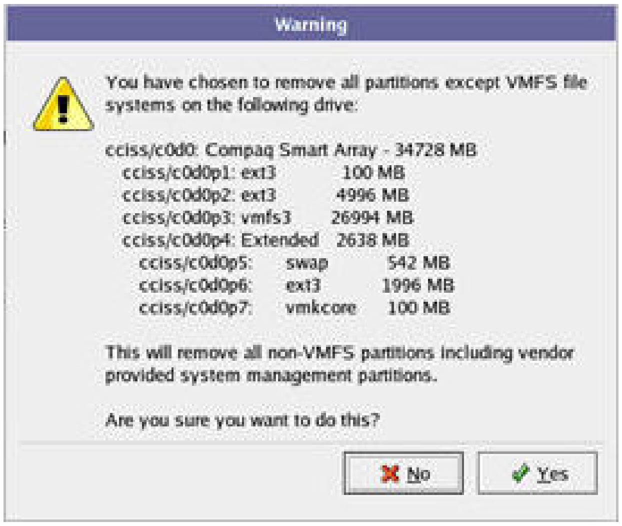
## Guideline 2: Be concise and accurate

| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 2.a | The warning message must be brief. Remove redundant text. | [1, 2, 3, 11] |
| 2.b | The warning message should stated from the user's viewpoint, and not from the designer's or the computer's viewpoints. Avoid technical jargon; replace technical terms by phrases or expressions that might be better understood by the user. Some examples of terms replacements suggested by MS Windows HIG are:<br>1. Do not use the terms **caution**, **danger** or **warning**. The warning icon, if present, should convey those meanings.<br>2. Do not use **error** or **failure**: Use **problem** instead.<br>3. Do not use **failed to**: Use **unable to** instead.<br>4. Do not use **illegal**, **invalid**, **bad**: Use **incorrect** or **not valid** instead.<br>5. Do not use **abort**, **kill**, **terminate**: Use **stop** instead.<br>6. Do not use **catastrophic**, **fatal**: Use **serious** instead. | [1, 2, 3, 8, 11] |
| 2.c | Avoid ambiguous terms: provide specific names, locations, and values of the objects involved. | [3, 10] |
| 2.d | Be polite, supportive, and encouraging | [3] |

**Comments:**

This guideline represents a trade-off between the amount and the quality of information included in the warning. The user should be presented with only enough information for making an informed choice (and no more). Some warnings might sound overly technical, strong, or even offensive to the average user. The text should be polite and encouraging when possible, without being inaccurate. If the warning message is long, uses technical terms, or is presented in an intimidating or offensive tone, the user will not only dismiss it but will develop a negative predisposition toward warnings. At the same time, if a warning does not present enough information for the user to make a reasonable choice, the user can only choose blindly from the presented options. Replace technical terms (“website certificate”, “antivirus software”) by common language descriptions (“site’s identity details”, “security program”). Where possible, all ambiguous references (e.g., “the sender”, “the program”) should be replaced with available information (e.g., “abc@gmail.com”, “the security program from NetShield Inc.”).

**Examples:**



Warning

You have chosen to remove all partitions except VMFS file systems on the following drive:

```
cciss/c0d0: Compaq Smart Array - 34728 MB
  cciss/c0d0p1: ext3        100 MB
  cciss/c0d0p2: ext3       4996 MB
  cciss/c0d0p3: vmfs3     26994 MB
  cciss/c0d0p4: Extended   2638 MB
    cciss/c0d0p5:    swap      542 MB
    cciss/c0d0p6:    ext3     1996 MB
    cciss/c0d0p7:    vmkcore   100 MB
```

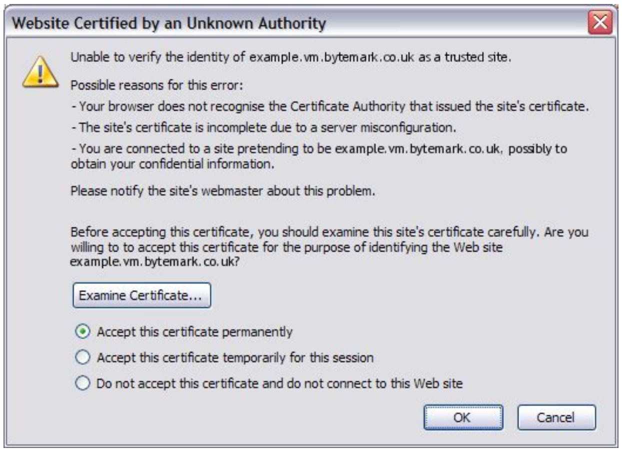
This will remove all non-VMFS partitions including vendor provided system management partitions.

Are you sure you want to do this?

Dialog shown during the installation process of Fedora Linux 9 [a] on a computer with an HP Smart Array RAID controller.

In this dialog, the information presented in the first paragraph is restated almost verbatim in the paragraph before the question. A better design would merge these two paragraphs in a single more compact statement (e.g., “You are about to remove all non-VMFS partitions on the drive shown below, including vendor provided ones: ...”).

[a] http://fedoraproject.org/



Website Certified by an Unknown Authority

Unable to verify the identity of example.vm.bytemark.co.uk as a trusted site.

Possible reasons for this error:

- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be example.vm.bytemark.co.uk, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site example.vm.bytemark.co.uk?

● Accept this certificate permanently

○ Accept this certificate temporarily for this session

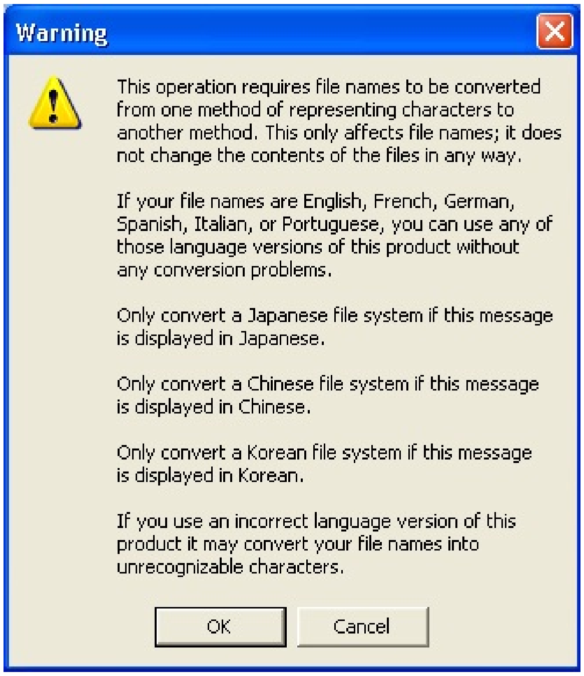
○ Do not accept this certificate and do not connect to this Web site

Dialog presenting a certificate problem in the email client Thunderbird version 2, running on Windows Vista.

This dialog is triggered when the user attempts to connect to a mail server that issues a certificate not recognized by Thunderbird [a].

This dialog contains many technical terms that confuse all but the most expert users (“Certificate Authority”, “site’s certificate”, “server misconfiguration”, etc.). A better design would consider replacing these terms with less technical explanations.

[a] http://www.mozilla.org/en-US/thunderbird/



Warning

This operation requires file names to be converted from one method of representing characters to another method. This only affects file names; it does not change the contents of the files in any way.

If your file names are English, French, German, Spanish, Italian, or Portuguese, you can use any of those language versions of this product without any conversion problems.

Only convert a Japanese file system if this message is displayed in Japanese.

Only convert a Chinese file system if this message is displayed in Chinese.

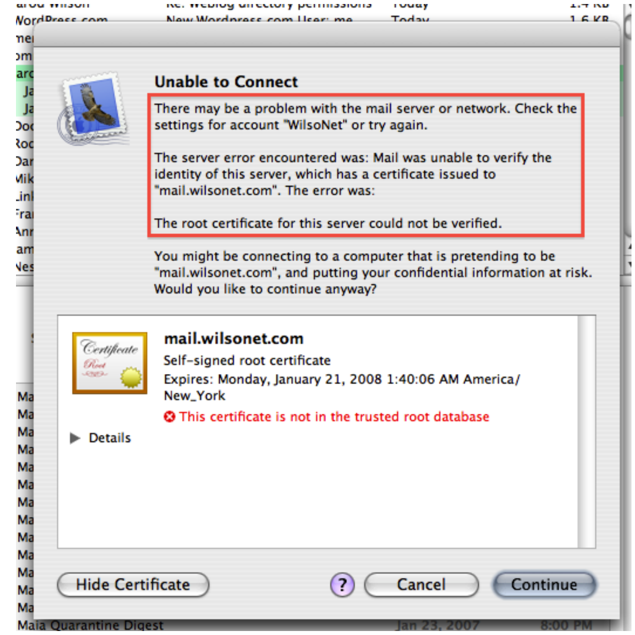
Only convert a Korean file system if this message is displayed in Korean.

If you use an incorrect language version of this product it may convert your file names into unrecognizable characters.

Dialog triggered by Partition Magic 8 (discontinued) on Windows XP.

The message in this dialog is long and includes technical information that should not be conveyed to the user.

Since the language of the warning depends on internal options that are probably available internally to the message, this dialog could be avoided completely by automatically determining which language is being used and utilizing that information to make a decision on the user’s behalf.



**Unable to Connect**

There may be a problem with the mail server or network. Check the settings for account "WilsoNet" or try again.

The server error encountered was: Mail was unable to verify the identity of this server, which has a certificate issued to "mail.wilsonet.com". The error was:

The root certificate for this server could not be verified.

You might be connecting to a computer that is pretending to be "mail.wilsonet.com", and putting your confidential information at risk. Would you like to continue anyway?

**mail.wilsonet.com**

Self-signed root certificate

Expires: Monday, January 21, 2008 1:40:06 AM America/New_York

This certificate is not in the trusted root database

Dialog triggered by the Apple Mail.app on Mac OS X.

This dialog is triggered on a failed attempt to connect to a mail server through the IMAP protocol, from the Mail application on Mac OS.

This dialog has redundant text (e.g., "There may be a problem...", "The server error encountered...", "The error was..."). Multiple versions of the problem are presented in the first three paragraphs, which is very confusing for the non-expert user.

A better design would be obtained by removing the text enclosed in the red box, since information in this box is already presented more accurately in the "progressive disclosure"[a] zone of the dialog.

[a] For more information about "Progressive Disclosure", please see [1].

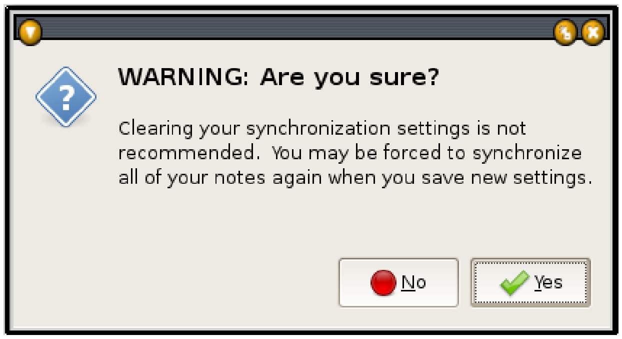
## Guideline 3: Offer meaningful options

| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 3.a | A warning dialog should present a decision to be made, not a dilemma. Provide enough information to the user to allow him or her to make a safe decision. | [10] |
| 3.b | A safe choice should always be presented and be the default option. The safest choice should be located above all others. | [1, 2, 3, 8, 9, 10] |
| 3.c | Do not label the close action as 'OK', 'Close' or 'Cancel'. Instead, prefer labels as 'Ignore this warning' or 'Cancel the update', which make explicit the choice being taken to the user. | [8, 9] |
| 3.d | A warning dialog must have two or more options. If it has only one option, it should be considered a notification; if it does not have any, it should be considered a status indicator. | [7, 10] |

### Comments:

It should always be possible to determine which available option is the safest. Make that option the default one, and locate it in the lower right corner. If there is any keyboard shortcut by default (the 'enter' or 'space' keys), associate that shortcut with the default. Because "[u]sers are far more likely to read command button labels than static text" [3, 10], it should be possible for them to read the question and the labels of the options, and to make a choice without reading the secondary text. The only requisite is that of consistency between the questions and the options; however, since users seem to look first at the labels in buttons, longer and more meaningful labels for the buttons are recommended. When users don't understand the options presented, or when they want to dismiss the warning without reading the options, they often pick the default option as a way of getting rid of the dialog without thinking about it [9]. In these cases the warning should offer the safest option as default, thus not exposing the user to unnecessary risk.

**Examples:**



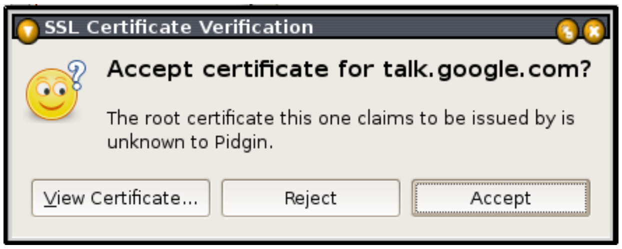
WARNING: Are you sure?

Clearing your synchronization settings is not recommended. You may be forced to synchronize all of your notes again when you save new settings.

Dialog triggered by Tomboy 1.6, a note-taking application in Ubuntu 10.04.

This dialog presents an example of a dilemma presented to the user. The dialog is triggered when the user chooses an option labeled "Clear synchronization settings" in a Linux-based note-taking software.

This is an example of presenting a "dilemma" to the user. There is not enough information for the user to decide what choice to make or why this choice is important. The presented question is ambiguous, and the options are thus meaningless ("Why is this action not recommended? What will I lose if I choose 'Yes'? What does it mean 'to synchronize all the notes again'?").



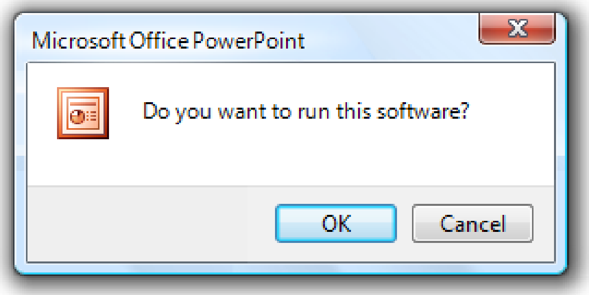
SSL Certificate Verification

Accept certificate for talk.google.com?

The root certificate this one claims to be issued by is unknown to Pidgin.

Dialog triggered by Pidgin 2.0, a text messenger client in Ubuntu 10.04.

In this dialog, the safest choice ("Reject") is in the middle. The default option ("Accept") is also the riskiest, and is located to the right.

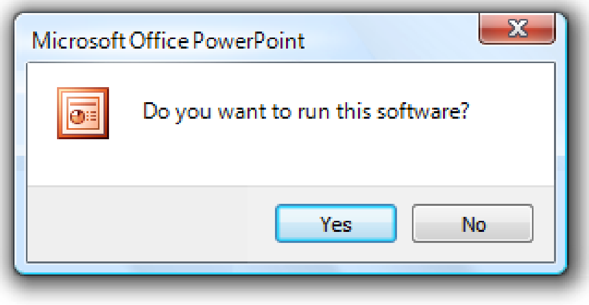


Microsoft Office PowerPoint

Do you want to run this software?

Example of a dialog taken from the Windows Vista/7 Human Interface Guidelines [3].

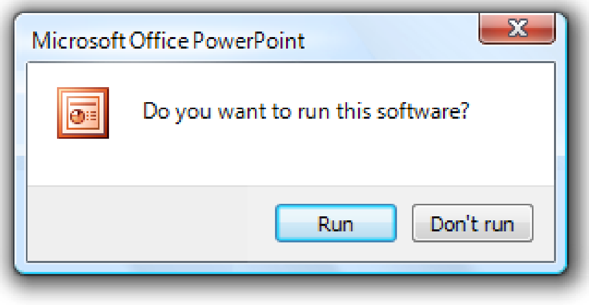
Example of poor options in response to a question. The options in this dialog are not answers to the question asked of the user.



Do you want to run this software?

Example of a dialog taken from the Windows Vista/7 Human Interface Guidelines [3].

In this dialog, the options are possible answers to the question, but more meaningful labels would be preferred.



Do you want to run this software?

Example of a dialog taken from the Windows Vista/7 Human Interface Guidelines [3].

This dialog shows options with labels that correspond to meaningful answers to the question asked of the user.

## Guideline 4: Present relevant contextual information

| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 4.a | If the hazard involves deciding whether to run an unknown or unverified application, if appropriate, tell the user:<br>1. Its name, execution path, and the rights of the user that might execute it,<br>2. Whether or not the application has been checked by the antivirus program,<br>3. The current state of the antivirus program,<br>4. Whether a record of the access will be kept for the user to audit. | Observations 2–8 (see Table 1). |

| | | |
|---|---|---|
| 4.b | If the hazard involves deciding whether to let an unknown agent obtain access to a known object, if appropriate, tell the user:<br>1. What information is being accessed,<br>2. What kind of access is being requested (creating, reading, updating, deleting, other),<br>3. An assessment obtained from a trusted source about the agent,<br>4. The most likely reasons why this information might be accessed,<br>5. Whether a record of the access will be kept for the user to audit. | Observations 2–8. |
| 4.c | If the hazard involves deciding whether to let a known agent obtain access to an unknown or unspecified object, if appropriate, tell the user:<br>1. Whether the accessed information might include the user's personally identifiable information,<br>2. Whether a record of the access will be kept for the user to audit,<br>3. The identification of the accessing agent. | Observations 2–8. |
| 4.d | If the hazard involves deciding whether to trust a previously unknown agent for a known purpose, if appropriate, tell the user:<br>1. All available information about the unknown agent that might reasonably allow the user to decide whether she knows the agent (e.g., a human-readable name, a TLD DNS domain, an email address; not an IP, not a full URL, not a PKI certificate),<br>2. What is the scope of trust (i.e., what the agent is being trusted for),<br>3. Whether a record of the access will be kept for the user to audit. | Observations 2–8. |
| 4.e | If the hazard involves deciding whether to trust a known agent for an unknown or unspecified purpose, if appropriate, tell the user:<br>1. What information might be accessed by the agent now or in the future,<br>2. How long the agent will be granted access,<br>3. What kind of access will be granted (creating, reading, updating, deleting, other),<br>4. Whether a record of the access will be kept for the user to audit,<br>5. Whether the audit log includes a history of accesses granted to this agent. | Observations 2–8. |
| 4.f | If there are any important options that have been discarded before presenting the warning, briefly describe what are those options and why they were discarded. | Observations 4 and 5. |

| | | |
|---|---|---|
| 4.g | If the hazard involves deciding whether to send information over an unsecured channel, scan the information for obvious pieces of personally identifiable information (PII) (SSNs, credit card numbers, email addresses, etc.). If no PII is found, ask the user to evaluate the sensitivity of the information being sent (for example, on a 5-point Likert scale). Only display a warning either if PII was found, or the user declares that the information is very sensitive to her. In this case, let the user know that the information being sent can be eavesdropped by unknown third parties. | Observations 2–8. |
| 4.h | If the warning was triggered by a known application, include a link to the public online forum that the software vendor maintains for the application. | Observations 2, 4–6, and 8. |

**Comments:**

This guideline describes common scenarios where contextual information (usually not presented) might be helpful to the user. An example for guideline 4.f follows: Executing an unknown application is hazardous due to at least two not mutually exclusive risks:

1. The application might be malware,
2. The application might access and misuse the user's personally identifiable information.

A smart operating system would discard the first alternative by executing an antivirus program first. If the antivirus program reports that the application is free from known malware, then a warning should be triggered alerting the user about the second alternative. In this case, the warning message should also tell the user that the application has been checked and is free from known viruses.

## Guideline 5: Present relevant auditing information

| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 5.a | An application triggering warning dialogs should keep a private record of:<br>1. Access granted to the information it keeps or manages (who, what, when, what for),<br>2. Access requested to information that other applications manage (what, when, what for),<br>3. Changes introduced to the information it keeps or manages (who, what, when). | Observations 5 and 9. |
| 5.b | A warning dialog should include selected portions of the audit record, relevant to the hazard being warned about. If there is too much relevant information to be presented in the dialog, the dialog should present a link to the audit log. | Observations 5 and 9. |

**Comments:**

An example of guideline 5.b follows: Accessing what is, from the perspective of a computer, an unknown website might be risky because it might be a phishing attempt that, e.g., mimics a bank's website through a fake domain. In this case, the computer may recognize that the domain is being accessed for the first time. Hence, the application accessing the website (likely a browser) should display a warning displaying the fact (based on the audit log) that this website has not previously been visited by the user. If it is not the user's first visit to her bank's website, this should alert her that something anomalous is happening.

## Guideline 6: Follow a consistent layout

| *Id* | *Guideline* | *Ref. or origin* |
|---|---|---|
| 6.a | A critical warning dialog should not have a ‘close’ button in the upper right corner. | [9, 8] |
| 6.b | A warning dialog should use only one icon. This icon should be used to convey the level of urgency to the user. | [1, 8, 2, 11] |
| 6.c | A critical warning should shade the rest of the screen while being shown. The used dialog should be modal (no interaction is possible with any other application until the dialog has been dismissed). | Observations 1, 9, and 11.Also [9, 8]. |
| 6.d | A warning dialog should have a primary text, which should not be longer than a single, correctly expressed sentence in newspaper style. | [1, 2] |
| 6.e | If necessary, a warning dialog may have secondary text giving more information about the risk than contained in the primary text. The secondary text should be composed in a conversational style. | [1, 2, 10, 3] |
| 6.f | A warning dialog should pose an explicit question to the user, immediately above the options. | [1, 2, 10, 3] |
| 6.g | A warning dialog must have two or more options below the question. It is recommended that all options are presented as *command links* instead of regular buttons. Each option should have a brief description of the action, presented in a large font, and a brief explanatory text, if necessary, presented in a small font immediately below the description. | Observations 7–9 and 11. Also from the experience that is usually very hard to find one or two words (the label of a button) to adequately convey the meaning of the available options. The usage of command links allows to include longer explanations and keep these in the context of each option. |
| 6.h | All presented options should be possible answers to the explicit question. | [1, 2, 10, 3] |
| 6.i | According to guideline 2.b, a warning dialog should not contain technical terms. However, when it is not easy to replace such a term with non-technical words, transform the term into a link that, when clicked, displays a very small pop-up offering a definition or an explanation of the term. | Observation 10. Often it is not possible to completely avoid technical terms, and defining these in non-technical terms makes the message prohibitively long. |

**Comments:**

Human Interface Guidelines (HIG) are software development documents, written by and for software developers, containing advice on how to use effectively the visual elements (dialogs, toolbars, buttons, etc.) that some software offers to the users of that software. All three main HIG reviewed [1, 2, 3] broadly follow a common layout for warnings. Our suggested layout is presented in Figure 3, and has been included here an example of how to structure the information in a warning.

The suggested layout contains the following elements:

1. A single **icon**, put to orient the user to the severity level of this message. This icon is always visible.
2. A **primary text**, which explains the reason of the warning. This text is always visible.
3. A **secondary text**, which gives additional information about the warning, if necessary. This text may be initially hidden, and shown when the user clicks on the secondary option ‘More information’.
4. A **question**, directly posed to the user. This text should be always visible.

5. A set of **primary options**, in which the default and safest one should be placed above the others. These options should be presented as command links [1]. The options should be ordered from top (the default and safest option) to bottom (the most hazardous or difficult to follow). Each of these primary options include:

   (a) A description of the action, in a larger font, beginning with a verb. All these descriptions are always visible.

   (b) A brief explanatory text of the action, in a smaller font. These texts are initially hidden, and shown when the user clicks on the secondary option 'More information'.

6. A set of secondary options. These options don't respond directly to the question posed to the user. The most common secondary options are 'Help', 'Ignore this warning' and 'More information'. 'More information' should always be present, and is supposed to toggle between showing and hiding the elements that are initially hidden in the warning.

Some more comments about the guidelines:

1. Guideline 6.c implies the usage of modal interaction dialogs when presenting a warning. A modal interaction dialog takes control of the application being used and prevents any interaction between the user and the application until an option from the warning has been selected. This guideline has been described in detail by Egelman et al. [9, 8]. If the message is critical, and if designing out or guarding against the risk is not feasible or practical, the warning should be presented in a way that prevents the user from inadvertently or willingly dismissing the warning before having obtained all the relevant information or without having made a conscious choice. As a particular application of this guideline, a 'close' icon in the upper right corner provides the user with an easy way of dismissing the warning dialog without reading the message.

2. **Newspaper style** in 6.d is described in [2] as a complete sentence, with the first letter of the first word capitalized, not ending with a period but possibly with a question mark (and never with an exclamation sign). The sentence should convey the essence of what is being communicated.

3. **Conversational style** 6.e is described in [3] as follows: "Imagine yourself looking over the user's shoulder and explaining how to accomplish the task." If a pronoun is needed, use a second-person pronoun to address the user.

[1] Command links are part of the Human Interface Guidelines of MS Windows Vista and MS Windows 7 [3]; see `http://msdn.microsoft.com/en-us/library/aa511455.aspx`

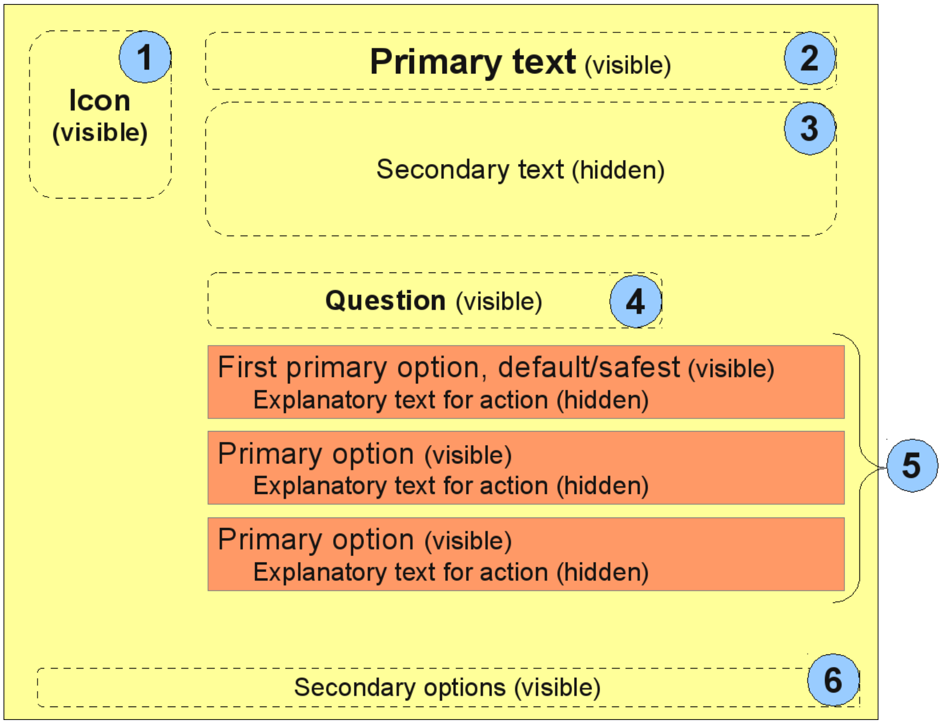
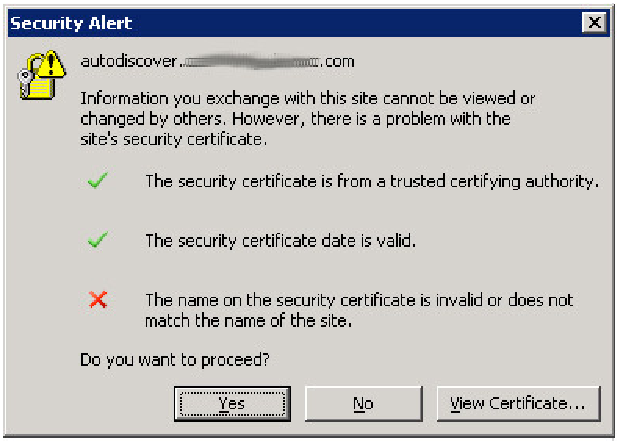

1
Icon (visible)
Primary text (visible)
2
3
Secondary text (hidden)
Question (visible)
4
First primary option, default/safest (visible)
Explanatory text for action (hidden)
Primary option (visible)
Explanatory text for action (hidden)
Primary option (visible)
Explanatory text for action (hidden)
5
Secondary options (visible)
6

Figure 3: Suggested warning dialog layout.

**Examples:**



autodiscover.[redacted].com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

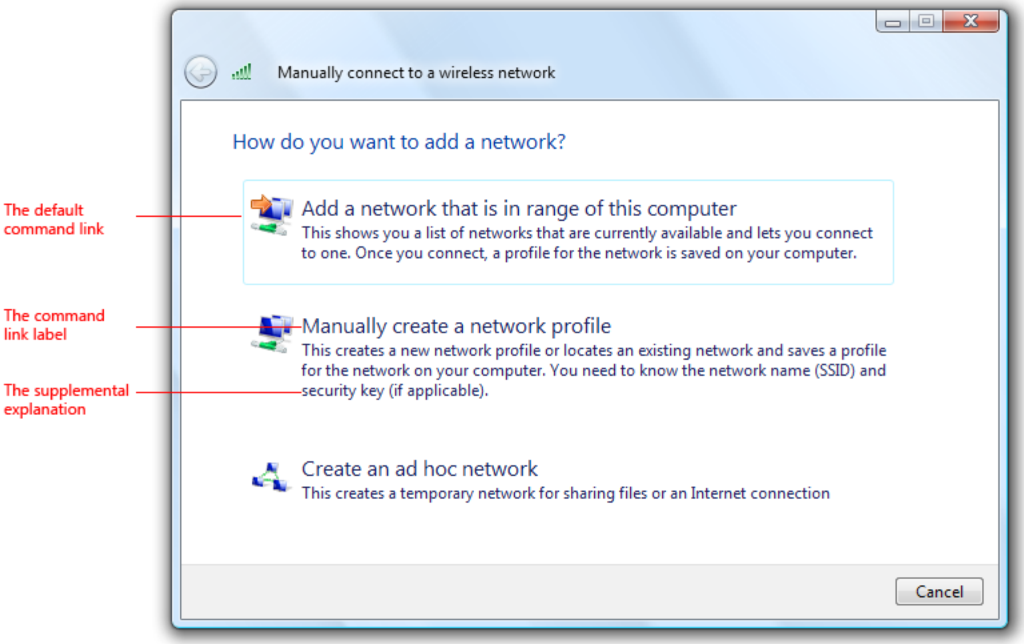
✓ The security certificate date is valid.

✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

SSL certificate problem dialog displayed by MS Outlook 2010.

This dialog includes a main icon at the left, and additional icons to indicate conditions that might be relevant to the warning. The inclusion of additional icons (specially of tick/cross icons) might be confusing to users, either giving a false sensation of security ("since there are two tick signs, this can't be that bad") or by distracting users from the message conveyed by the main icon.



Manually connect to a wireless network

How do you want to add a network?

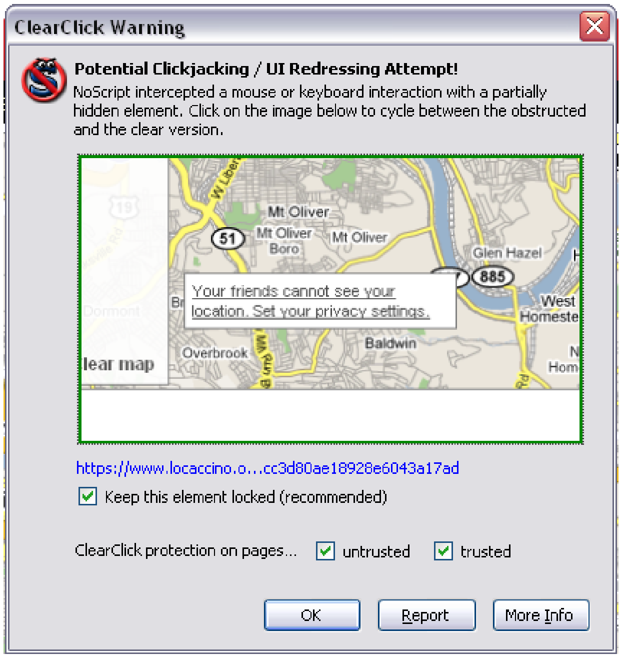
Add a network that is in range of this computer
This shows you a list of networks that are currently available and lets you connect to one. Once you connect, a profile for the network is saved on your computer.

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

Figure 4: An example of the usage of command links, taken from the Windows Vista/7 Human Interface Guidelines [3].

---



ClearClick Warning

**Potential Clickjacking / UI Redressing Attempt!**
NoScript intercepted a mouse or keyboard interaction with a partially hidden element. Click on the image below to cycle between the obstructed and the clear version.

Your friends cannot see your location. Set your privacy settings.

https://www.locaccino.o...cc3d80ae18928e6043a17ad

☑ Keep this element locked (recommended)

ClearClick protection on pages... ☑ untrusted ☑ trusted

Dialog displayed by NoScript 2.x, an add-on for Firefox, on Windows XP.

This dialog is triggered by NoScript, a security add-on installed in Firefox, when the user visits a website that attempts to fraudulently interact with a web page on the user's behalf.

This warning does a poor job at conveying an important risk, and it violates the guideline by offering an easy way of dismissing the dialog (the 'close' button in the upper right corner). If the information is worth presenting to the user, the dialog should not provide a way of dismissing it before the information could be read and understood by the user.

---

# 4 Examples of warnings relevant to identity management

Each of the examples in this section includes a screenshot of a dialog, along with a brief explanation of the interactions that led to the dialog popping up on user's screen. A number of observations are then presented for every guideline. Observations that begin with a plus or minus sign are to be considered positive or negative, respectively, whereas a question mark denotes an observation that is to be pondered depending on the specific situation.

A potential confusion between apps and websites in lay users should be kept in mind while checking the examples in this section.

## 4.1 Vimeo and Facebook

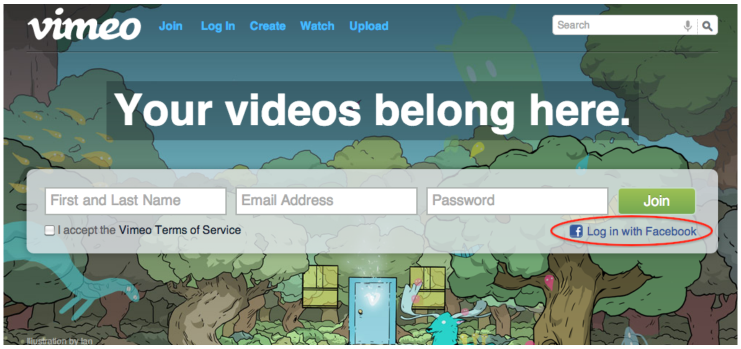
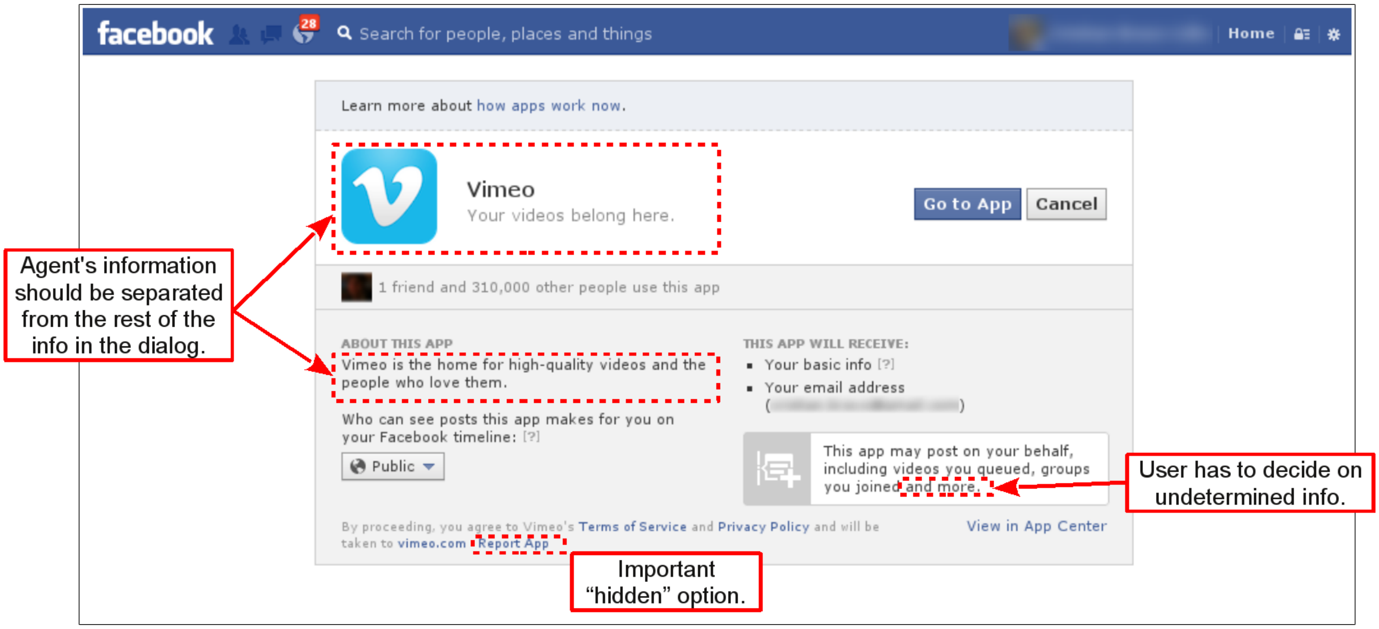


Figure 5: Vimeo website (www.vimeo.com) with a "Log in with Facebook" link. Accessed 01/31/2013.



[redacted]

Learn more about how apps work now.

Vimeo

Your videos belong here.

Go to App | Cancel

1 friend and 310,000 other people use this app

ABOUT THIS APP

Vimeo is the home for high-quality videos and the people who love them.

Who can see posts this app makes for you on your Facebook timeline: [?]

Public

THIS APP WILL RECEIVE:

- Your basic info [?]
- Your email address ([redacted])

This app may post on your behalf, including videos you queued, groups you joined and more.

By proceeding, you agree to Vimeo's Terms of Service and Privacy Policy and will be taken to vimeo.com · Report App

View in App Center

Agent's information should be separated from the rest of the info in the dialog.

User has to decide on undetermined info.

Important "hidden" option.

Figure 6: Facebook confirmation dialog. Accessed 01/31/2013.

**Interaction:** A typical interaction with Facebook as an identity provider is presented above. When a user visits `www.vimeo.com` (Figure 5), the "Log in with Facebook" option is presented as a method for logging in (Figure 5, red oval). Assuming that the user has previously logged into Facebook (and her browser has a cookie identifying her), then when the user clicks on "Log in with Facebook" she is taken to the Facebook website, which presents her with a confirmation dialog (Figure 6).

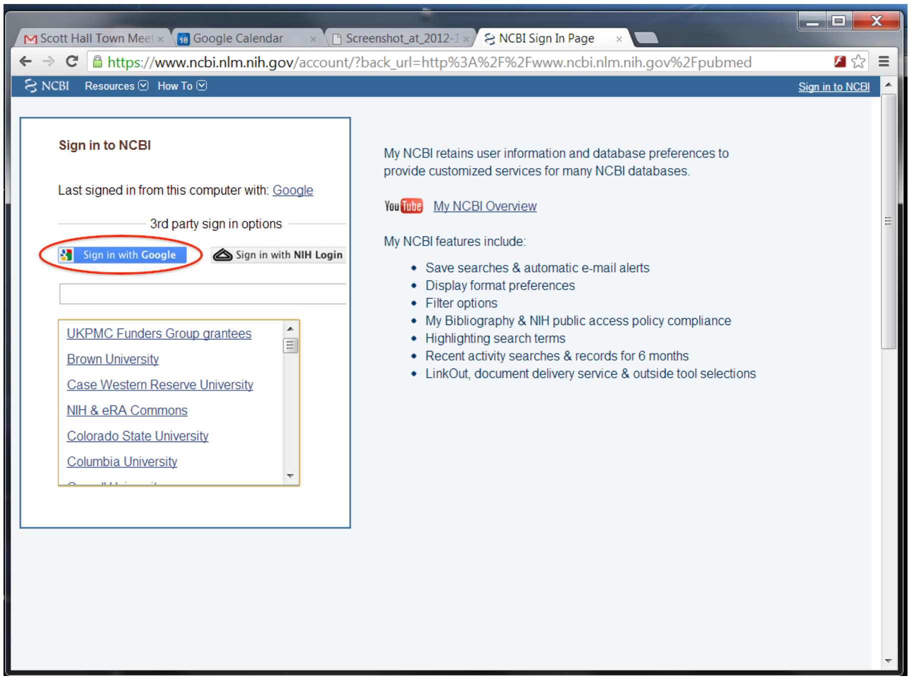
**Risk assessment:** From the point of view of the user, the dialog should be considered a warning. The user has to decide whether to grant this (possibly) unknown application access to her basic information and her email address, and whether to allow the application to post on her behalf in an undetermined set of places. The main risk is a privacy violation, which may be understood as a mismatch between the manner in which the application will use the user's information and user's expectations of such usage. Since these expectations come from the perceived purpose of the application, making this purpose explicit is important.

## Comments

| *Guideline* | *Observations about the guideline* | *Possible Improvements* |
|---|---|---|
| Describe the risk comprehensively | [-] There is no explicit description of the risk.<br>[-] There is no description of the consequences of the risk.<br>[-] There is no actionable advice to avoid the risk. | Present the risk explicitly.<br>Describe the consequences in case the danger is realized.<br>Give actionable advice to avoid the risk. |
| Be concise and accurate | [+] Message length is appropriate.<br>[+] The message is described from the point of view of the user (e.g., "Your basic info", "Who can see posts this app makes for you", "By proceeding, you agree to...").<br>[+] No technical jargon is used. | |
| Offer meaningful options | [-] The choice presented is a dilemma. There is not enough info presented through the dialog for the user to make an informed choice.<br>[-] An important safe choice ("Report App") is presented in small font.<br>[-] The default option ("Go to App") is not safest.<br>[-] The "Cancel" option is ambiguous. What is canceled if the user clicks "Cancel"? | Replace "Cancel" by "Block app" or "Deny access to this app". Make a safe option (either "Report app" or "Cancel") the default. |

| | | |
|---|---|---|
| Present relevant contextual information | [-] The hazard involves deciding whether to let an unknown agent obtain access to undetermined information about the user (“This app may post on your behalf... groups you joined **and more**”), and this information is not reachable.<br>[+] The user is asked to trust a possibly unknown agent, and this agent is sufficiently identified.<br>[-] Information about the agent should be presented separately from the rest of the information in the warning. | If possible, put all of a user’s info that will be passed to the agent into the dialog. If not possible, provide a link to this info. |
| Present relevant auditing information | Possibly not applicable | |
| Follow a consistent layout | [-] There is no explicit question for the user (what is the user being asked to do?).<br>[-] Relevant options (“Go to App”, “Cancel”, and “Report App”) are not visually equally important.<br>[-] Information on top (“Learn more about how apps work now”) is important, but should be presented after presenting the decision to be made.<br>[-] Information is scattered throughout the dialog. It’s not easy to make sense of it. | Pose an explicit question to the user (e.g., “Do you trust this App with your private information?”)<br>Reorganize the info to make it more accessible. |

## 4.2 NIH and Google



Sign in to NCBI

Last signed in from this computer with: Google

3rd party sign in options

Sign in with Google

Sign in with NIH Login

UKPMC Funders Group grantees
Brown University
Case Western Reserve University
NIH & eRA Commons
Colorado State University
Columbia University

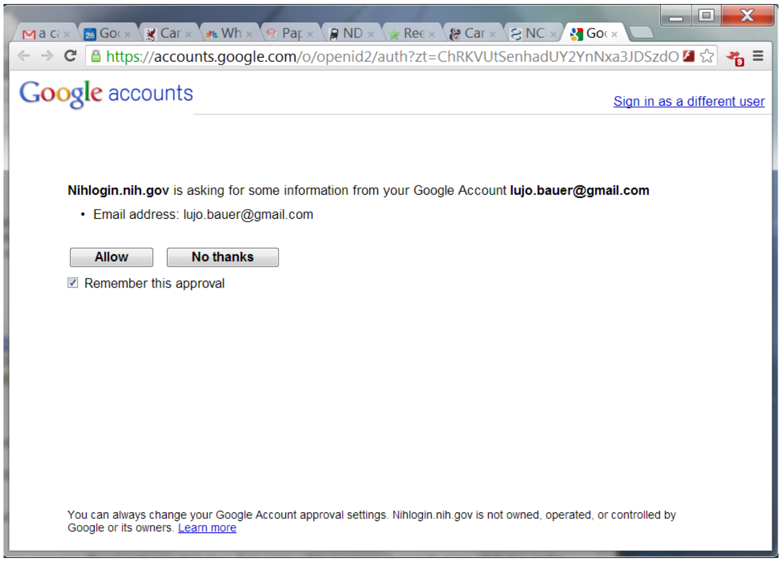
My NCBI retains user information and database preferences to provide customized services for many NCBI databases.

My NCBI Overview

My NCBI features include:

- Save searches & automatic e-mail alerts
- Display format preferences
- Filter options
- My Bibliography & NIH public access policy compliance
- Highlighting search terms
- Recent activity searches & records for 6 months
- LinkOut, document delivery service & outside tool selections

Figure 7: NIH website (`www.ncbi.nlm.nih.gov`) showing a “Sign in with Google” link. Accessed 10/18/2012.


https://accounts.google.com/o/openid2/auth?zt=ChRKVUtSenhadUY2YnNxa3JDSzdO
Google accounts
Sign in as a different user

**Nihlogin.nih.gov** is asking for some information from your Google Account **lujo.bauer@gmail.com**

- Email address: lujo.bauer@gmail.com

Allow    No thanks

☑ Remember this approval

You can always change your Google Account approval settings. Nihlogin.nih.gov is not owned, operated, or controlled by Google or its owners. Learn more

Figure 8: Google consent dialog. Accessed 10/18/2012.

**Interaction:** A typical interaction with Google acting as an identity provider is shown in Figures 7 and 8. When a user tries to sign in to `www.ncbi.nlm.nih.gov` (Figure 7), the “Sign in with Google” option is shown (Figure 7, red oval). Assuming that the user has previously logged into Google (and her browser has a cookie identifying her), then when the user clicks on “Sign in with Google” she is taken to the Google accounts website, presenting her with a confirmation dialog (Figure 8).

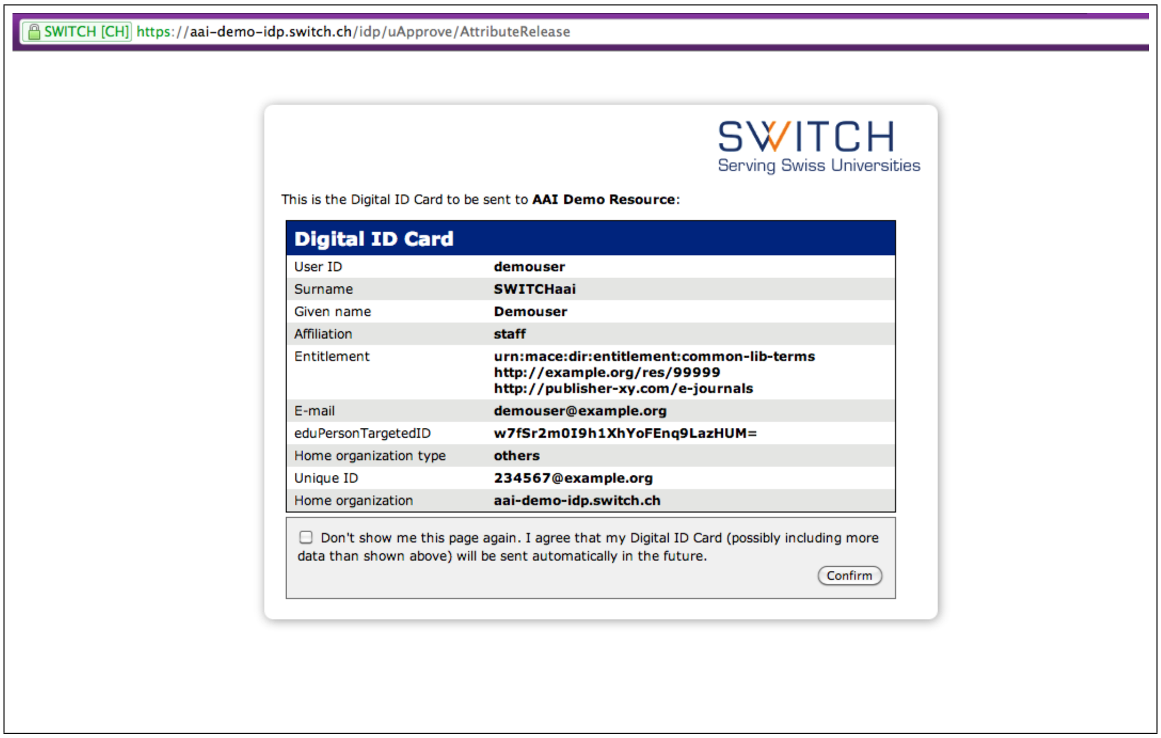
**Risk assessment:** Although it does not look like a dialog, the interaction presented in Figure 8 corresponds to a consent dialog, a type of warning. The user has to decide whether to grant this (possibly) unknown application access to her email address. The main risk is a privacy violation, that is, letting other persons/organizations know about the user’s private information in a way that makes the person feel uncomfortable or harmed. Another way in which this can be understood is as a mismatch between the application’s usage of the user’s information and user’s expectations of such usage. Since these expectations come from the perceived purpose of the application, making this purpose explicit is important.

## Comments

| *Guideline* | *Observations about the guideline* | *Possible Improvements* |
|---|---|---|
| Describe the risk comprehensively | [-] There is no explicit description of the risk.<br>[-] There is no description of the consequences of the risk.<br>[?] There is no actionable advice to avoid the risk. | Present the risk explicitly.<br>Describe the consequences in case the risk realizes.<br>The actions might be obvious to the user. |
| Be concise and accurate | [+] Message is short.<br>[-] The website (`Nihlogin.nih.gov`) is not described with a human-readable name.<br>[-] It is not clear what “some information” refers to.<br>[-] The name of the account (`lujo.bauer@gmail.com`) is the same as the label of the information to be released, making it ambiguous what information will be released. | Replace the URL with the name of the website (“National Center for Biotechnology Information”).<br>Replace “some information” with either “the following information” or “your email address from your Google account”. |
| Offer meaningful options | [?] The decision presented is a dilemma. Not enough information is presented for the user to make an informed decision.<br>[-] There is no default option.<br>[-] “No thanks” option is ambiguous: Does it mean that one can enter the website without revealing one’s email or that one cannot enter at all?<br>[-] “Remember this approval option” is ambiguous. If the checkbox is ticked, are both of the choices (“Allow” and “No thanks”) permanent or only one of them? | Replace “No thanks” by “Block website” or “Deny access to this website”.<br>Make a safe option (either “Report website” or “Deny access to this website”) the default.<br>Be clear about what “Remember this approval” means. |

| | | |
|---|---|---|
| Present relevant contextual information | [+] The hazard involves deciding whether to let an unknown agent obtain access to a known object, the user's email address.<br>[-] The user is asked to trust a possibly unknown agent, and this agent is not sufficiently identified.<br>[-] No reasons are given to explain why this information needs to be accessed. | Give more (human readable) information about the external website.<br>Provide the reason the website needs this information. |
| Present relevant auditing information | Possibly not applicable | |
| Follow a consistent layout | [-] No explicit question is posed. What is the user being asked to do? | Pose an explicit question to the user (e.g., "Do you trust this website with your private information?") |

## 4.3 UApprove (by Swiss Universities SWITCH)



SWITCH [CH] https://aai-demo-idp.switch.ch/idp/uApprove/AttributeRelease
SWITCH
Serving Swiss Universities

This is the Digital ID Card to be sent to **AAI Demo Resource**:

| Digital ID Card | |
|---|---|
| User ID | **demouser** |
| Surname | **SWITCHaai** |
| Given name | **Demouser** |
| Affiliation | **staff** |
| Entitlement | **urn:mace:dir:entitlement:common-lib-terms**<br>**http://example.org/res/99999**<br>**http://publisher-xy.com/e-journals** |
| E-mail | **demouser@example.org** |
| eduPersonTargetedID | **w7fSr2m0I9h1XhYoFEnq9LazHUM=** |
| Home organization type | **others** |
| Unique ID | **234567@example.org** |
| Home organization | **aai-demo-idp.switch.ch** |

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Figure 9: UApprove confirmation dialog (https://aai-demo.switch.ch/secure-uApprove/). Accessed 10/24/2012.

**Interaction:** A demo of the module UApprove (www.switch.ch/aai/support/tools/uApprove.html) is presented above. uApprove is an extension for the Shibboleth Identity Provider (IdP) to enable acceptance of terms of use and user attribute release consent. When a user tries to log in to a website using her Swiss university account, she is presented with a confirmation dialog (Figure 9) informing her which of her private information is being passed to the external website.

**Risk assessment:** Although the interaction is similar to the one described in Figure 8, the dialog in Figure 9 does not have an explicit way to prevent the release of the shown information. The user has to decide whether she grants this (possibly) unknown application access to her private information. Similarly to the previous case, the main risk is a privacy violation and may be understood as a mismatch between application's use of the user's information and the user's expectations of such usage. Since these expectations come from the perceived purpose of the application, making this purpose explicit is important.

## Comments

| *Guideline* | *Observations about the guideline* | *Possible Improvements* |
|---|---|---|
| Describe the risk comprehensively | [-] There is no explicit description of the risk.<br>[-] There is no description of the consequences of the risk.<br>[-] There is no actionable advice to avoid the risk. | Present the risk explicitly.<br>Describe the consequences in case the risk is realized.<br>Give actionable advice to avoid the risk. |
| Be concise and accurate | [-] Message is not concise; user is overwhelmed with detail.<br>[-] There is not enough information about the external website.<br>[-] The message is not described from the point of view of the user.<br>[-] Technical jargon is used in the dialog (e.g., "Entitlement", "eduPersonTargetedID", "Unique ID"). | Provide more information about the external website.<br>Replace technical terms with phrases that might be better understood by the user or omit them entirely. |
| Offer meaningful options | [-] The user has no decision to make; she can only confirm.<br>[-] There is no safe option.<br>[-] The checkbox option allows the user to agree that future communications may include more data than shown in this message. | Have a safe option and make it the default.<br>Do not offer an option that allows releasing undefined data in future communications. |
| Present relevant contextual information | [+] The hazard involves deciding whether to let an unknown agent obtain access to a user's known information.<br>[-] The user is asked to trust a possibly unknown agent, and this agent is not sufficiently identified.<br>[-] There are no reasons reported that explain why this information needs to be accessed. | Give more (human readable) information about the external website.<br>Provide the reason the website needs this information. |
| Present relevant auditing information | Possibly not applicable | |
| Follow a consistent layout | [-] No explicit question is posed to the user. What is the user being asked to do?<br>[-] Information is not always meaningful to the user. | Pose an explicit question to the user (e.g., "Do you trust this website with your private information?"). |

# References

[1] Apple human interface guidelines. http://developer.apple.com/Mac/library/documentation/UserExperience/Conceptual/AppleHIGuidelines. [accessed 21-Jan-2013].

[2] Gnome human interface guidelines 2.2.1. http://library.gnome.org/devel/hig-book/stable/index.html.en. [accessed 21-Jan-2013].

[3] Windows user experience interaction guidelines. http://msdn.microsoft.com/en-us/library/aa511258%28v=MSDN.10%29.aspx. [accessed 21-Jan-2013].

[4] J. R. Anderson. *Cognitive Psychology and its implications*. Worth publishers, 41 Madison Avenue, New York, 2005.

[5] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, 9(2), Mar. 2011.

[6] S. Breznitz. *Cry wolf: The psychology of false alarms*. Lawrence Erlbaum Associates, Hillsdale, New Jersey, 1984.

[7] L. F. Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, pages 1:1–1:15. USENIX Association, 2008.

[8] S. Egelman. *Trust me: Design patterns for constructing trustworthy trust indicators*. PhD thesis, School of Computer Science, Carnegie Mellon University, 2009.

[9] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1065–1074. ACM, 2008.

[10] C. Nodder. Users and trust: a microsoft case study. In L. F. Cranor and S. L. Garfinkel, editors, *Security and Usability: designing secure systems that people can use*. O'Reilly Media, 2005.

[11] M. Wogalter. Purposes and scope of warnings. In M. Wogalter, editor, *Handbook of warnings, Human Factors and Ergonomics*. Lawrence Erlbaum Associates, 2006.