Security warnings

Cristian Bravo-Lillo

Carnegie Mellon

CMU **U**sable **P**rivacy and **S**ecurity Laboratory
http://cups.cs.cmu.edu/

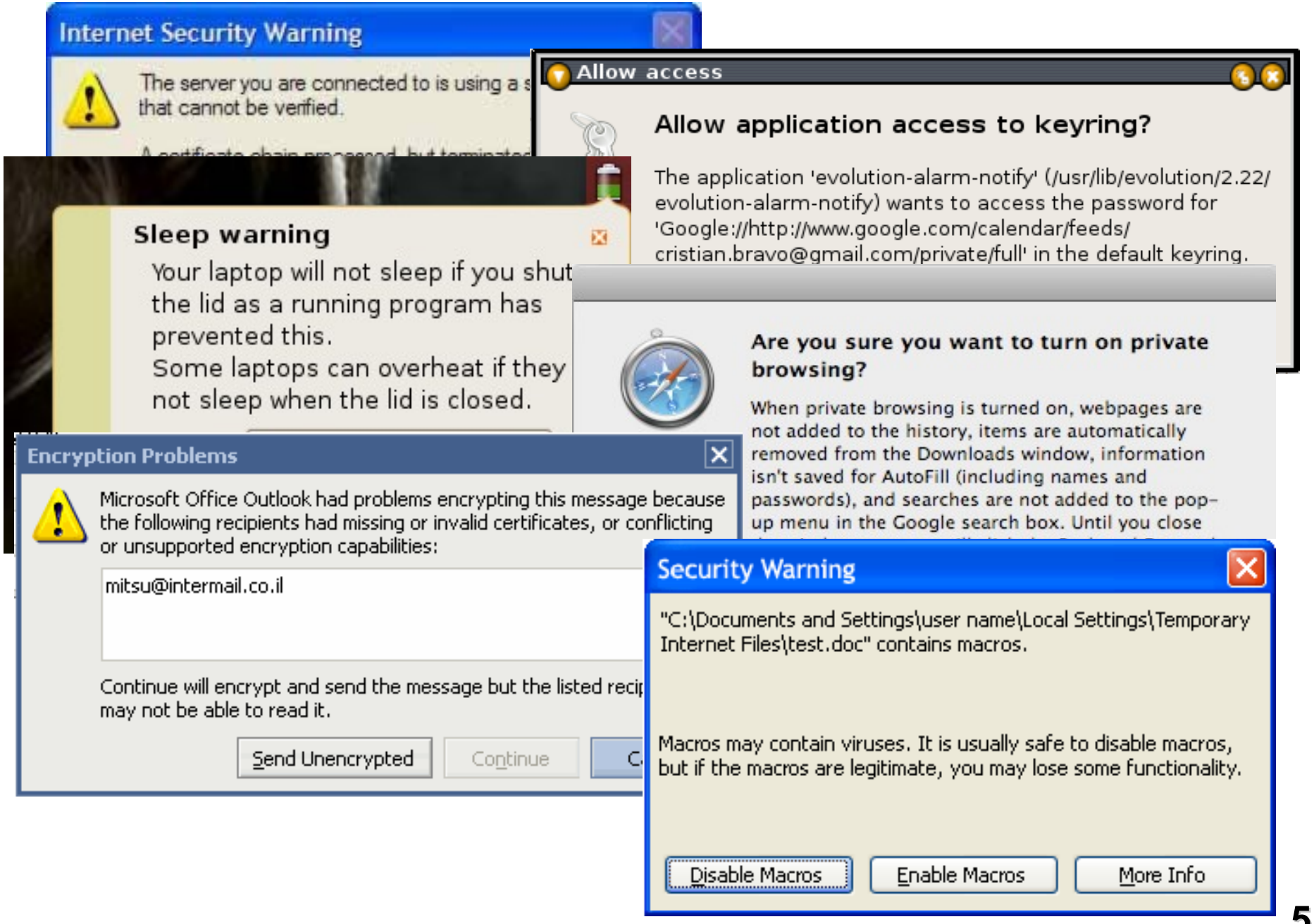
Sources:
http://www.homebizseo.com
http://purpleslinky.com/humor/travel/nine-funny-warnings-signs-to-make-you-laugh/

Warning signs go up to stop Poles stealing river fish for Christmas dinner

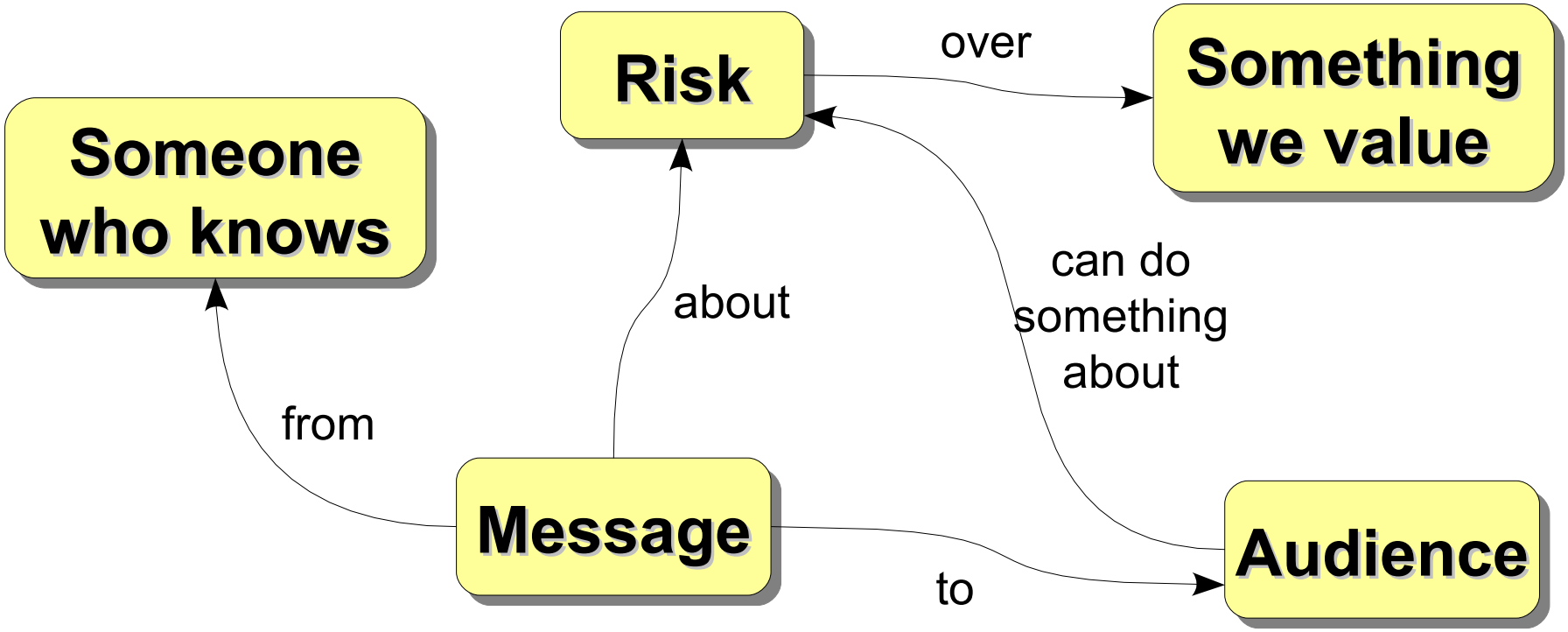
To any peckish Poles or ravenous Romanians, the message could not be clearer: Keep off our fish.
Three roadsign-style warnings were launched yesterday to stop Eastern European immigrants from spearing, taking home and cooking coarse fish from our rivers, lakes and canals.
The initiative is timely because carp and pike are a traditional Christmas dish in Poland and officials fear an increase in fish rustling over the next few weeks. (...)
The trust's director, Michael Heylin, said: **"These are easy to understand so there will be no excuses. "The pictures clearly mean, "Don't steal, cook or kill fish".**
"The Environment Agency has signs in 19 languages, but unless you know the nationality of the thief they won't work." (...)

Source: http://www.dailymail.co.uk/news/article-495199/Warning-signs-stop-Poles-stealing-river-fish-Christmas-dinner.html

Sources:
http://purpleslinky.com/humor/travel/nine-funny-warnings-signs-to-make-you-laugh/
http://www.piste-off.com/photos-signs.asp
http://www.govisithawaii.com/2009/02/03/signs-of-hawaii-beach-safety-warnings/


Internet Security Warning
The server you are connected to is using a s
that cannot be verified.
Allow access
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.
Sleep warning
Your laptop will not sleep if you shut
the lid as a running program has
prevented this.
Some laptops can overheat if they
not sleep when the lid is closed.
Are you sure you want to turn on private browsing?
When private browsing is turned on, webpages are not added to the history, items are automatically removed from the Downloads window, information isn't saved for AutoFill (including names and passwords), and searches are not added to the pop-up menu in the Google search box. Until you close
Encryption Problems
Microsoft Office Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:
mitsu@intermail.co.il
Continue will encrypt and send the message but the listed recip
may not be able to read it.
Send Unencrypted
Continue
Security Warning
"C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\test.doc" contains macros.
Macros may contain viruses. It is usually safe to disable macros, but if the macros are legitimate, you may lose some functionality.
Disable Macros
Enable Macros
More Info

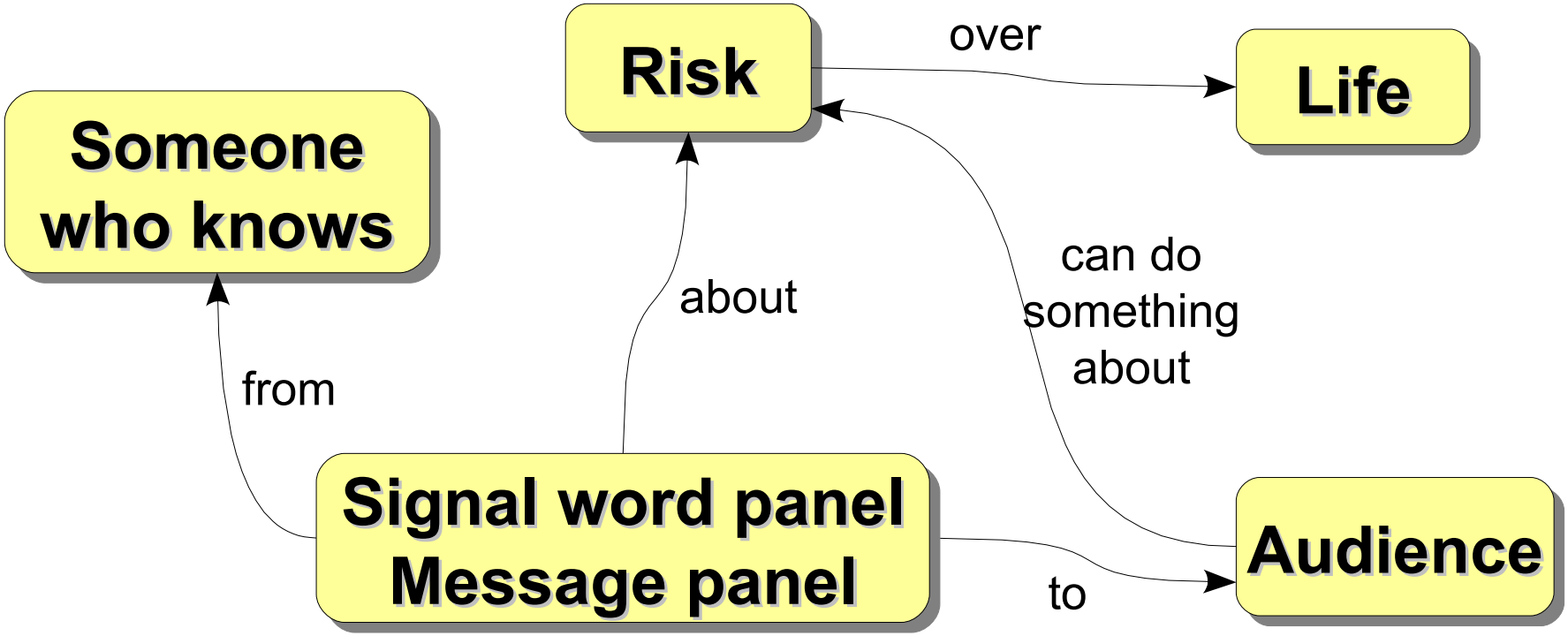
Elements common to all warnings



What is a warning anyway?

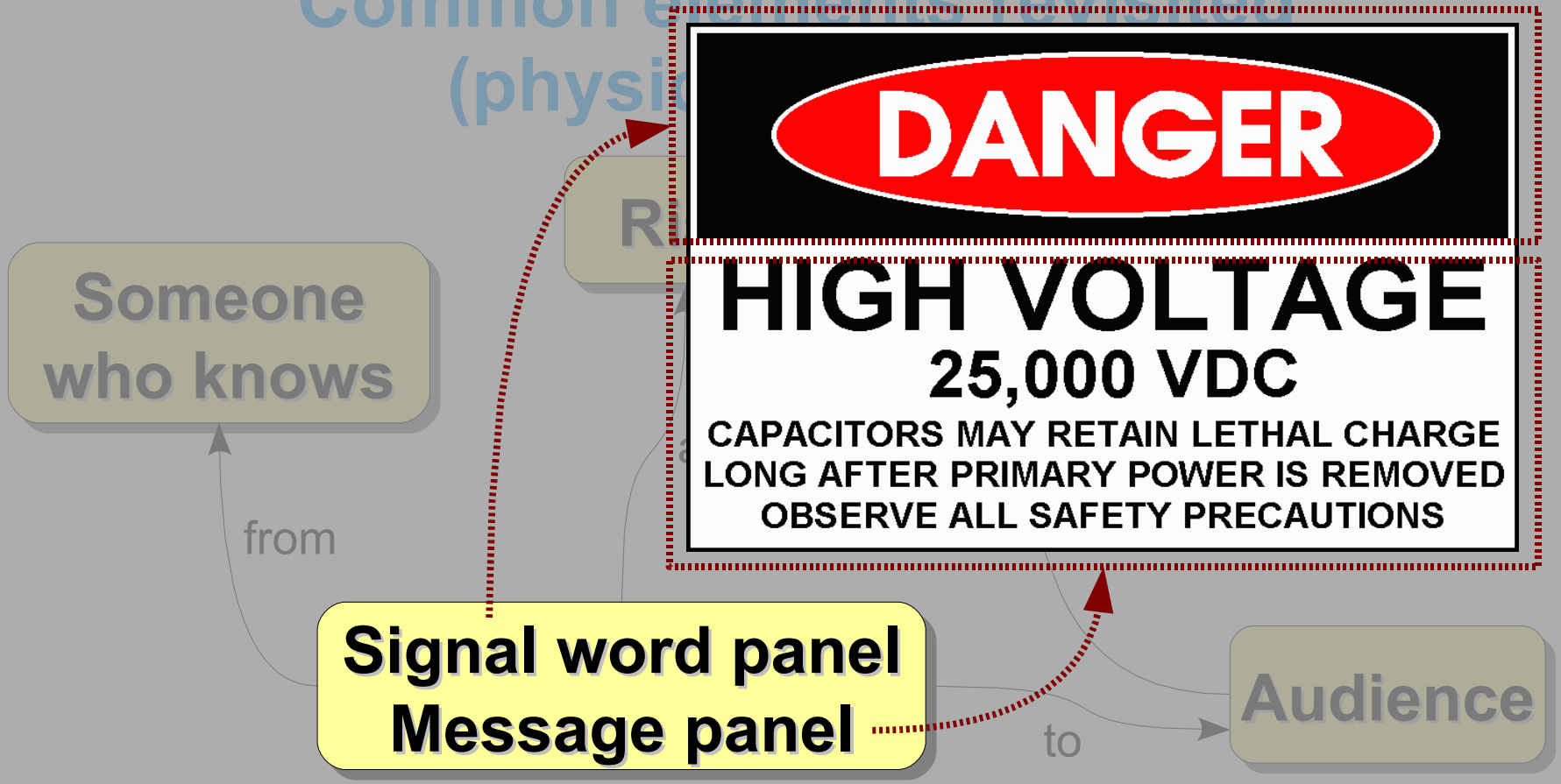
- Warnings are communications to avoid people hurt themselves or hurt others (Wogalter 2006)
- Purposes:
  1. To avoid people being hurt by an external factor.
  2. To modify people's behavior, to promote compliance with safety regulations.
  3. "To reduce or prevent health problems, workplace accidents, personal injury, and property damage".
  4. Intended as reminders of a hazard to already-aware people.
  5. Warnings may also serve as a legal instrument to transfer liability from the maker of a product to the consumer.

Common elements revisited (physical warnings)



- Typical fields for warnings:
  - Foods, chemicals, road signs, kids toys, heavy machinery, lab facilities, etc.

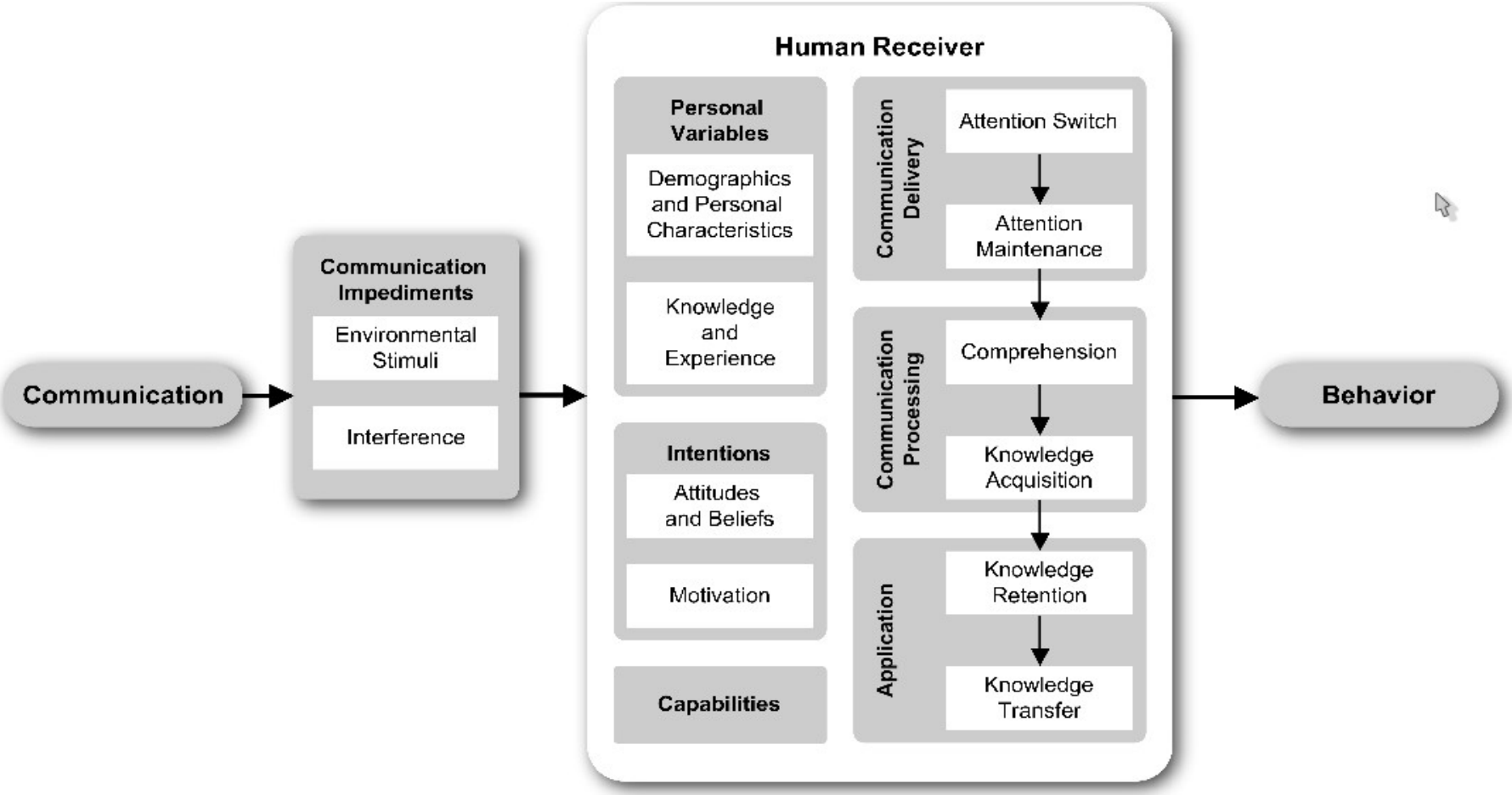
Common elements revisited (physi



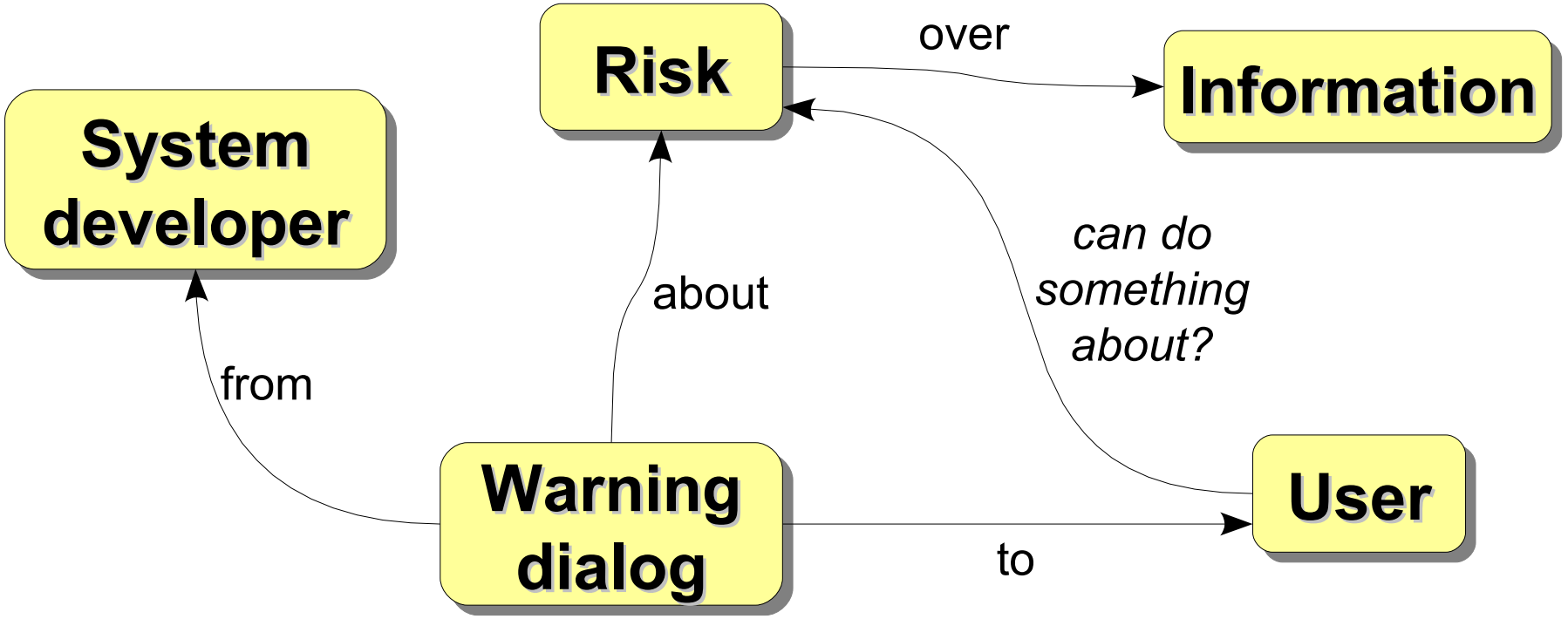
- Typical fields for warnings:
  - Foods, chemicals, road signs, kids toys, heavy machinery, lab facilities, etc.

What about computer warnings?

- "Communications that alert users to take immediate action to avoid a hazard" (Cranor 2008)



Common elements revisited (computer warnings)



- Typical fields for warnings:
  - Operating system, browsers, email clients, productivity software, entertainment software, etc.

People do not heed (computer) warnings

- Some results on computer warnings:
  - People provide their passwords even in absence of security indicators or in presence of warnings (Schechter et al 2007)
  - People do not heed passive SSL indicators unless primed to (Whalen et al 2005)
  - Users trust more in sites' “look-and-feel” than security on websites (Wu et al 2006)
  - Users do not pay attention to security toolbars (Wu et al 2006)

Example 1: phishing warnings (1/2)

- Phishing is specially dangerous
- Egelman et al performed a study about phishing warnings effectiveness:
  - 4 different conditions
    - Active Firefox 2.0 warning
    - Active MSIE 7.0 warning
    - Passive MSIE 7.0 warning
    - No warning
  - Spear phishing messages were sent to 60 participants with spoofed versions of Amazon and eBay.

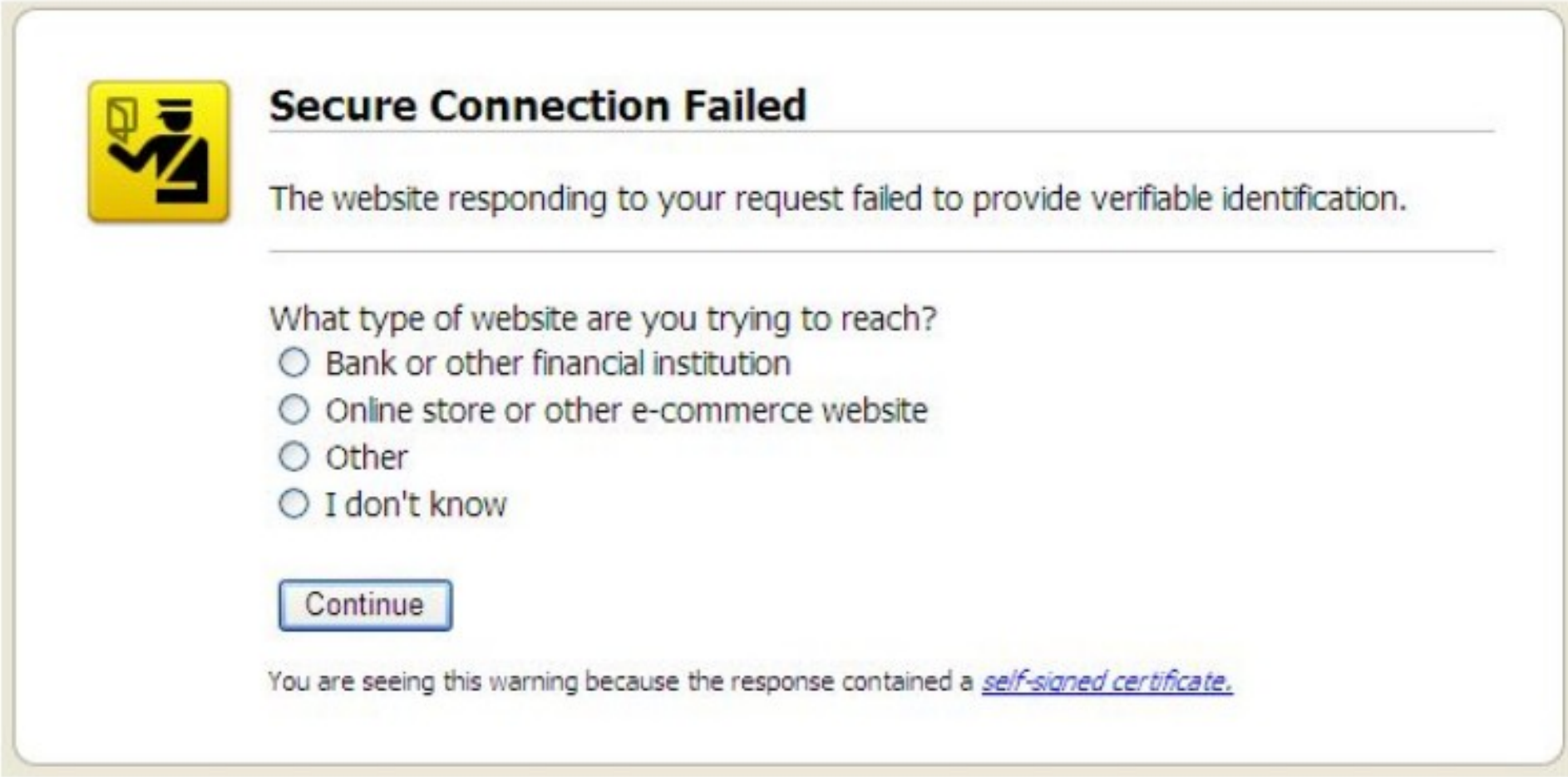
Example 1: phishing warnings (2/2)

- Results?
  - 97% fell for at least one phishing message
  - 79% of users who received an active warning heeded it
  - 13% of users who received a passive warning heeded it
  - Firefox active indicators were better understood and heeded more often than active MSIE warnings
  - Active warnings are better than passive ones
- It's worst:
  - Correlation found between recognizing the warning and heeding it
  - 32% of those who heeded the warnings believed that emails were legitimate (*what?*)

Example 2: SSL warnings (1/3)

- Sunshine et al performed a study about SSL warnings:
  - An online survey:
    - 409 users, screenshots of SSL in FF2, FF3 and IE7
    - Expired certificates, with unknown issuer and with mismatched domain names
    - Between ~30% (IE7, domain mismatch) and ~60% (FF2, expired certificate) reported they would proceed to the site
    - Belief on protection due to op. System (Linux, Mac)
  - A lab between-subjects study:
    - 100 users were shown two new “cooked” warnings

Example 2: SSL warnings (2/3)



Example 2: SSL warnings (2/3)

Example 2: SSL warnings (3/3)

- Results?
  - Single page performed better than FF2 and IE7
  - Multi-page performed better than FF2 and IE7
  - FF3 performed better than FF2 and IE7, and almost equal to single and multi-page warnings.
  - People more likely to read multi-page than FF2, FF3 and IE7.
- Promising, but:
  - 30% of participants who saw the redesigned warnings thought they had seen them **before** (*what?*).

Tools for computer warning analysis

- Warnings can be analyzed from a psychological view:
  - Hazard control hierarchy (Wogalter 2006)
    - Design out → Guard against → Warn about
  - False-alarms decrease trust in detection systems (Breznitz 1984)
- Human-in-the-loop framework (Cranor 2008)
  - Modified C-HIP to better suit computer warnings
- An iterative trust-game

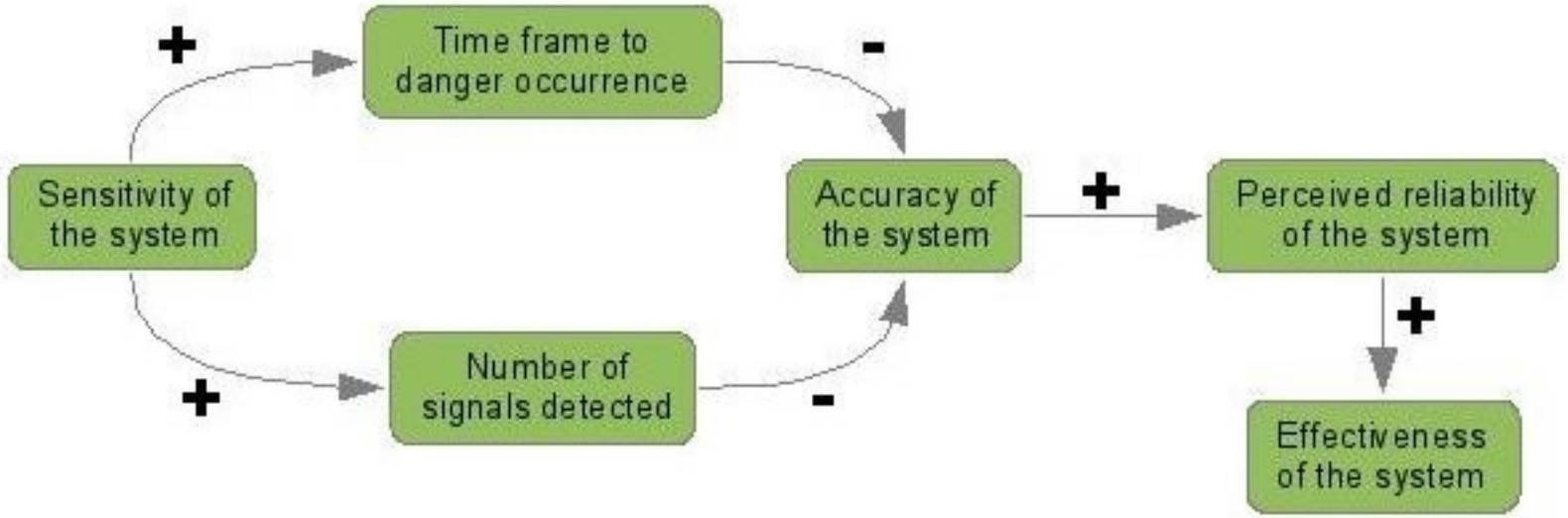
Hazard control hierarchy

1. Design out:
   - Can the risk be eliminated from the system?
2. Guard against:
   - Can the risk be guarded so the user does not fall for it?
3. Warn: clearly indicate:
   - What is the risk
   - What are the consequences of not complying
   - How to avoid the risk

The False-Alarm Effect (1/2)

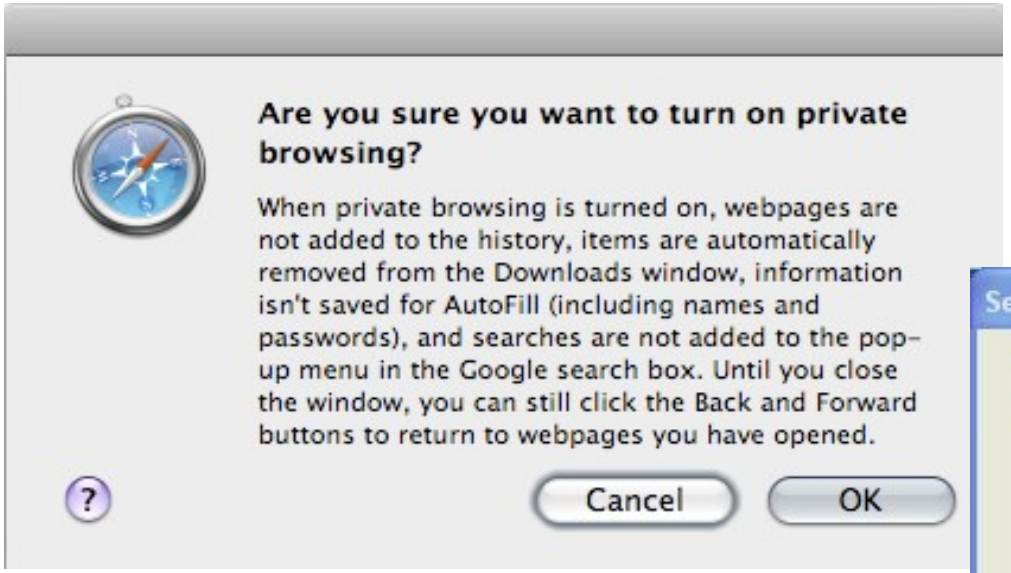
- Described by Breznitz:
  - 1900: a tornado gets near Florida
    - Nobody knows → nobody is scared.
    - When you see it → too late → alarms are "certain"
  - 2000: a tornado gets neat Florida
    - Weather forecast networks announces tornado may hit Florida 11 days in advance
    - At last moment, the tornado heads to Atlantic → False-alarm
- What is different?
  - 1900: No ability to forecast → No "false alarms"
  - 2000: Ability to forecast → false alarms → decrease in trust on detection system

The False-Alarm Effect (2/2)



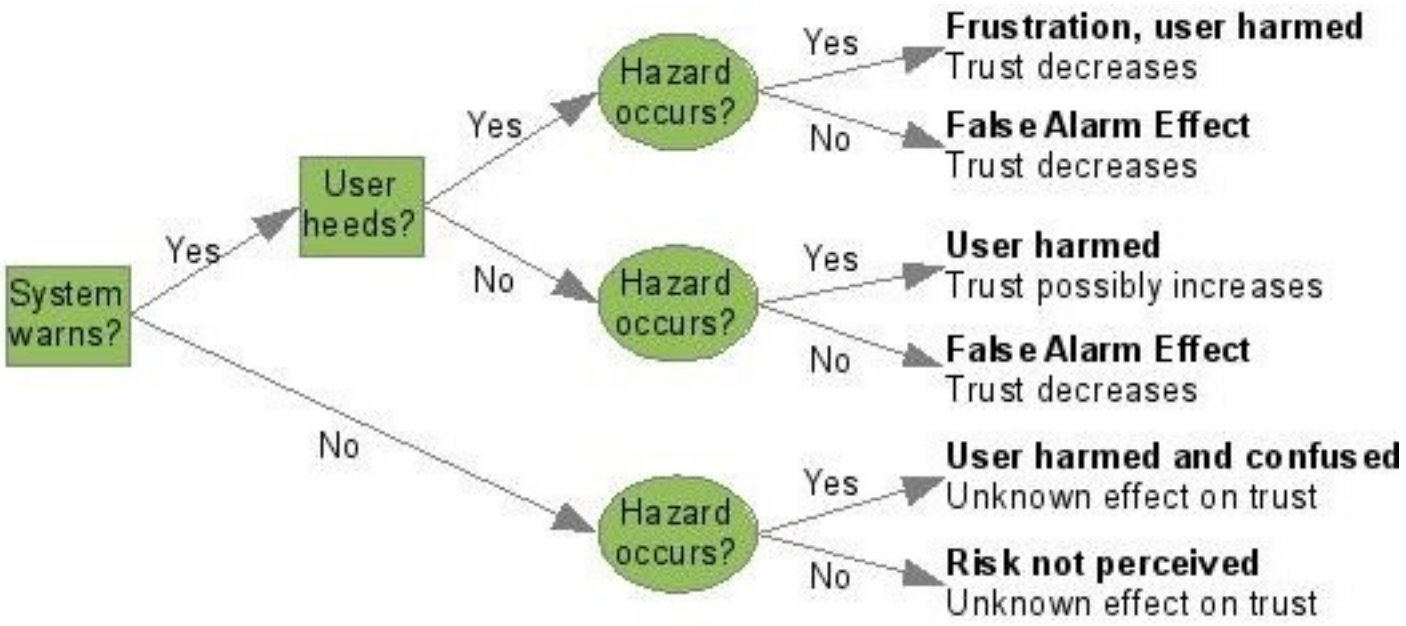
The False-Alarm Effect (applied to computer warnings)

- "Detection system" ≈ "System"
- If risk is not immediate, warning the user will decrease her trust on the system



The iterative trust game

- If there is a hazard,
  - System may choose to warn or not
  - In case the user is warned, she may choose to heed or not
- In almost any case, there is an undesired outcome



Recommendations for phishing warnings (from Egelman Et al., 1/2)

1. Interrupt the primary task of the user
   - active warnings are better than passive ones.
2. Provide clear choices
   - Most people fail to obey a warning when they do not understand what the options are.
3. Fail safely
   - Warning content should be read before the user could dismiss the warning; no familiar option should be used to allow the user to dismiss the warning without reading its content.

Recommendations for phishing warnings (from Egelman Et al., 2/2)

4 Prevent habituation

- "Phishing warnings" must be designed with a different appearance than "regular warnings" to avoid visual recognition and early dismissal.

5 Alter the phishing website

- Users trust websites mainly because of their look and feel; hence, warnings should distort websites detected as phishing cases.

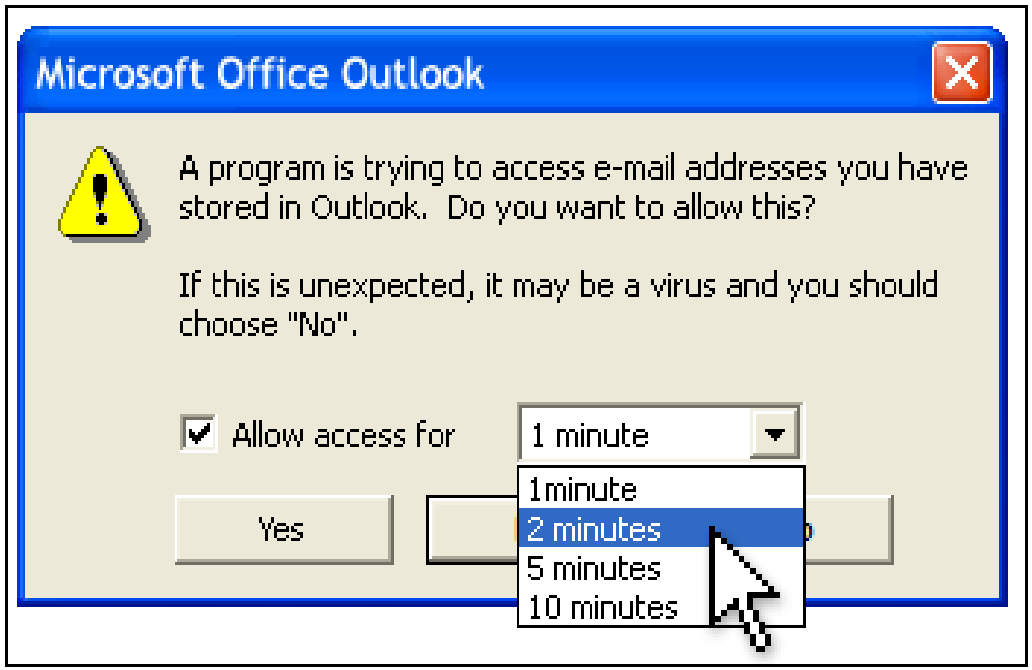
Some more recommendations

- User's trust on the system is “precious”:
  - If the “impact” of confusing/annoying the user is higher than the “impact” of the problem that the system is trying to warn about → don't warn!

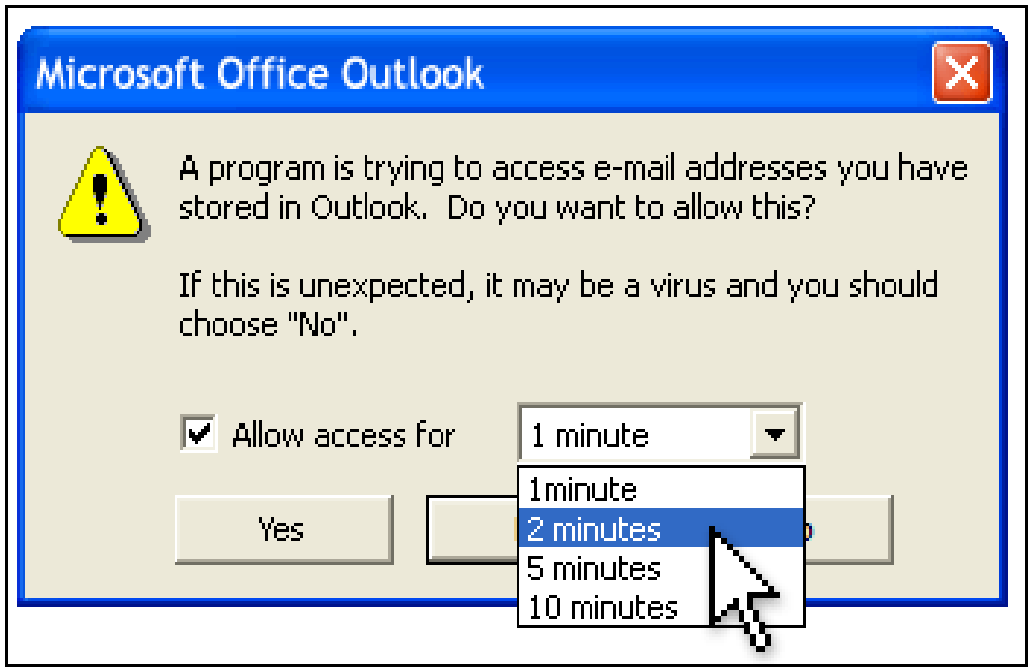
- The user is not prepared to understand certain situations:
  - If the “impact” of a problem is too high → don't allow → don't warn!

Computer warnings checklist

1. About the warning:
    1. What is the risk that can be identified from the warning wording?
    2. What is the actual risk?
    3. Are those related?
    4. Are there instructions on how to avoid the risk?
    5. Are these instructions clear?
    6. Is there an option to comply?
    7. Is the default option the safest one?
2. Consequences:
    1. Are the consequences of not complying indicated?
    2. Are these the same than actual consequences
3. Antecedents:
    1. Can the risk be eliminated?
    2. (If not) Can the risk be guarded?
    3. Can the contextual information change the assessment of the warning? If so, how?

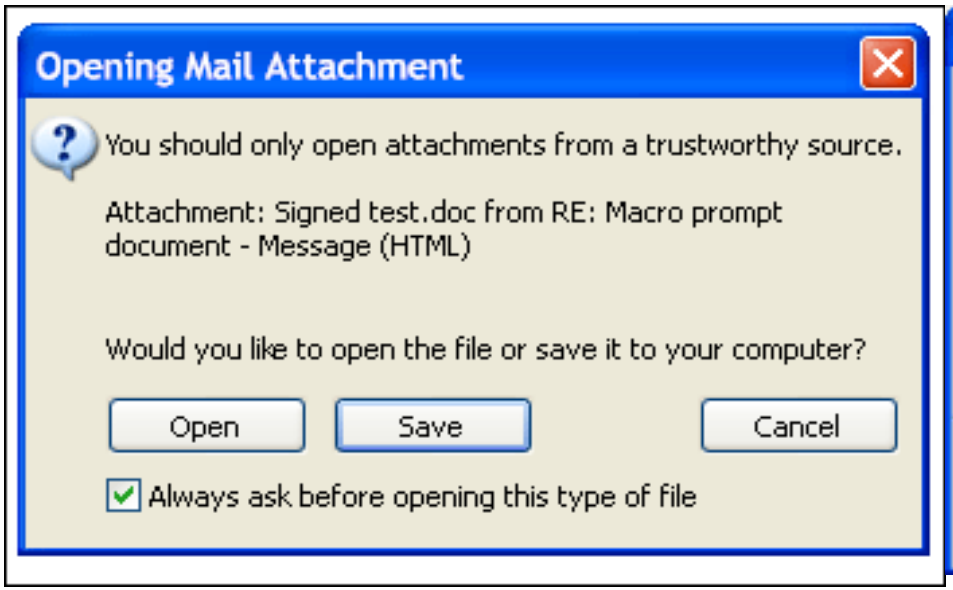


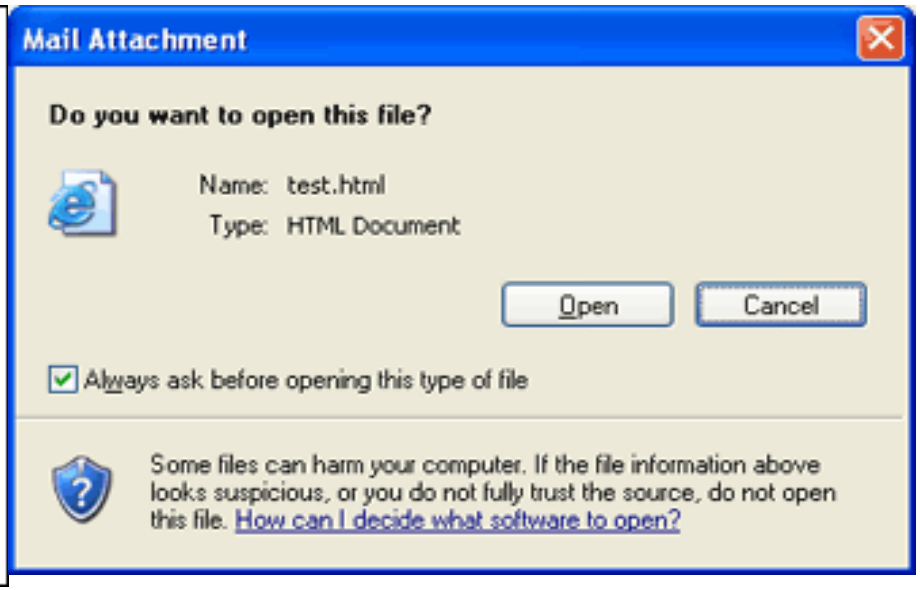
- **Can the hazard be designed out/guarded?** Partially. One possible solution is to provide Outlook with a list of "known or trusted programs" and devices to the user (managed by the OS). If a program is explicitly trusted, access is granted and no warning is shown. If a program is explicitly not trusted, no access is granted and again no warning is shown. If in doubt, check if there is a currently updated working antivirus software. If so, access is granted on the basis of trust on the antivirus software doing its job. If there is no antivirus working, or if it is not updated, then the user should be asked. Two things would be necessary:
  - That the OS maintained a list of "known" programs, along with a way to check their code integrity (a CRC hash, or an MD5 signature would suffice), where the addition of a program to this list occurs every time the user installs a new software (since the user is installing it, the computer should trust it).
  - That the OS had a way to know about the existence of an installed and working antivirus (MSWin from XP does this).



How can the warning be improved?

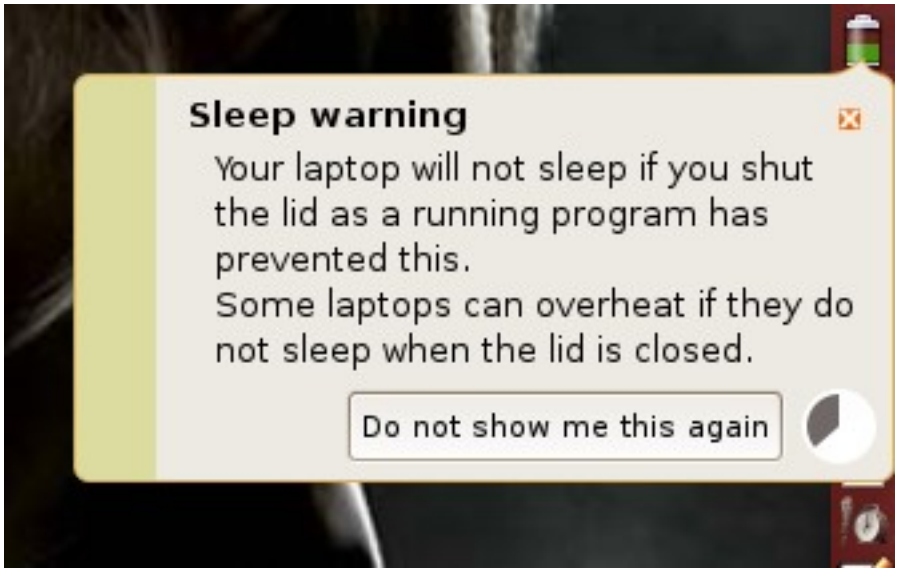
- By identifying the program that is accessing the Outlook API.
- By identifying what information is the program asking.
- By informing the user about the status of the antivirus.
- By offering not a time frame, but an program-identification-dependent access to the API.



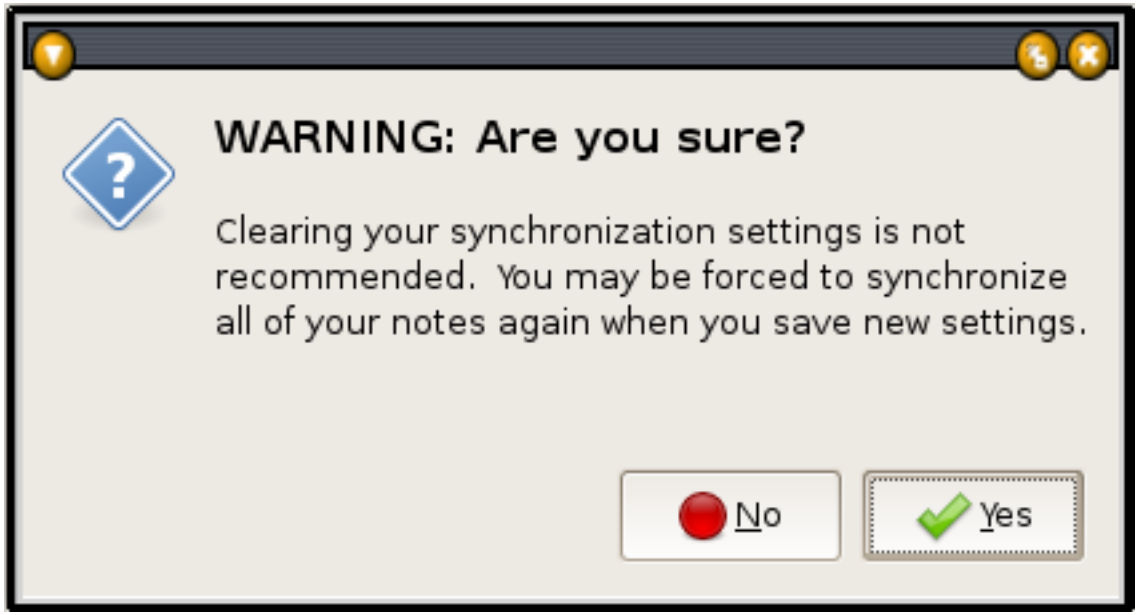


- **Can the hazard be designed out/guarded?** Partially. Since the risk comes from the execution of potentially malicious code contained in the file that might change OS files or resources, the file could be always open on behalf of a dummy user, with no privileges to write or change any OS file or resource. Additionally:
  - If an updated antivirus is currently running, and
  - If the specific file could be checked against viruses, worms, trojans and other virus-like threats, and
  - If other preventing measures taken by the OS are fulfilled (like the ones described in the comments),
- Then the file might be opened without asking. Otherwise, a warning should be displayed informing the user it is risky to open the file, and that the file should be saved and quarantined, waiting for an antivirus to check it (if possible). If there is no antivirus working, an indicator should be displayed informing that the file won't be open since it is too risky.


Allow access
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.
Deny
Allow Once
Always Allow


Sleep warning
Your laptop will not sleep if you shut the lid as a running program has prevented this.
Some laptops can overheat if they do not sleep when the lid is closed.
Do not show me this again


SSL Certificate Verification
Accept certificate for talk.google.com?
The root certificate this one claims to be issued by is unknown to Pidgin.
View Certificate...
Reject
Accept


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.
No
Yes


This accessory is not made to work with iPhone
Would you like to turn on Airplane Mode to reduce audio interference? You will not be able to make or receive calls.
Yes
No


AT&T
12:53 PM
Easy Wi-Fi
Dizzy Bee
Crash Kart
iBART
Delete "iNetworkTest"
Deleting "iNetworkTest" will also delete all of its data.
Delete
Cancel
NetShare
NightCamera
Cat Piano
Dictionary
Phone
Mail
Safari
iPod