Potential of Visual Narrative as Risk Communication to Affect Behavioral Change.

Tonya Stroman

Abstract

Risky user behavior is a threat to system security. Current approaches to understanding and addressing this threat do not offer a definitive solution that can guarantee a congruous relationship between emerging technologies and evolving user attitudes and experiences. As the correlation between a users' system activity and the users' offline security increases, new ways of improving user understanding of the relationship between user actions and system security need to be considered and evaluated. In this paper I present this human-computer interaction problem as a communication problem and more specifically, a problem of poor risk communication. I also suggest that risk communication, through interactive visual narrative, may alleviate the problem. First, I review current approaches to risk communication. Then, I discuss possible causes and consequences of miscommunication of risk. I continue the discussion with an examination of effective risk communication. Next, I consider the potential effectiveness of visual narrative as an effective risk communication tool. Supporting this concept, I describe a conceptual user test of a risk-communicating visual narrative where I found that providing risk related information in this format significantly changed user behavior from risk-ignoring to risk-avoiding. This suggests that, as a better risk communication method, interactive visual narratives can change user behavior and, consequently, help maintain system security.

Introduction

Every good relationship relies on effective communication. The relationship between a computer and it's owner is no different. System visibility [1], which strengthens system security, is a result of good storytelling. A computer has information that must be shared with a user, In order to maintain the security of the system and protect the user's personal information. This information can be considered a story, which describes system behavior, strengths and weaknesses. If the story is difficult to understand or identify with, the effects of user actions on the system will not make sense to the user.

For example if a user does not realize that by default the system grants certain privileges to everyone, friend or foe, visiting the machine, the user may have an unrealistic expectation of safety while using the machine. So, while the user may feel safe sharing identifying or financial information with the system, the system, with default settings, is not a trustworthy confidant. Ignorance of this generous "door policy" leaves

the owner vulnerable. Even worse, based on personal frustrations and barriers in accessing certain system resources, the impression the owner may have, until something goes wrong, is that the system's admission policy is more in line with that of a V.I.P room. This conceptual model of system behavior influences decisions made by the user while on the system. A more usable approach to educating people about security issues will help users become informed about the risks associated with system behavior and user actions.

Current approach to risk communication

Existing recommendations about computing risk communication offer a variety of approaches to educating end-users and changing end-user behavior. Some are more user-centered than others. One approach suggests creating a “security culture” at work through administrative policies enforced by a straightforward reward and punishment system.[2]. This is approach is not because it doesn’t really address why security information, on it’s own, is ineffective. This approach basically relies on peer pressure and fear of embarrassment by the non-compliant.

Another approach rests on the notion that maintaining secure behavior requires effort on the part of the user with no immediate reward, so information about risk must be persuasive by: creating a risk that is immediate, like punishment for risky behavior. [3]. Again, this is a usability challenged approach. Fear of punishment is not necessarily going to be effective. However, a more interesting suggestion from this persuasive approach involves social marketing techniques, such as self-image related advertising.

An extremely human-centered approach requires designers and developers to completely abstract security related information and allow the user to focus solely on desired task. The user interface should make any user action implicitly secure. [4] Although, on the surface, this appears to be the most user-centered approach, it actually robs users of any amount of autonomy. If properly implemented, granularity and flexibility of system control and information will be friendlier to a larger number of users.

An opposite approach asserts that making user-action-system-consequence information visible to users will empower users to make better decisions about behaviors that affect system security. [5] This may be effective for more knowledgeable users, but too much information can be confusing and discouraging to less experienced computer users.

The most promising solutions lie in a mental model approach to risk communication. Because the mental model of developers is very different from that of the average “non-expert” user, risk communication provided by developers fails. The mental models approach requires the communication to match the expectations of the user, which creates a more usable and secure user experience. [6]

Despite the insights into communicating risk provided by these approaches, a huge gap remains between risk communication and behavioral change. This is the result of information miscommunication .[7] This miscommunication can result in a lack of understanding about risk or not being convinced to care enough about the risk to change. Ultimately, in order to better communicate security risks to end-users, it is necessary to understand why, despite measures for increased risk communication, users just don't understand or just don't care.

The miscommunication:

For this paper, I define miscommunication as the inability to make information understood and also the inability for information, which is understood, to motivate behavioral change. Many human focused concerns contribute to this communication failure.

Sometimes the type or amount of information is cognitively taxing: Remembering security information is the problem [8]. If the user can't remember, they can't use the information or pass it on to others. Finding ways to make information stick is crucial.

In some cases conflicts between user goals and security measures are not identified or addressed. [9]

Also, many people don't feel as if they will be affected, even if the feel the risk is real for someone else [10]. They are informed but aren't convinced to change their behavior.

Another problem is that often users go through the motions without ever being aware of the consequences of their actions. Knowing the implications of every action is too difficult and since the system responds as they expect, despite risky behavior, they can't distinguish between secure and "unsecure" behavior. [7]

And finally, the user mental model and actual system behavior frequently do not match. This leads the user to draw analogies between the operating system and non-information sensitive systems, which exposes the user to security risks. [11]

When risk communication works

Outside of the IT domain, different forms of risk communication effectively influence human understanding of reality and elicit behavioral change. I divide these forms into two types, informal communication and formal communication. Informal is social in nature and is not necessarily an explicit effort to train someone about a concept. Formal communications is more organizational, with a directed or planned dissemination of information. Within both types of communication, it seems that people like to listen to stories. One form of informal communication is word of mouth (WOM). WOM is especially powerful in peer to peer risk communication. This is evident in the

persistence of cautionary and moral tales and, most importantly, their ability to change and guide behavior.[12] Another informal form is the cyber urban legend. This is a narrative, which spreads online and is used to effectively warn about dangers, both real and imaginary; these stories also inform people about expected online behavior.[13, 14] A type of formal communication, public health information distributed by agencies, has shown that delivery of the content is just as important as the content itself. People are more receptive to behavioral advice perceived as a conversation rather than a command.[15] Even in the most formal communication environment, such as corporations with formal organizational security training, narratives effectively instill widespread understanding of acceptable social behavior and social risks associated with unacceptable behavior. [16] And finally, formal attempt to use employee mental models to make workplace safety information relevant through context, has proved successful.[17]

Potential of visual narrative as an effective risk communication tool.

Again, the mental models approach is interesting in that it creates a useful reference for the user each time system interaction takes place. However, trying to anticipate and accommodate the mental models of all users, given human variability and operating system evolution, becomes untenable. At the same time, meeting user goals and expectations is essential to system security. A compromise is to try to communicate system behavior and consequences of interaction with the system in a manner which is familiar and natural to people, in narrative form. Additionally, It's not just about making a risk known and understood, it is also about making the risk important enough to the user that it provokes behavioral change.

One solution is to create a system that tells a better story to the user. So, what type of story is best and what is the best way to tell it? In terms of system security, it is not sufficient to describe system behavior. The consequences of user actions must be clearly defined and easily understood. Accordingly, the story needs to resemble a cautionary tale and it needs to have an impact on the way the user behaves. In other words, the system must become a better risk communicator.

In order to be considered successful, the communication of a risk must affect some behavioral change that reduces risk. So, the problem is figuring out a way to communicate risk to people that will have a lasting impact on their behavior. This involves determining the type of communication method that makes information sticky and creates a sense of immediacy or relevance.

One answer is that: "The type of risk where realistic perception can be expected appear to be the risks with which people have some experience, direct or indirect" [18]

The greater the personal relevance, the more likely a person is to respond to a risk and narrative provides this relevance. Onscreen visual narratives would be particularly powerful because visual images are particularly effective in communicating risk:

If I consider visual narrative communication, rather than a purely text based instructional communication, I see that:

1. People create mental models from narratives:[19]
2. People perceive risk as real when relevant to them: Narrative is contextual and context provides relevance to the user.[20]
3. Narrative provides experiential risk perception, which is most natural to people [21].
4. Narrative improves learners ablity to apply new knowledge critically [22]
5. People prefer a combination of graphical and textual risk related information.[23].

Also, risk communication, through visual narrative, would expose people to risks in a realistic way without exposing them the dangers associated with the risks. Narrative delivery of information also accommodates the instructional needs of a broad user group and should therefore effectively change user behavior.

Most importantly, mental models are essentially inner-narratives, or stories, that a person constructs to understand how things work in the world. Narrative communication will be effective in influencing mental models, and consequently behavior, because like speaks to like. The human mind is already full of these mental models and predisposed to understanding new concepts through narrative [24].

Even if we assume that narratives can change mental models, documenting any associated behavioral change of a user is problematic without constant monitoring of that user's behavior. However, in order to know if visual narrative works as an effective risk communicator I have to observe a change in behavior after exposure to the narrative.

Conceptual Narrative Test:

To test the narrative-as-medium concept, I conducted an initial conceptual user test with a Flash-based risk communicating visual narrative. With this test I wanted to prove that providing risk related information in this format could significantly change user behavior.

Method:

I implemented the visual narrative as a stand alone Flash SWF file, with content from the Sims 2 machinima engine. I tested 6 students, 3 female and 3 male, between the ages of 18 and 23. I gave all participants a pre-test questionnaire. All scored at the novice level of knowledge of computer systems; level was determined by the perceived

level of knowledge indicated by the participant and the number of “yes” answers on the pretest questionnaire (see appendix).

1. For the first task, I allowed each participant sign in by choosing the “full access” or “restricted access” sign-in option. Due to potential usability issues with the labels “administrator” and “guest’, I used labels that described the concept I wanted to explain through the narrative. (see appendix)
2. I then allowed the participant to read through the narrative as slowly as needed.
3. The last screen of the narrative instructed the participant to sign in again to complete some final questions.
4. In reality, I wanted to see if the narrative changed the participants choice of sign in option.

Results and Discussion:

All 6 participants initially signed in with “full access”. After exposure to the narrative, all 6 participants signed in the second time using “restricted access”. This strongly suggests that interaction with the narrative immediately influenced the participants behavior.

Mental Model Test

In this section I describe a follow up test I will conduct, which will attempt to capture user mental model before and after exposure to the visual narrative, in addition to detecting behavioral change. Although my initial test showed a behavioral change, in order to know if method changes mental model, I must extract and document mental model before and after narrative exposure. There must be an observable difference in the mental model. [25]

Method:

For this test, I will have a much larger participant pool. I will test 50 participants with the same Flash narrative from the conceptual test.

1. First, I will determine technical knowledge level of each participant, before the test, by using the pretest questionnaire from the conceptual test.
2. In order to capture the participant pre-test mental model I will ask each participant, the following interview style questions [26]
    a. What happens inside your computer when you sign in?
    b. What happens inside your computer when you open a file?
    c. If someone else wanted to use your computer do you mind? Why?
3. I will hand the participant a pen and ask the participant to draw an “idea” map, representing the interview question #1, on a blank sheet of paper [27]

4. I will allow the participant to sign in by choosing the “full access” or “restricted access” sign-in option
5. I will allow the participant to read through the narrative as slowly as needed.
6. The last screen of the narrative will instruct the participant to sign in again to complete some final questions.
7. In reality, I want to see if the narrative changes the participants choice of sign in access option.
8. In order to capture the participant post-test mental model I will ask each participant, the following interview style questions [26]
    a. What happens inside your computer when you sign in?
    b. What happens inside your computer when you open a file?
    c. If someone else wanted to use your computer do you mind? Why?
9. I will then hand the participant a pen ask the participant to draw an “idea” map, representing the interview question #1, on a blank sheet of paper [27]

Mental Model Test Predictions

I predict that I will again observe a considerable change in user behavior post-narrative. I also predict that the answers to the pre-narrative mental model questions will differ from the post-narrative answers. The post-narrative conceptual maps should also look significantly different, structurally or substantively, from the pre-test maps. This will indicate a change in mental model of the user, as well as any behavioral change.

Conclusion & Discussion

In conclusion, poor communication of computer risk contributes to user conceptual understanding of technology and, ultimately, system insecurity. If users do not understand the way a system works, they will never be able to understand how their behavior affects the stability of the system. Many of the approaches, which are meant to improve risk communication, poorly address the human component of the communication failure. Of course, making the information easy to grasp is very important. However, it is just as important to make the information compelling. If the information does not inspire behavioral change, system security does not improve. So, the solution to this problem requires much more than just accurate information about risk, it also requires an understanding of the complexity of human nature. Even though there was observable behavioral change in the participants of my test, I have provided only half of the story. Showing a connection between narrative exposure, mental model change and behavioral change is the next step. Once this relationship is established, I will be able to provide strong evidence that narrative communication of risk is a highly effective, user-centered method of risk communication.

Future Work

If my next test proves to change user mental models and behavior related to administrative access, I will then create narratives with content that reflects different system concepts, such as installing updates or file sharing. I also intend to conduct a separate labeling test to find out which terms make sense to people in an everyday way. I believe that some confusion about system behavior may also stem from poor labeling of user interface components.

References

Adams Users are not the enemy Communications of the ACM [0001-0782] yr:1999 vol:42 iss:12 pg:40

F Asgharpour, D Liu, LJ Camp - weis2007.econinfosec.org

DeWitt, A. J. and Kuljis, J. 2006. Is usable security an oxymoron?. interactions 13, 3 (May. 2006), 41-44. DOI= http://doi.acm.org/10.1145/1125864.1125889

Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, D.K. Smetters, "In Search of Usable Security: Five Lessons from the Field," IEEE Security and Privacy, vol. 02, no. 5, pp. 19-24, September-October, 2004

(bardzell, blevis, lim),

Dourish, P. and Redmiles, D. 2002. An approach to usable security based on event monitoring and visualization. In Proceedings of the 2002 Workshop on New Security Paradigms (Virginia Beach, Virginia, September 23 - 26, 2002). NSPW '02. ACM, New York, NY, 75-81. DOI= http://doi.acm.org/10.1145/844102.844116

Risk creation in traveling Backpacker Adventure Narration Annals of Tourism Research [0160-7383] Elsrud yr:2001 vol:28 iss:3 pg:597

Flechais, I., Sasse, M. A., and Hailes, S. M. 2003. Bringing security home: a process for developing secure and usable systems. In Proceedings of the 2003 Workshop on New Security Paradigms (Ascona, Switzerland, August 18 - 21, 2003). C. F. Hempelmann and V. Raskin, Eds. NSPW '03. ACM, New York, NY, 49-57. DOI= http://doi.acm.org/10.1145/986655.986664

Threats to Information Systems: Today's Reality, Yesterday's Understanding MIS quarterly [0276-7783] Loch yr:1992 vol:16 iss:2 pg:173

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal 19, 3 (Jul. 2001), 122-131. DOI= http://dx.doi.org/10.1023/A:1011902718709

Smith, S. W. 2003. Humans in the Loop: Human-Computer Interaction and Security. IEEE Security and Privacy 1, 3 (May. 2003), 75-79. DOI= http://dx.doi.org/10.1109/MSECP.2003.1203228

Weirich, D. and Sasse, M. A. 2001. Pretty good persuasion: a first step towards effective password security in the real world. In Proceedings of the 2001 Workshop on New Security Paradigms (Cloudcroft, New Mexico, September 10 - 13, 2001). NSPW '01. ACM, New York, NY, 137-143. DOI= http://doi.acm.org/10.1145/508171.508195

[13] Modern Folklore: Cybermythology in Western Culture. Darrell A. Joyce. 307-283 sauceykat.com

[14] Fernback, J. (2003) 'Legends on the Net: An Examination of Computer-Mediated Communication as a Locus of Oral Culture' , New Media & Society 5(1): 29–46

[15] Evaluating risk communication: examining target audience perceptions about four presentation formats for fish consumption health advisory information. Risk Analysis [0272-4332] Connelly yr:1998 vol:18 iss:5 pg:649 -59

[16] Poulton Michael S, Organizational Storytelling, Ethics and Morality: How Stories Frame Limits of Behavior in Organizations Electronic Journal of Business Ethics and Organization Studies
Vol. 10, No. 2 (2005) pg:4-9

[17] The use of mental models in chemical risk protection: developing a generic workplace methodology. Risk Analysis [0272-4332] Cox yr:2003 vol:23 iss:2 pg:311 -24

[18] Factors in Risk Perception Sjoberg Risk Analysis, vol 20. No. 1, 2000 page 2

[19] Gordon H. Bower; Daniel G. Morrow Mental Models in Narrative Comprehension *Science*, New Series, Vol. 247, No. 4938. (Jan. 5, 1990), pp. 44-48.

[20] BRUNER, J. (1991). `The narrative construction of reality'. Critical Inquiry, 18, Autumn, 121.

[21] Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004).Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and rationality. *Risk Analysis*, *24*, 311–322

[22] Active learning through multimedia IEEE multimedia [1070-986X] Schank yr:1994 vol:1 iss:1 pg:69

[23] Evaluating Risk Communication: Examining Target Audience Perceptions abut Four Presentation Formats for Fish Consumption Health Advisory Information Connelly & Knuth Risk Analysis, Vol 18, No. 5, 1998 p649-659

[24] Doyle, J. K., and Ford, D. N. (1998). Mental models concepts for system dynamics research. *System Dynamics Review* **14**, 3-29.

[25] Doyle, J., Radzicki, M.,& Trees, W. S. (1998). Measuring change in mental models of dynamic systems: An exploratory study. Proceedings of the 1998 International System Dynamics Conference(pp. 30-31). Montreal, Québec, Canada.

[26] Carley, K. & Palmquist, M. (1992). Extracting, representing, and analyzing mental models. *Social Forces, 70* (3), 601--636.

[27] Williams, Carol G. Using Concept Maps to Assess Conceptual Knowledge of Function *Journal for Research in Mathematics Education*, Vol. 29, No. 4. (Jul., 1998), pp. 414-421.

Appendix

Pretest Questionnaire

1. How would you characterize your knowledge level of computer systems?
   (mark most accurate answer)

   0 - I'm totally clueless

   1 - I don't know how things work exactly, but I have a general idea about how my system works.

   2 - I understand how my system works but feel uncomfortable about making changes to my system.

   3 - I understand how my system works and I regularly make changes to system configurations

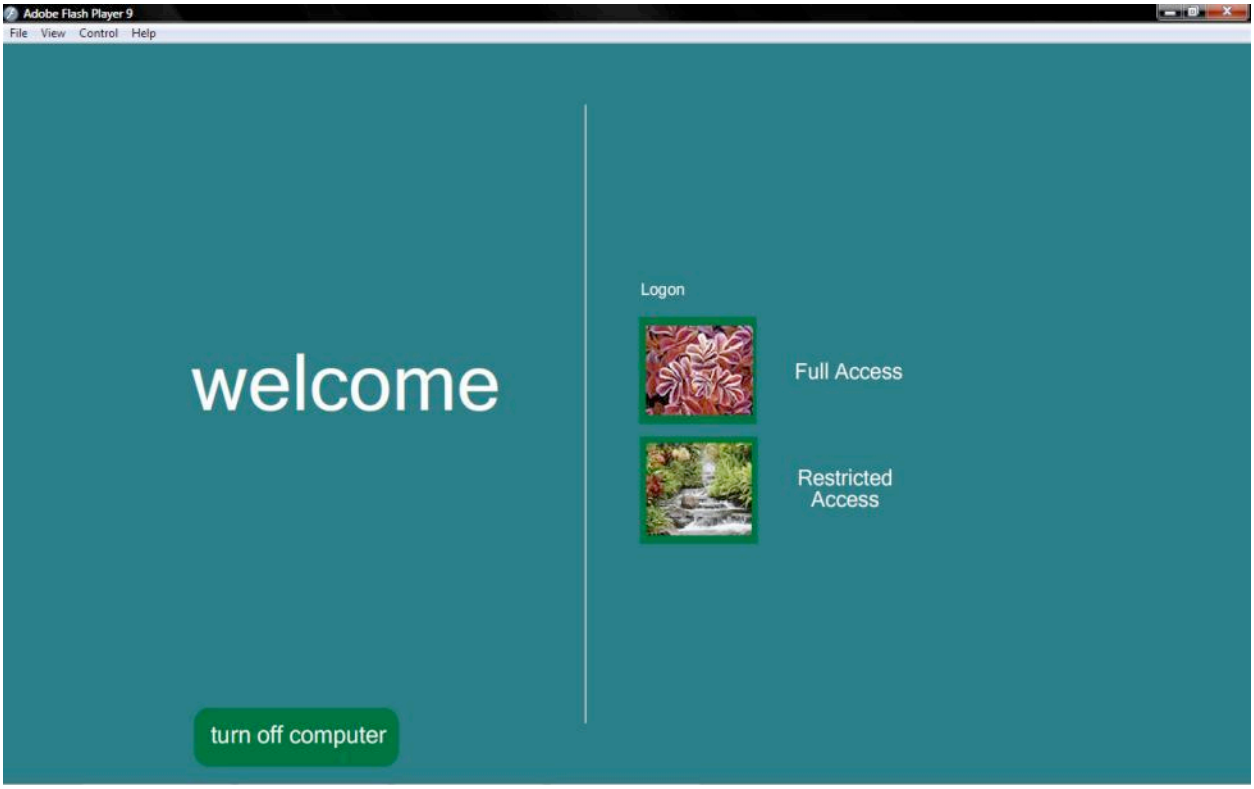
   4- I understand my system and can diagnose/fix most problems with my system.

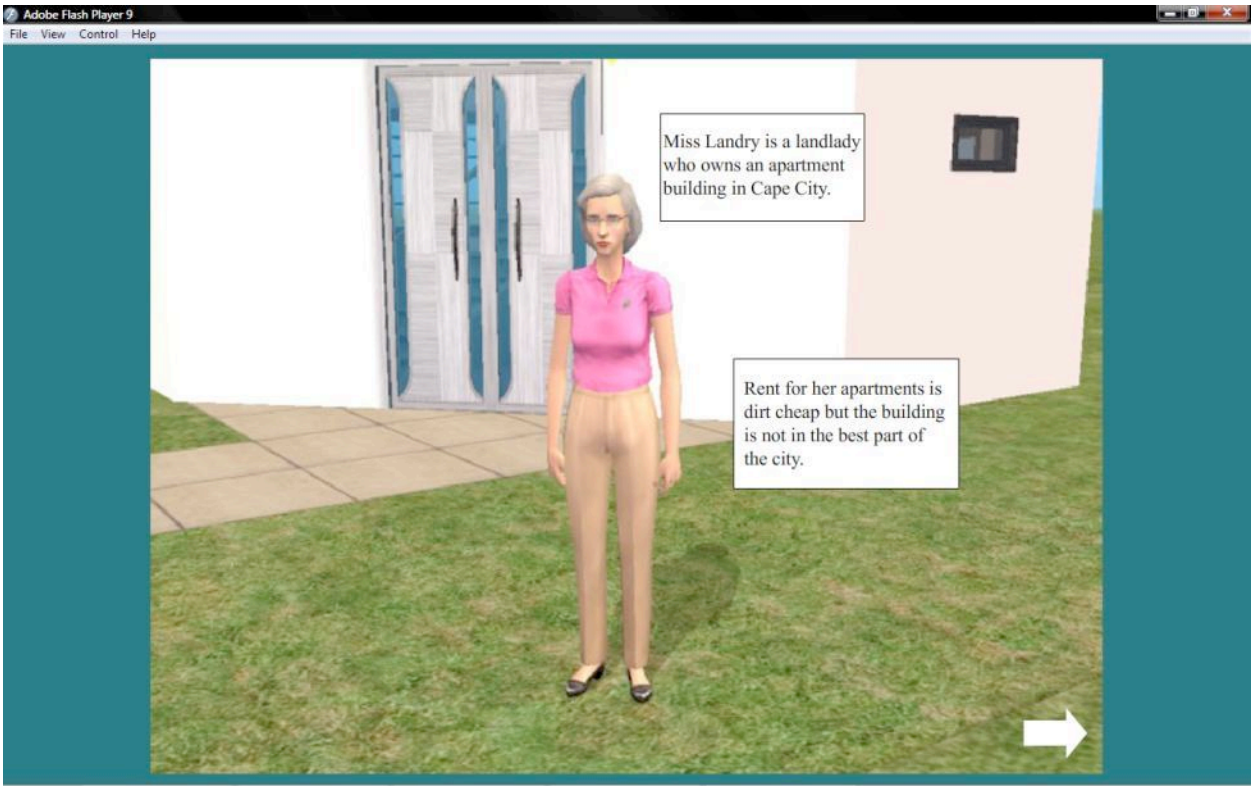
2. Do you know what a NIC is?

3. Do you know what a registry key is?

4. Do you know what a system bus is?

Screenshots of Flash narrative

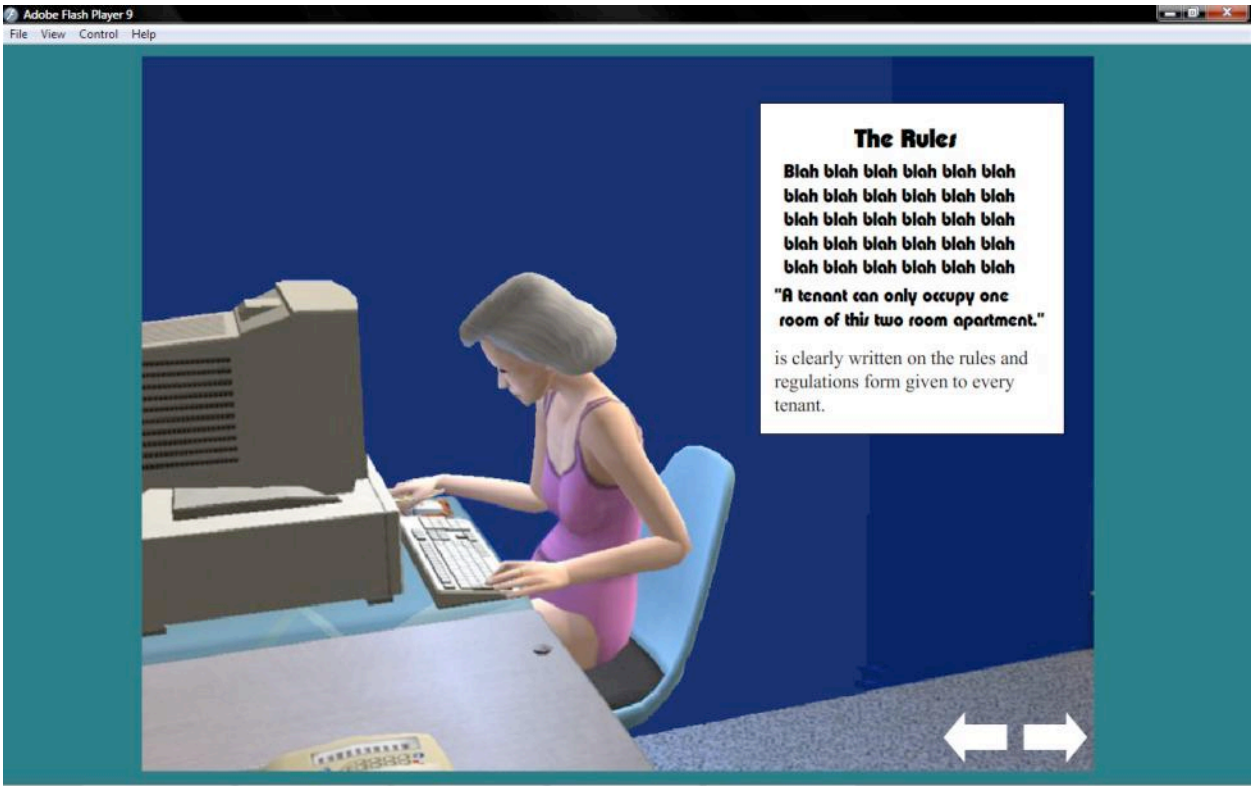





Adobe Flash Player 9
File View Control Help
Although Miss Landry is known for being kind and attentive, she is also known for being a little odd.

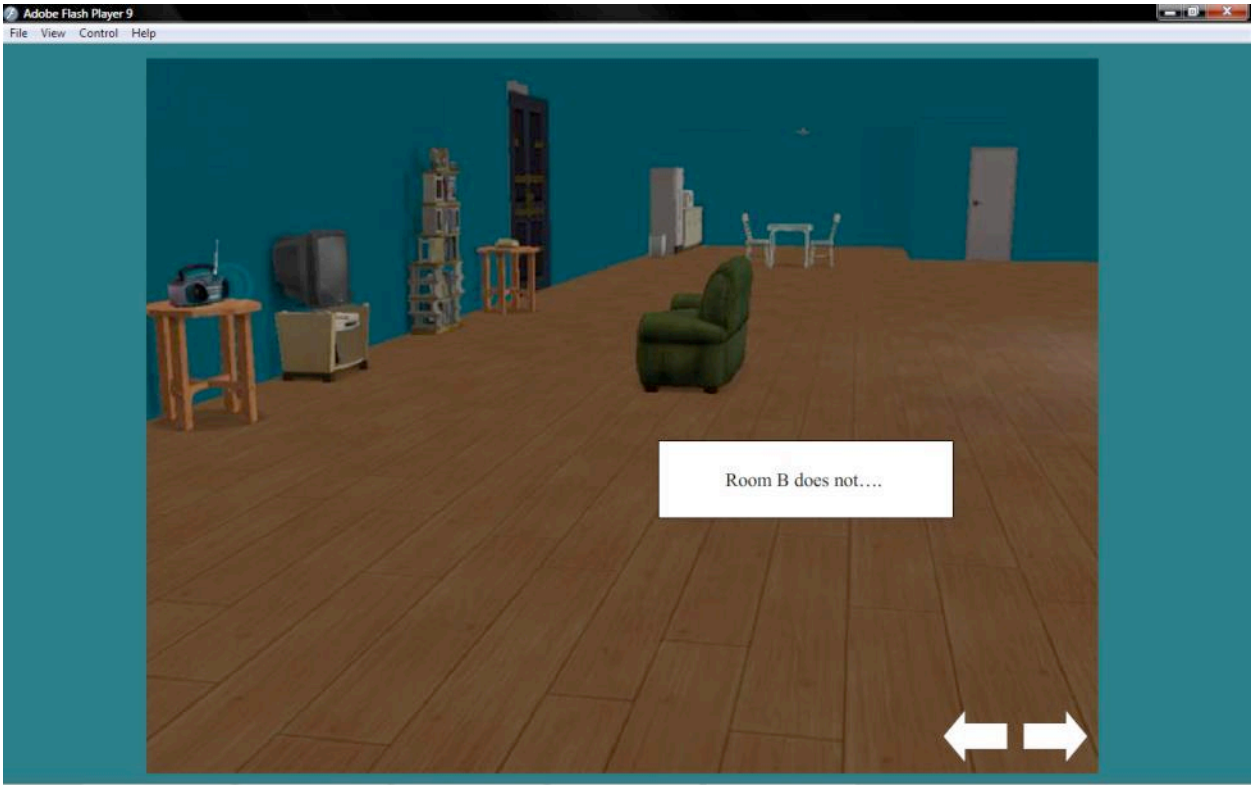

Adobe Flash Player 9
File View Control Help
For example, she has very strange and rigid rules for her tenants. Her apartments have two living areas, but the tenant must choose to live in only one of them.
So, if you rent an apartment from her, one room is occupied while the other room must remain vacant.


Adobe Flash Player 9
File View Control Help
The two rooms are attached by a very sturdy locked door.


Adobe Flash Player 9
File View Control Help
The Rules
Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah
"A tenant can only occupy one room of this two room apartment."
is clearly written on the rules and regulations form given to every tenant.


Adobe Flash Player 9
File View Control Help
Miss Landry has her rules; no one understands them, but the rules are the rules!
So, when you move in you must decide to live in room A or room B.


Adobe Flash Player 9
File View Control Help
Room A comes furnished with every possible comfort and type of entertainment you can imagine.

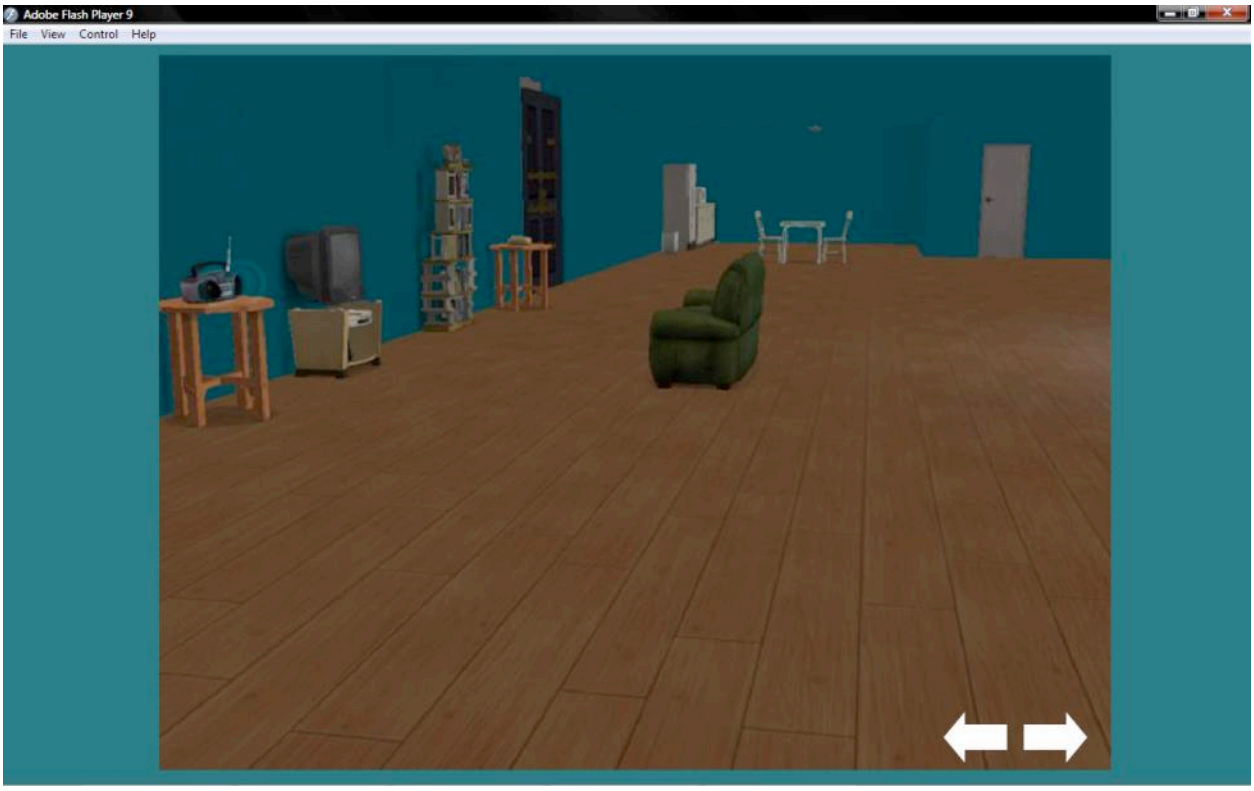

Adobe Flash Player 9
File View Control Help
Room B does not….


Adobe Flash Player 9
File View Control Help
If you choose room A, you can use anything in the room that you like as much as you want.


Adobe Flash Player 9
File View Control Help

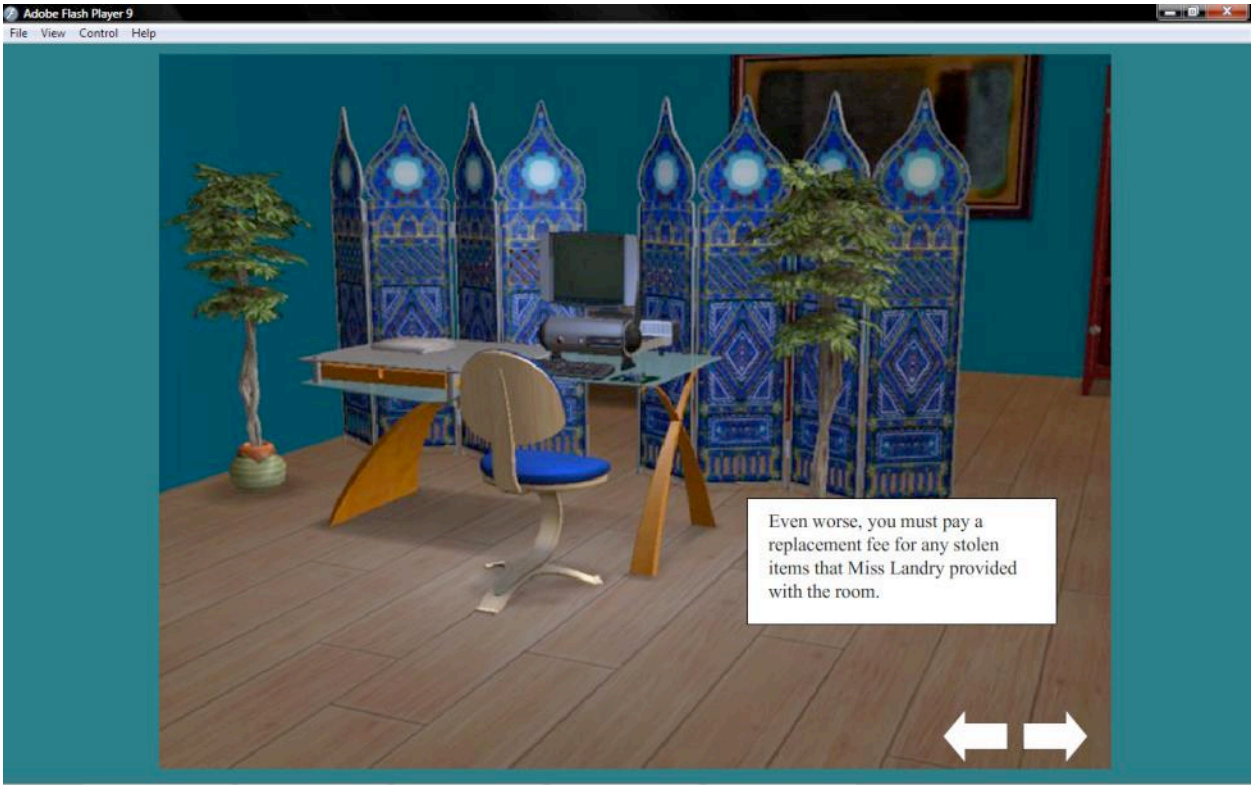

Adobe Flash Player 9
File View Control Help

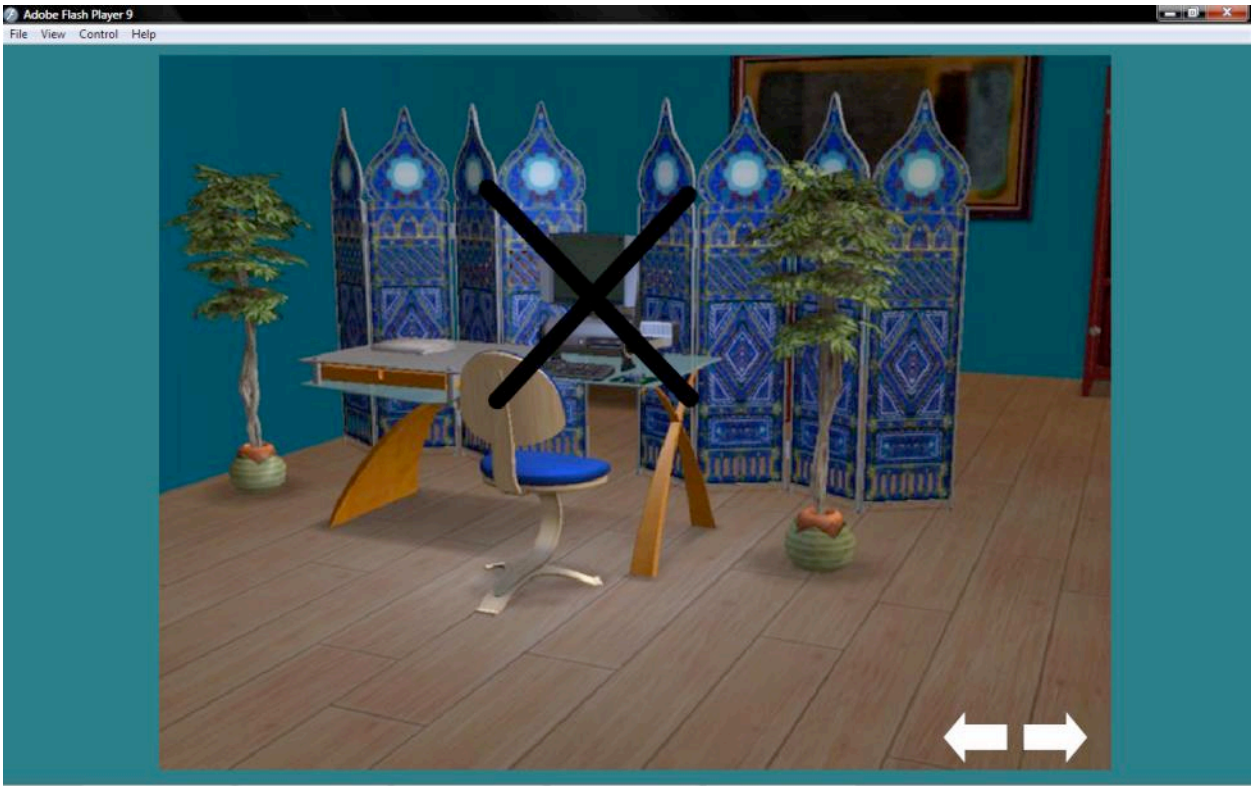

Adobe Flash Player 9
File View Control Help
You have a key to the locked door so you can also visit room B whenever you like.


Adobe Flash Player 9
File View Control Help


Adobe Flash Player 9
File View Control Help
However, this is a high crime area of the city and if anyone decides to break into the apartment building, they can take whatever they want from the room you occupy, room A


Adobe Flash Player 9
File View Control Help
There is no chance that the items will be recovered so any personal items you brought with you are also gone for good.


Adobe Flash Player 9
File View Control Help
Even worse, you must pay a replacement fee for any stolen items that Miss Landry provided with the room.


Adobe Flash Player 9
File View Control Help


Adobe Flash Player 9
File View Control Help
Miss Landry will refurnish the room the best that she can, but there are no guarantees.


Adobe Flash Player 9
File View Control Help
Those are the rules.


Adobe Flash Player 9
File View Control Help
Room B is very basic. It is furnished but the furnishings are modest and there are very few extras.


Adobe Flash Player 9
File View Control Help

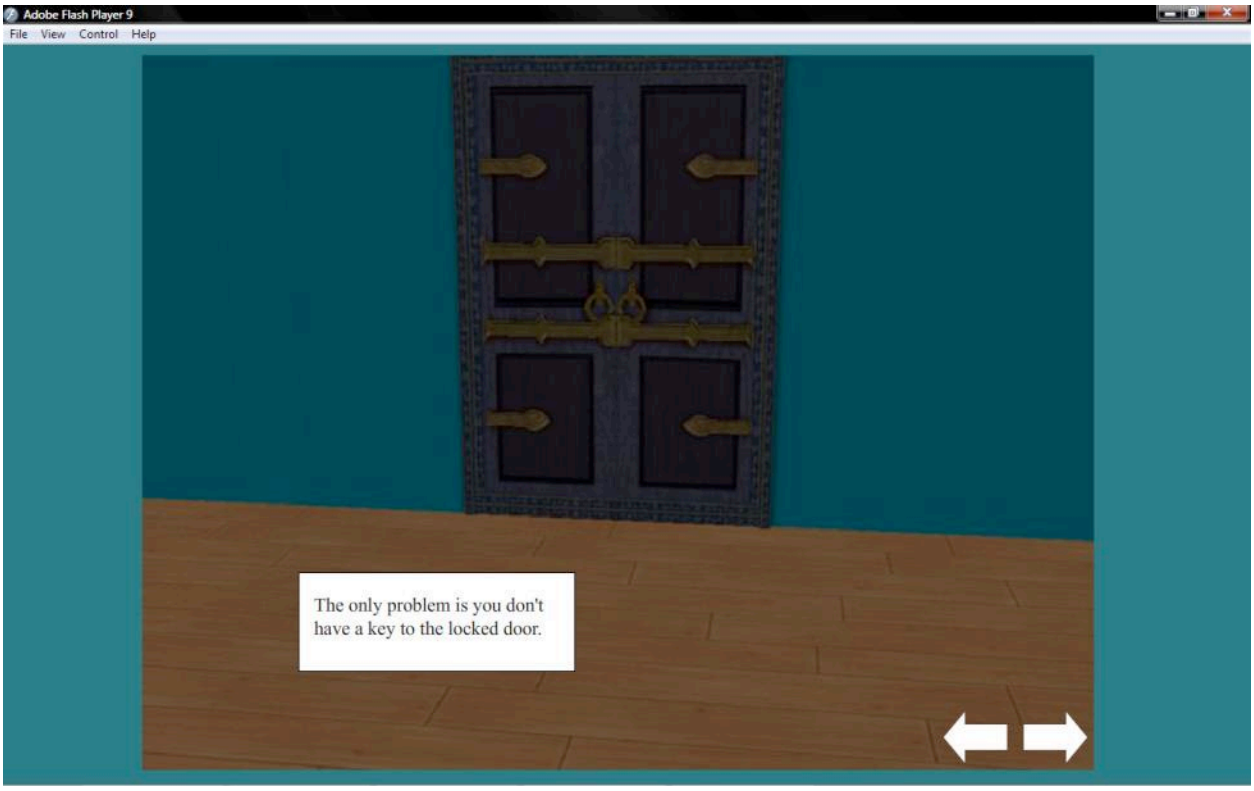

Adobe Flash Player 9
File View Control Help
This is a room that satisfies your basic needs of eating, studying and sleeping.

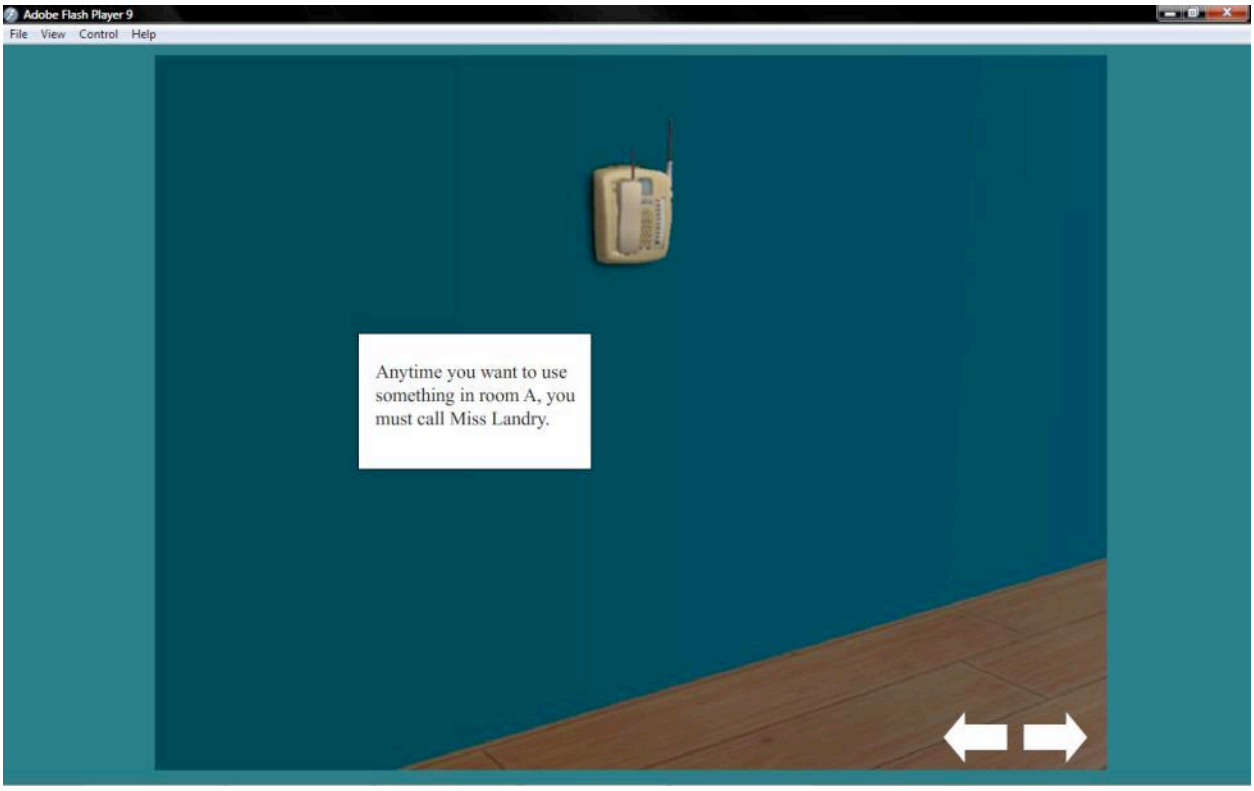

Adobe Flash Player 9
File View Control Help
Of course, you are free to use the few items in the room as much as you like.


Adobe Flash Player 9
File View Control Help
The great thing about room B is that if someone breaks in, even though you have to pay a replacement fee, there is nothing worth stealing really.


Adobe Flash Player 9
File View Control Help
Remeber, intruders can only steal from the room you actually live in, room B.


Adobe Flash Player 9
File View Control Help
Also, if you occupy room B you can use the amenities in room A

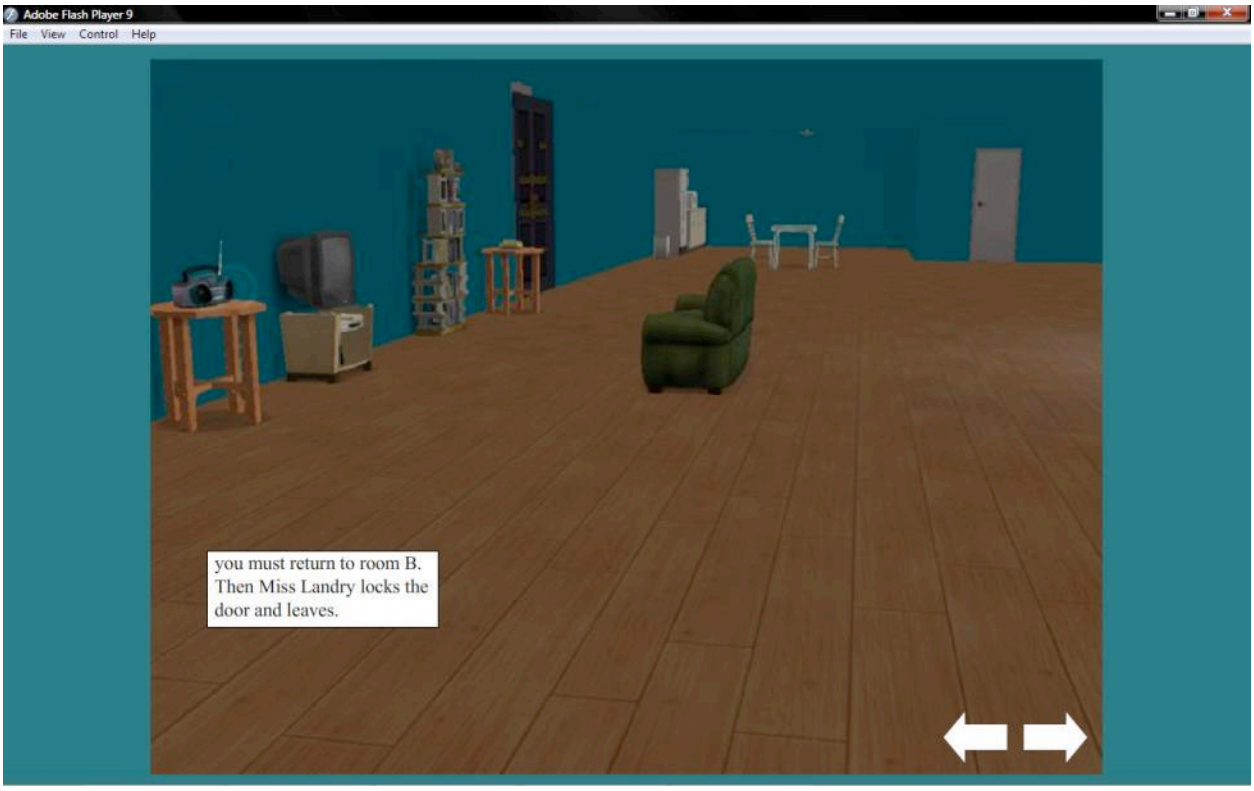

Adobe Flash Player 9
File View Control Help
The only problem is you don't have a key to the locked door.


Adobe Flash Player 9
File View Control Help
Anytime you want to use something in room A, you must call Miss Landry.


Adobe Flash Player 9
File View Control Help
She will come over, 24/7, and unlock the door to the room for you.

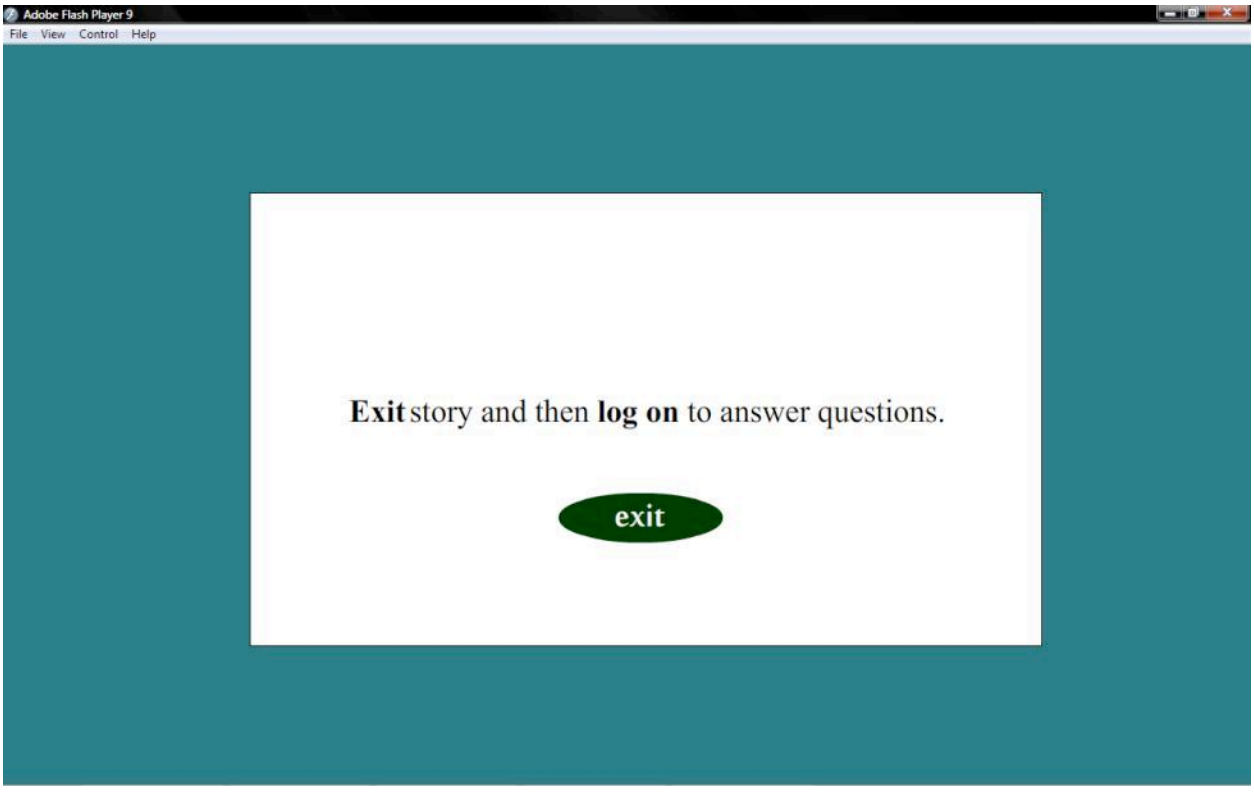

Adobe Flash Player 9
File View Control Help
Unfortunately, Miss Landry can't drive and she walks very slowly. She has to call a taxi and once she arrives, it takes her a while to get to your room.

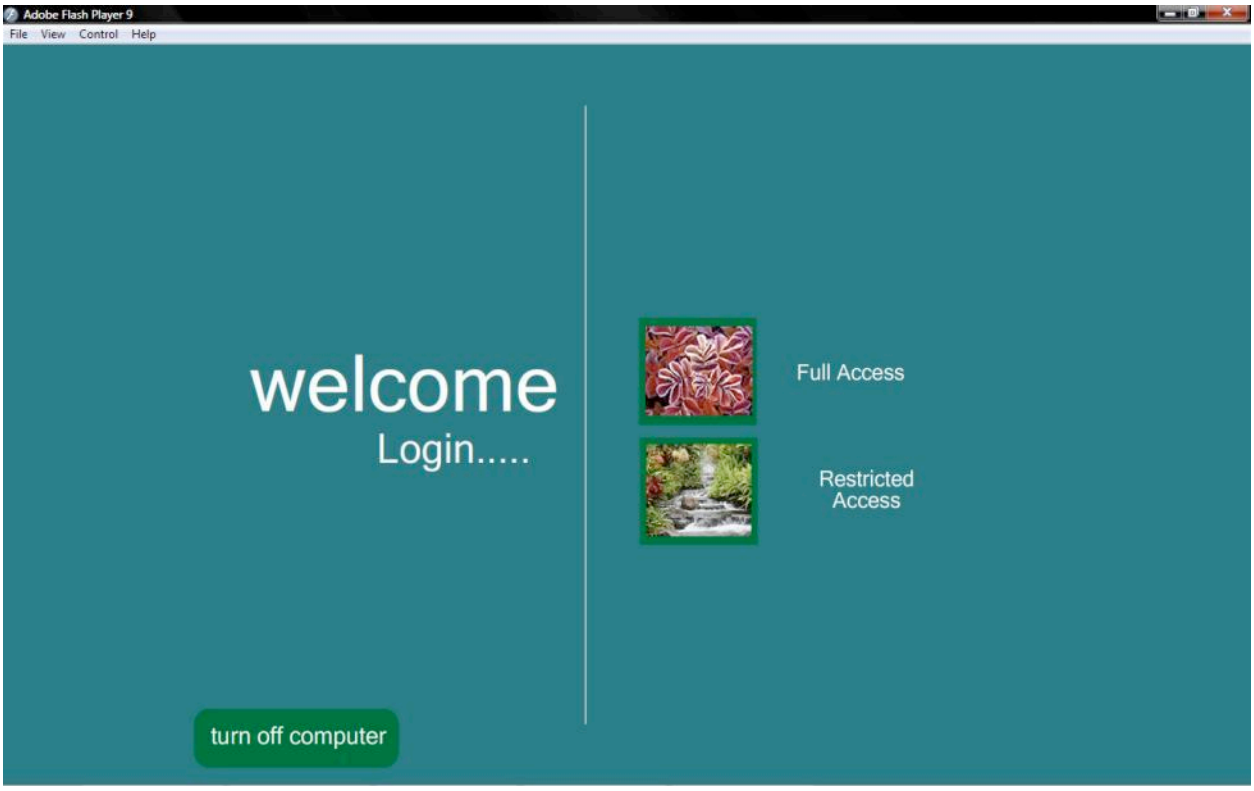

Adobe Flash Player 9
File View Control Help
When you are finished in room A...

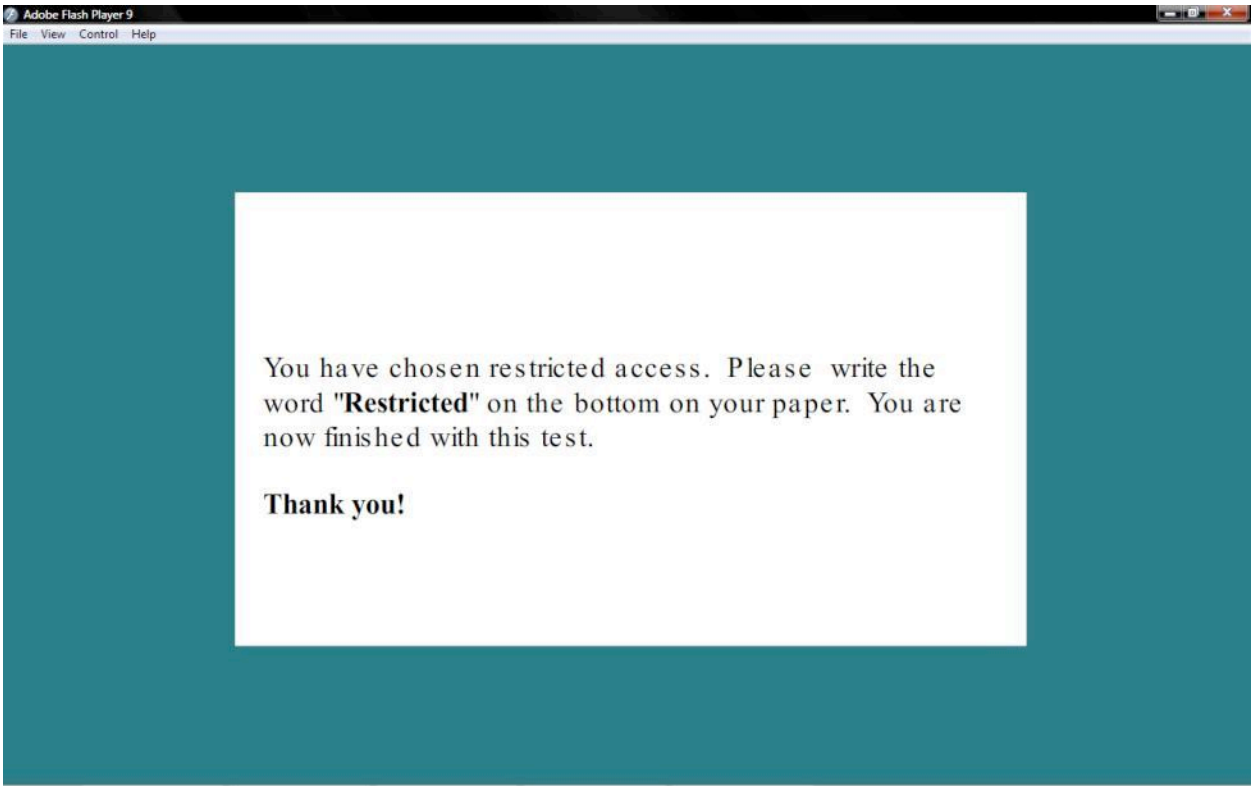

Adobe Flash Player 9
File View Control Help
you must return to room B. Then Miss Landry locks the door and leaves.


Adobe Flash Player 9
File View Control Help
If you want to use anything in room A again, you have to call Miss Landry and she will return to unlock the door.


Adobe Flash Player 9
File View Control Help
I told you she's odd!


Adobe Flash Player 9
File View Control Help
Exit story and then log on to answer questions.
exit


Adobe Flash Player 9
File View Control Help
welcome
Login.....
Full Access
Restricted Access
turn off computer


Adobe Flash Player 9
File View Control Help
You have chosen restricted access. Please write the word "Restricted" on the bottom on your paper. You are now finished with this test.
Thank you!