

KEEPING STIMULI SECURE

September 2006

During the course of providing more online research options to our clients, conducting either real-time or bulletin board focus groups online has become an excellent option that we offer our clients. Online qualitative groups have numerous benefits over traditional focus groups: faster turnaround, more detailed and thoughtful responses from participants, and a reduced travel schedule. They also offer flexibility for participants and clients, which can sometimes translate to lower project costs. Discussions take place at a secure, hosted website and can accommodate a variety of stimuli. (For more information on online qualitative methods and our experience, refer to the white papers “At My Own Pace, In My Own Place” and “Threaded Qualitative Discussions.”)

One of the key questions that clients have inquired about, however, concerns the security measures in place during an online group to ensure that any proprietary stimuli (i.e., new product concepts) are kept confidential to the participants, and not somehow duplicated or retransmitted. In online qualitative research, as in all research Doxus conducts, confidentiality is a top priority. This paper discusses the security measures that are currently available for online focus groups and bulletin board threaded discussions.

HOW SECURE IS THE ONLINE ENVIRONMENT FOR QUALITATIVE RESEARCH?

Currently, there is no 100% guaranteed method of protecting materials from being duplicated or retransmitted, but there is an arsenal of security measures that Doxus can employ, as well as techniques that clients and researchers can use, to reduce the risk.

Most vendors doing online qualitative research have designed their software to provide certain measures of security, anything from password protection for participants and observers, which helps to prevent uninvited participants from entering the virtual facility, to SSL data transfer encryption. There are additional steps that can be taken if presenting stimuli to participants.

WHAT CAN BE DONE TO ENSURE SECURITY OF PROPRIETARY STIMULI DURING ONLINE QUALITATIVE RESEARCH?

Although there is nothing that will guarantee that an image or concept cannot be duplicated while presented on an online bulletin board or to an online focus group, there are some precautions that can make it more difficult for this to occur.

The screening process takes on greater importance when recruiting for an online group as it is an opportunity to set clear expectations regarding confidentiality and weed out respondents who might not comply. One method is to require participants to sign a non-disclosure agreement (NDA) before allowing them to participate.

During an online focus group, the moderator controls when the stimulus is presented and can close it at any time. In terms of bulletin board focus groups, respondents have more control over when they view stimuli, but the moderator can still limit exposure to a specific length of time. The moderator can also make it possible to see a stimulus only once, deterring respondents from going back to that image to copy it using the print screen function, right-clicking to save it to their hard drive or taking a picture of the monitor.

Other ways to deter misuse of stimuli include: limiting the number of sensitive stimuli that respondents can view each time they log into a bulletin board or online group, placing stimuli securely on the Doxus website server (only accessible by Doxus employees or logged-in participants and clients), and providing links for viewing from the group interface website.

Some vendors advertise the ability to protect visual concepts. There are software protection products that can disable certain download/saving functions, but these require respondents to install the software, which might inhibit participation. Doxus could also purchase special software to protect against these functions, and then run all stimuli through the software before loading them into the group interface website.

Any method of limiting exposure could add to the cost of a project, but does not need to be expensive. Downloads like SmartEncryptor are only about \$20, and Secure Image 2.2 is a free download. Secure Image protects images using image encryption and domain lock. Instead of placing a normal image onto an HTML page, the image is first encrypted for insertion into a viewer. The applet viewer that sits on the page replaces the image. The encrypted image is unusable unless displayed from its viewer. Only the encrypted images are uploaded to the server, so the images are safe from everyone, including the group interface website vendor. Secure Image software prevents unauthorized linking of images from other websites, "right click" saving of image files and direct downloading to the hard disk.

SmartEncryptor has the option to "shred" the original file after it has been enciphered. Shredding a file means writing over the contents with meaningless data. This is much more secure than simply deleting the file. The operation of deleting a file can often be undone by a computer expert or a forensic computer examination.

It is possible to use some additional programming to prevent someone from right-clicking and copying the image, but nothing is going to prevent someone from being able to take a picture of it.

Digital watermarks can also be applied to images to "copyright" them as Doxus or client property. There are several software applications out there for about \$25 to \$30 that can be used to integrate watermarks into photos. No software program, even the watermark software itself, can remove the watermark without damaging the integrity of the images. Only the author has full control over his/her watermark since the author works with the original images. This concept is very similar to the Adobe PDF document that a reader cannot alter, except that PDF does allow minor changes at the author's discretion.

CONCLUSION: IS IT SAFE TO USE STIMULI DURING ONLINE GROUPS?

If content (visual or descriptive) is highly confidential, the benefits of testing it may not be worth the potential risk of compromising its security. However, if some of the above basic

steps are in place, the likelihood of respondents being able to redistribute such materials is very low—they'd have to be well-prepared to steal any industry secrets to pass them along to competing companies. If a client requires a 100% guarantee that it won't happen, then the stimuli shouldn't be put online. The extra steps that can be taken will help, but will not completely eliminate the chance that a stimulus can be copied. There will always be some way that a determined respondent might find to bypass security measures.

Any exposure to proprietary content, whether it takes place in face-to-face focus groups or online, means that this person or group will now have knowledge of it and could potentially share it with others. The best protection is to put additional screening steps in place, or an NDA, to recruit a group of respondents who have agreed to the confidentiality requirements of the research.