Evaluation of the Massachusetts Aggression Reduction Center's High School Cyberskills Curriculum (2010-2011)[1]

Background Information:

In September 2010, the Massachusetts Aggression Reduction Center published and made available to Massachusetts schools a Curriculum intended to increase Cyberskills among high school students (the "MARC High School Cyberskills Curriculum"). This Curriculum does not focus on basic technical knowledge (e.g., how to send an email) but rather seeks to increase knowledge about facts that impact student commission of, and vulnerability to, cyberbullying. The Curriculum offers 10 age-appropriate Lesson Plans for grades 9 and 10, and 5 Lesson Plans for grades 11 and 12. It uses Writing Prompts, Case Studies, and Discussion to teach the content to students.

During the fall of 2010, a pilot program was launched to systematically evaluate the potential impact of the Curriculum. This evaluation study was a within-subjects, pre-test post-test design. Students were tested on their knowledge prior to the Curriculum, and then re-tested afterwards. (Not all students completed both the pre-test and the post-test and thus not all students could be included in every analysis.) Changes in their knowledge levels were subsequently calculated and analyzed through Paired Samples T-tests and Time1-Time2 distributions.

The study was conducted in four high schools in Massachusetts. The study sample consisted of 1,444 children in grades 9 through 12, who were given the Lessons Plans in one of their classes (often Health or History) during the spring term of 2010-2011. Teachers did not rate students and official rates of cyberbullying were not measured. This evaluation directly measured *any change in student knowledge about Cyberskills following the implementation of the Curriculum.* The four schools described in this report all volunteered to participate.

Variables Measured:

---

[1] This report was written by Dr. Elizabeth Englander, Director, Massachusetts Aggression Reduction Center, Bridgewater State University, Bridgewater, MA. Contact us at MARC@bridgew.edu.

The variables studied were based directly upon the content of the Curriculum. Across grades 9 through 12, six general topics were examined:

- General knowledge about social networking;
- Knowledge about privacy limitations within social networking;
- General knowledge about cyberbullying and cyber-behaviors;
- Internet-based scams, theft, and phishing;
- Cookies, Behavioral Tracking, and Targeted Advertising;
- Laws about making and using video/audio recordings.

General Findings:

Every topic and grade level studied resulted in statistically significant differences between Time 1 (the pre-test) and Time 2 (post-curriculum) levels. A few individual lessons found no significant difference between the two Times. The Curriculum was moderately reliable (Chronbach's alpha = .37). Within-subjects differences were, across the entire Curriculum, statistically significant ($F=4.7, p<.000$). The analyses for separate curricular topics are found below.

Means for all variables measured can be found in Appendix A.

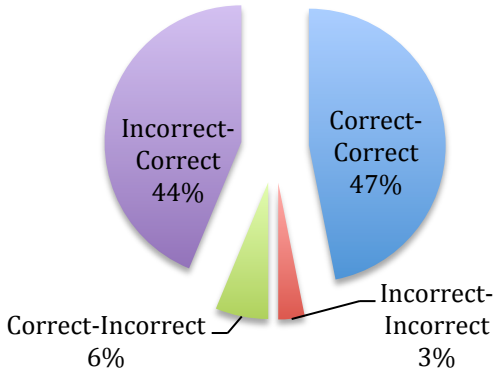
General knowledge about Social Networking:

Students significantly increased their general knowledge about social networking between Time 1 and Time 2. All questions in this category (100%) showed significantly higher mean scores after the Curriculum, when compared to pre-test levels of knowledge.

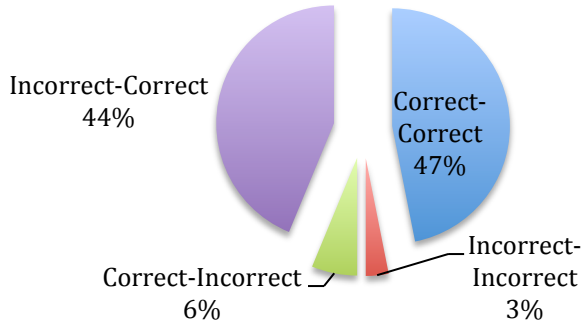
- Friends have power over you online ($t=-3.483(99), p<.002$).
- You cannot control what other people do with images or text online ($t=-3.483(99), p<.002$).
- New users in Social Networking often make the mistake of constantly posting about every detail of their lives ($t=-1.970(99), p<.052$).
- Geolocation apps (often used in social networking) can reveal your physical location to others ($t=-5.557(99), p<.000$).
- How to report abuse to a website ($t=-6.486(99), p<.000$).

Generally, students in this category of knowledge either knew the material before the Curriculum's implementation (at Time 1) or learned it during that implementation (by Time 2). The students were generally fairly equally split between those who knew items at Time 1, and those who knew it only at Time 2. One exception was the lesson about how new social networking users tend to over-expose themselves; most students knew this at Time 1 (prior to the implementation of the Curriculum). See several distribution examples (below).

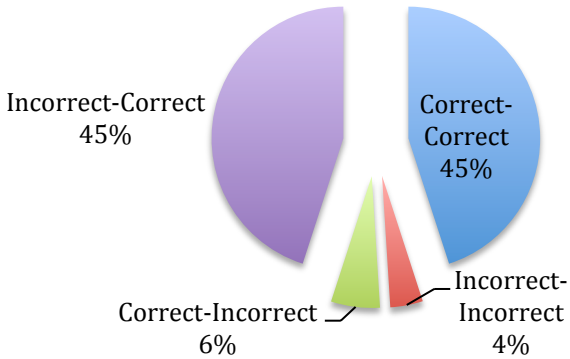
You can't control what your online "friends" do with your information. Change T1 to T2



Your online "friends" have some power over you. Change T1 to T2.



Knowing how to report abuse on a website. Change T1 to T2.

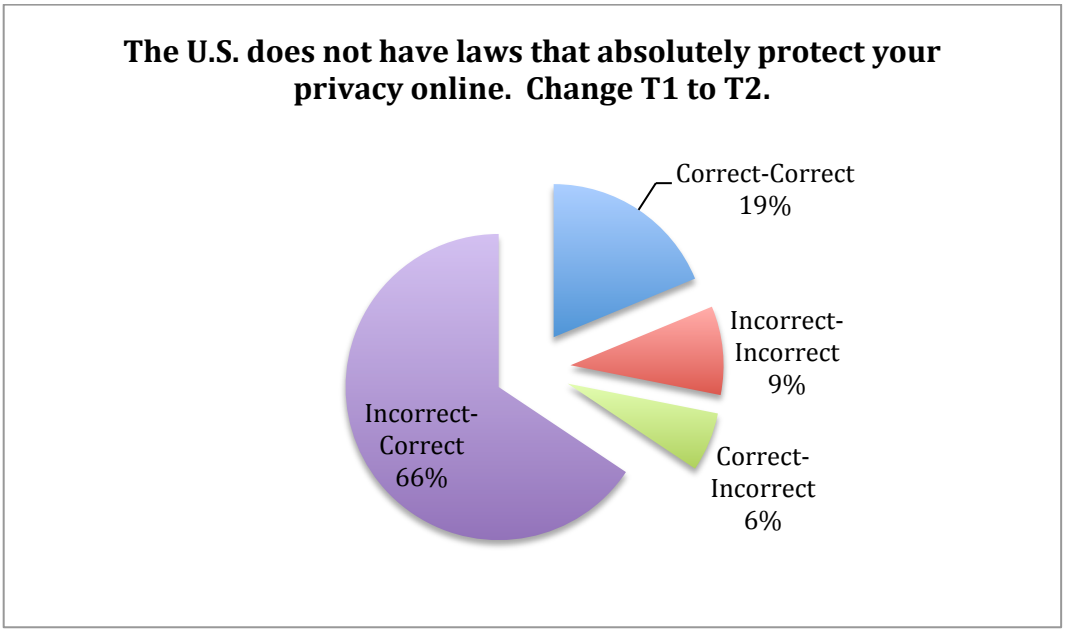


Privacy Online in Social Networking

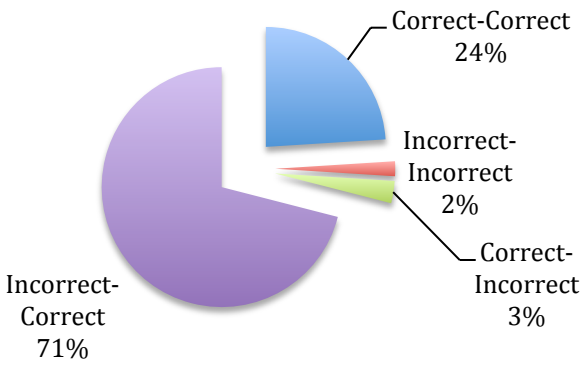
A second category taught students about the limitations of privacy within social networking. This category found that 80% (4 out of 5) of the lessons taught resulted in statistically significant gains in knowledge.

- As long as your profile is "private," you can do and say or tag anything or any body, and it won't be a problem (t=-18.303(99),p<.000).
- Making threats online is never ok, even in “private” profiles (t=-1.00(99),p=n.s.).
- There aren’t laws that guarantee your privacy online; you must protect it yourself (t=-5.463(99),p<.000).
- What are Internet Protocol Addresses, and how they are related to anonymity online (t=-12.842(99),p<.000).

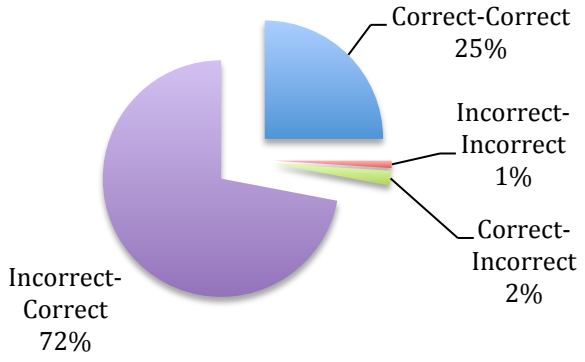
Distributions of these items varied. For some items, most students did not know the topics at Time 1, but learned them successfully by Time 2. However, students did know that “jokes” about serious threats cannot be made online, even in “private” profiles, so their scores on that lesson did not change much between Time 1 and Time 2. Finally, for some items, about an equal number of students knew the material at Time 1, and learned it by Time 2 (See examples below.)



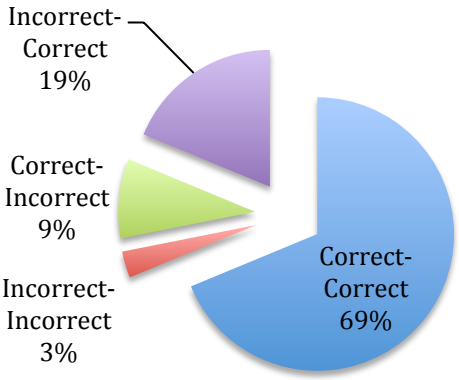
IP Addresses are unique to each device/computer. Change T1-T2.

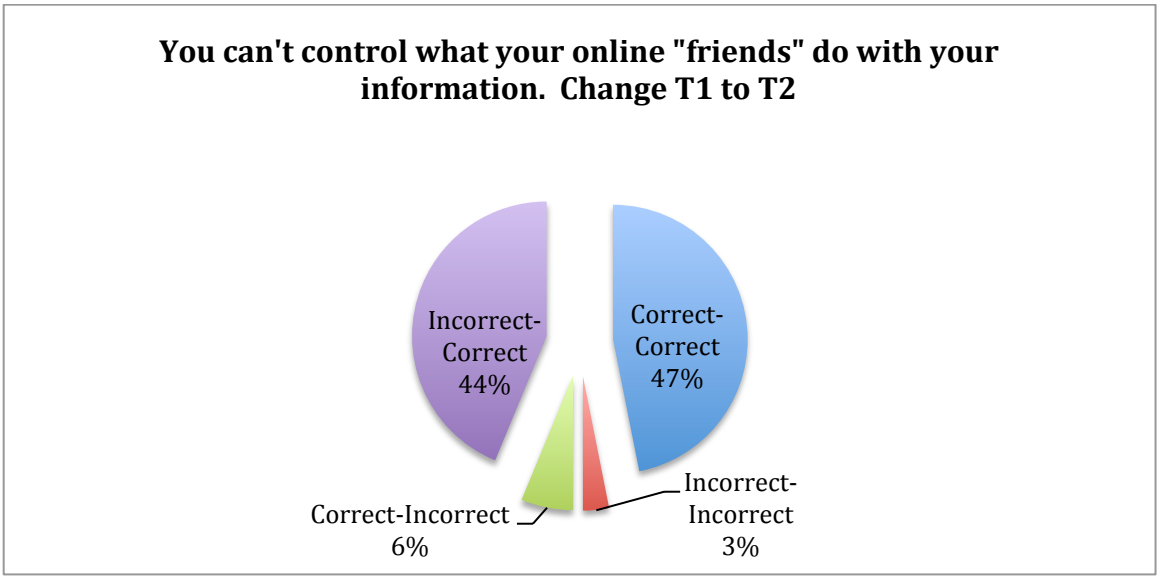


IP Addresses are used to identify computing devices. Change T1 to T2.



You can't make threats online, even in a "private" profile. Change T1 to T2.





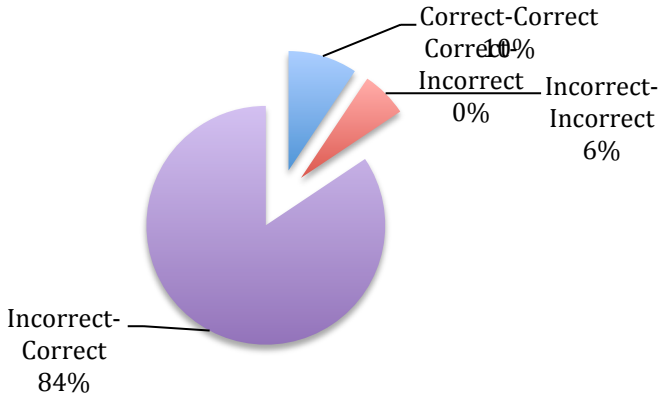
General knowledge about cyberbullying and cyber-behaviors:

Students were taught a relatively higher number of lessons that dealt directly with cyberbullying and cyber-behaviors. Students scored significantly higher in the post-test (Time 2) than they did during the pre-test (Time 1) in 89% of the lessons (8 out of 9).

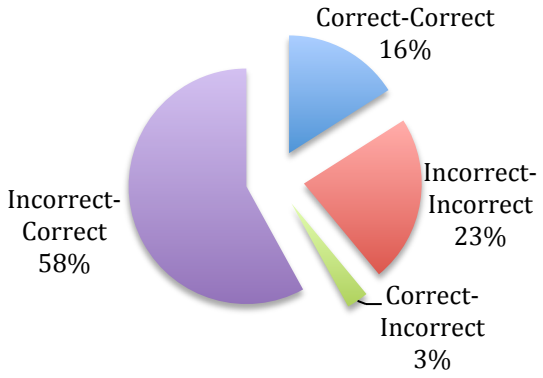
- Cyber-conflict versus cyberbullying (t=-9.869(99),p<.000).
- Cyber-conflict versus cyberbullying (t=-2.509(99),p<.018).
- Cyberbullying can sometimes involve criminal behaviors (t=-12.938(99),p<.000).
- Students do have freedom of speech when they are not at school, but there are limits to this type of freedom (t=-1.531(99),p=n.s.).
- Adults are sometimes over-anxious about cyberbullying, but it is still an important issue (t=-2.254(99),p<.032).
- How to end cyberbullying (Ignoring versus revenge) (t=-5.191(99),p<.000).
- Cyberbullying doesn't focus on personal vulnerabilities in the same way as bullying (t=-3.638(99),p<.001).
- Texting when you're upset can escalate your emotions (t=-12.574(99),p<.000).
- Sexting sometimes happens because someone is pressured, coerced, or bullied (t=-6.676(99),p<.000).

The distribution of these items primarily showed a pattern whereby most students learned the materials successfully by Time 2 but did not know them at Time 1. However, a few items were already known by a large minority of students at Time 1, and learned by another large minority by Time 2 (see examples below).

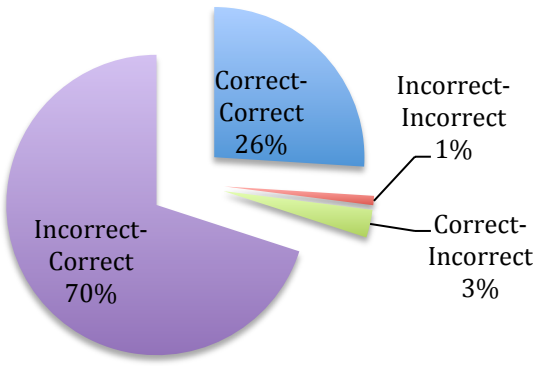
Cyberbullying can involve criminal behaviors. Change T1 to T2.



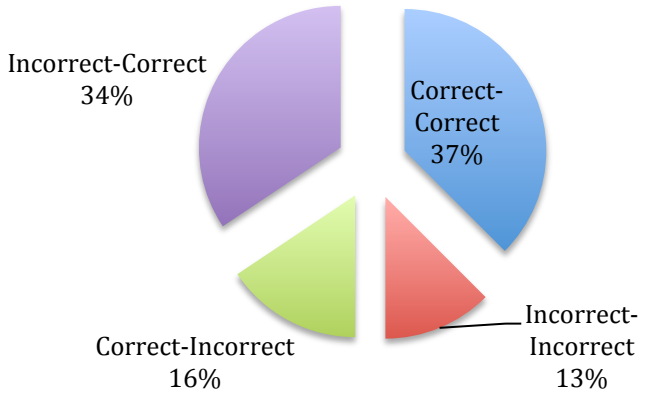
Cyberbullying versus Cyber-conflict. GR9. Change T1 to T2.



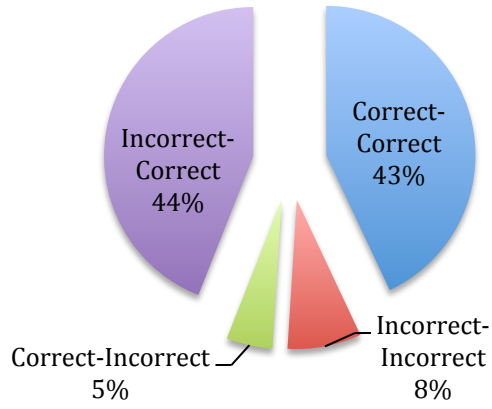
Texting while upset is a bad idea. Change T2-T1



Online behaviors that occur off-campus may be subject to school discipline (or not): U.S. Supreme Court. Change T1 to T2.



Sexting sometimes happens due to pressure or coercion. Change T1 to T2.



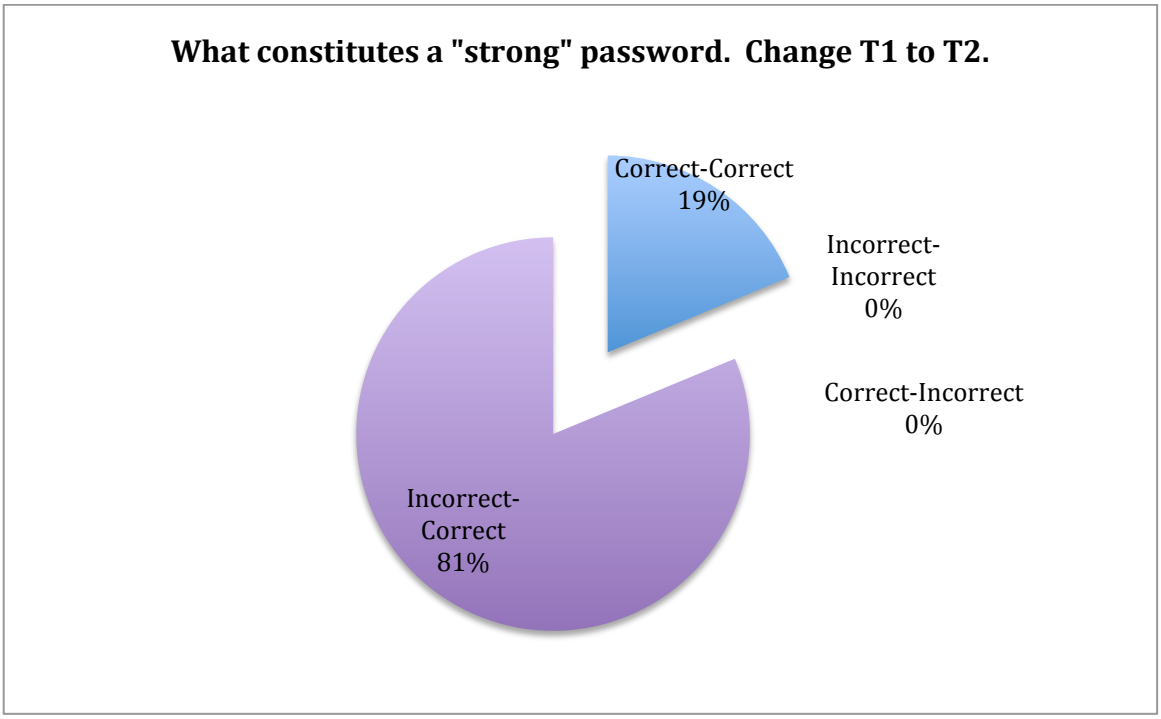
Computer scams, theft, and phishing:

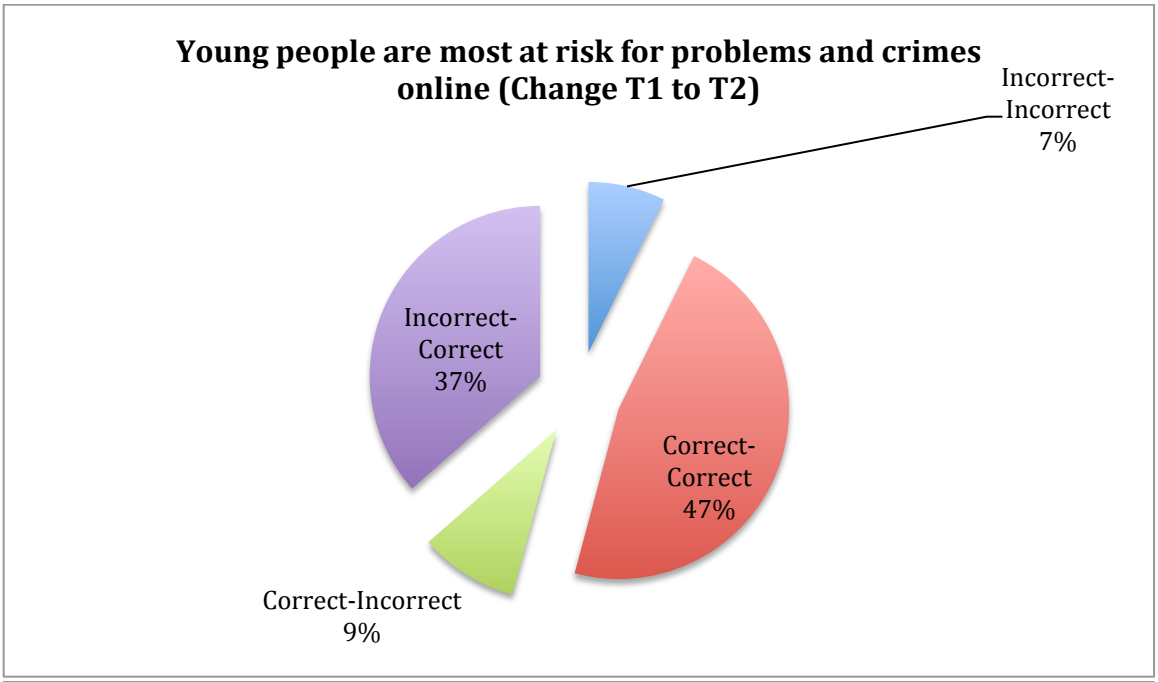
This area examined scams and theft that are largely internet-based and the vulnerability of young people to such scams. Students' scores at Time 2 were statistically significantly higher, compared to Time 1, for every lesson plan (100%) covering these topics.

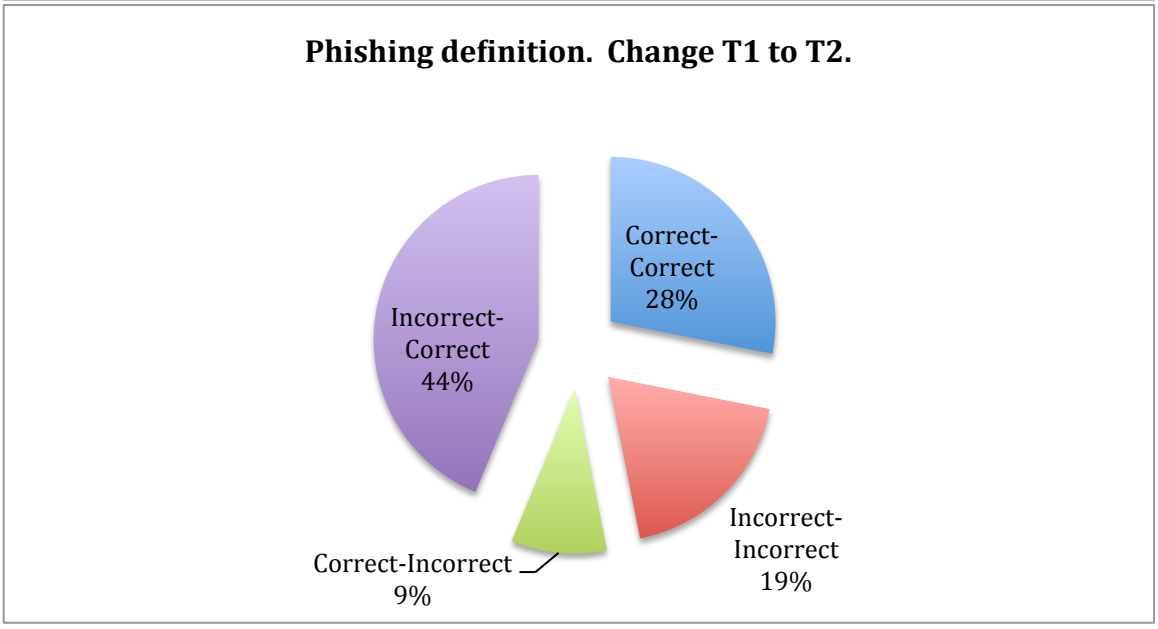
- Phishing is when messages or emails trick the user into revealing information about themselves (t=-2.978(99),p<.006).

- Younger people are more at risk for computer scams and theft (t=-3.184(99),p<.002).
- Phishing is when messages or emails trick the user into revealing information about themselves (t=-3.775(99),p<.001).
- URL Shorteners are sometimes used to hide fraudulent or dangerous websites (t=-5.191(99),p<.000).
- Smartphones are targets for computer scams and theft (t=-4.525(99),p<.000).
- What is a "strong password" (t=-11.59(99),p<.000).

Distributions showed some variation in how many students knew the topics prior to Time 1. In each case, students showed significant gains by Time 2, but for some items, a large minority of students already knew the topic at Time 1 (see examples below).





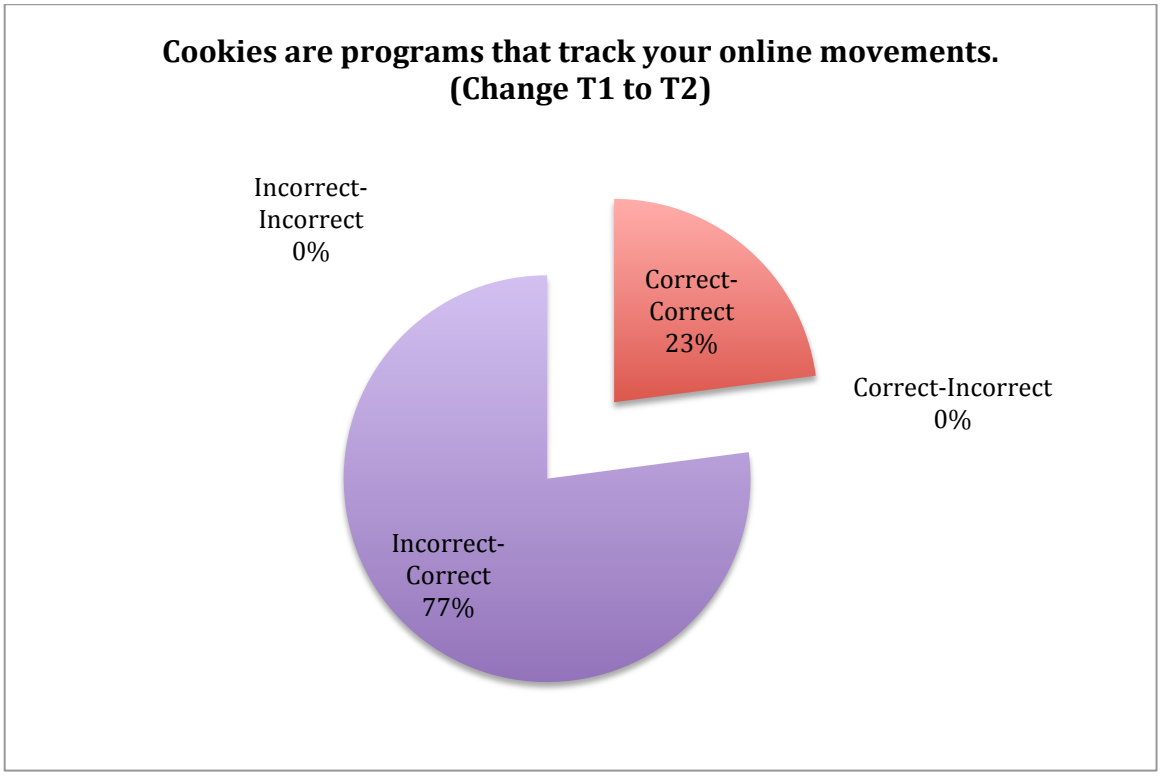


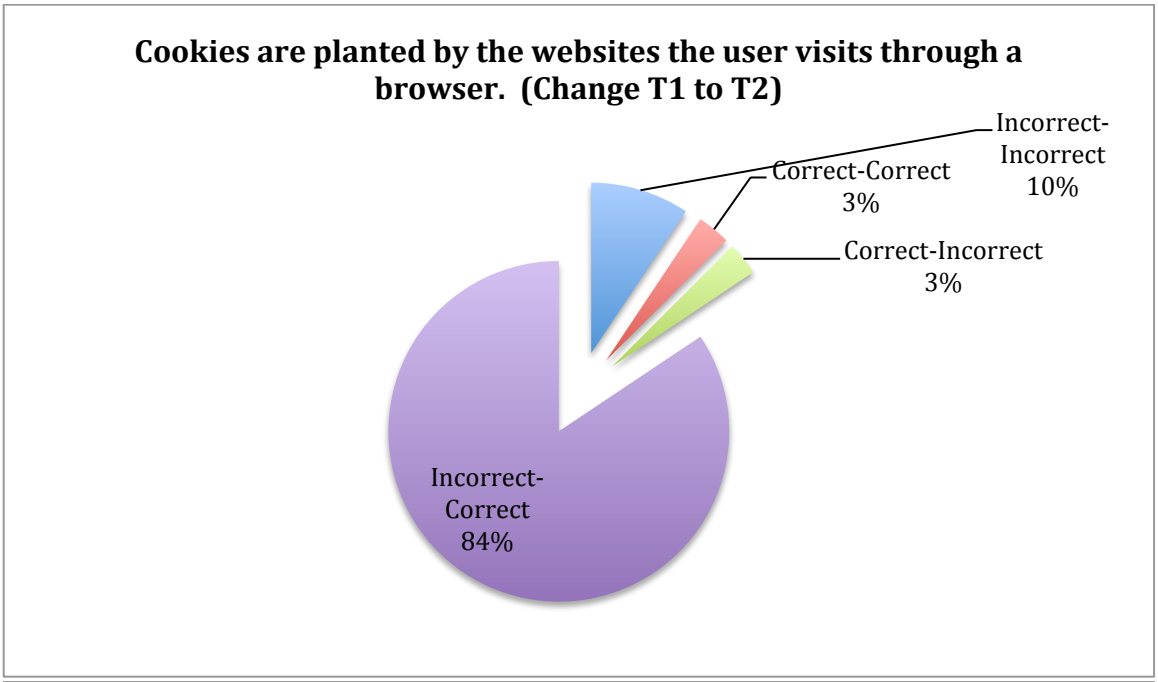
Cookies, Behavioral Tracking, & Targeted Advertising:

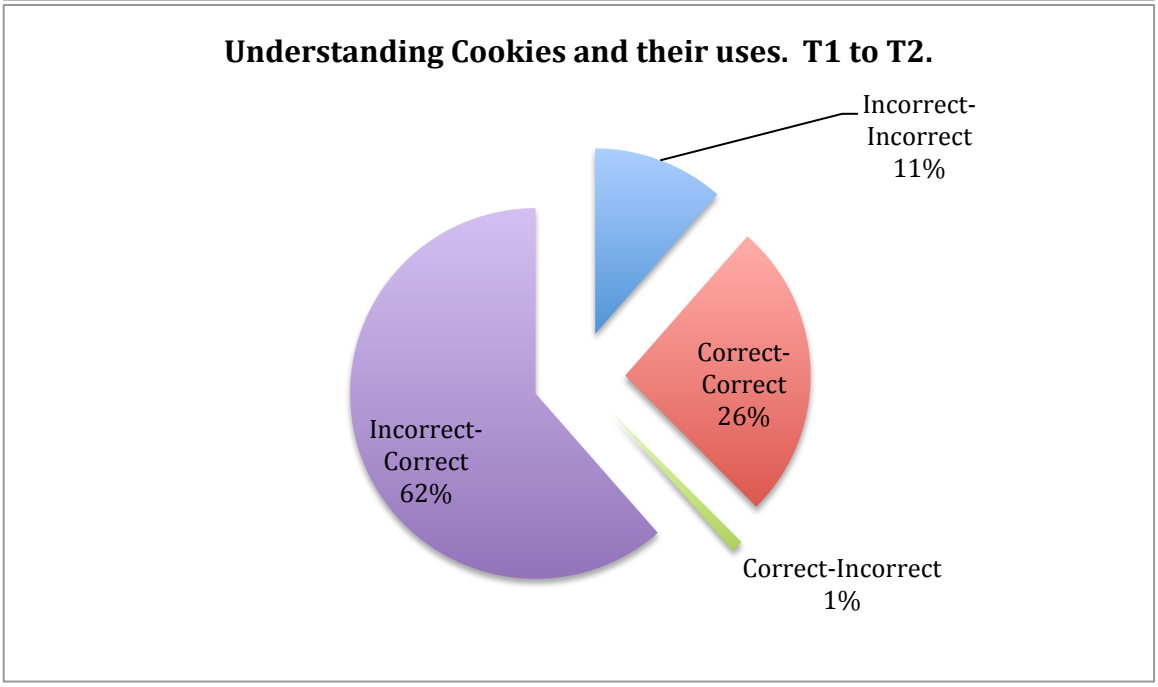
This topic taught students about how marketing utilizes technology and the Internet to learn how people navigate the web and target advertisements at their specific demographic profile. Every item (100%) increased significantly between Time 1 (pre test) and Time 2 (post test).

- Third party cookies (what they are; how they are acquired online) (t=-11.549(99),p<.000). 2nd question: (t=-17.085(99),p<.000). 3rd question: (t=-17.876(99),p<.000).
- What is targeted advertising, and how is it used? (t=-5.477(99),p<.000).
- What is behavioral tracking of online users, and how is it used? (t=-5.477(99),p<.000). Question #2: (t=-6.298(99),p<.000).

Overall, distributions showed that there were not high numbers of students who knew these items prior to Time 2. Most demonstrated increased knowledge between Time 1 and Time 2 (see examples below).





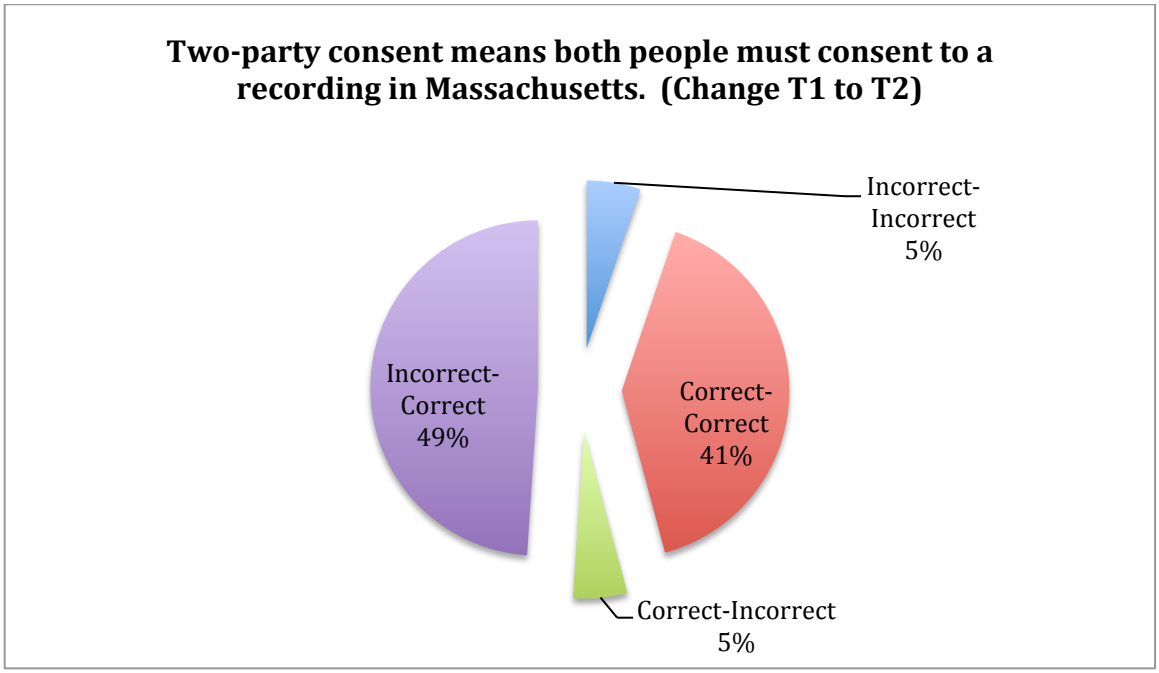


Laws about video/audio recording:

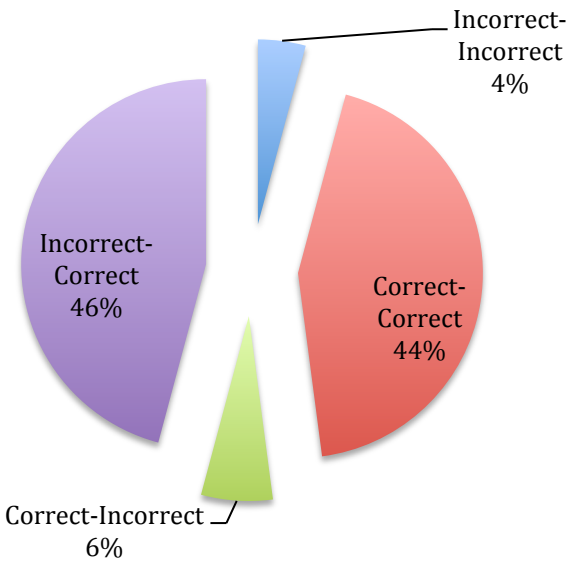
Most (80%) of the items in this section showed significant gains between Time 1 and Time 2. The exception was the illicit use of copyrighted video materials online, about which students demonstrated high knowledge at Time 1 (and thus there was little change by Time 2).

- Recording video/audio laws and two-party permission, and state law in Massachusetts (t=-6.393(99),p<.000). 2nd question: (t=-6.951(99),p<.000). 3rd question: (t=-8.618(99),p<.000).
- Legality of taking pictures in public (t=-12.842(99),p<.000).
- Copyrighted materials online cannot be re-used at will (t=-1.408(99),p=n.s.).

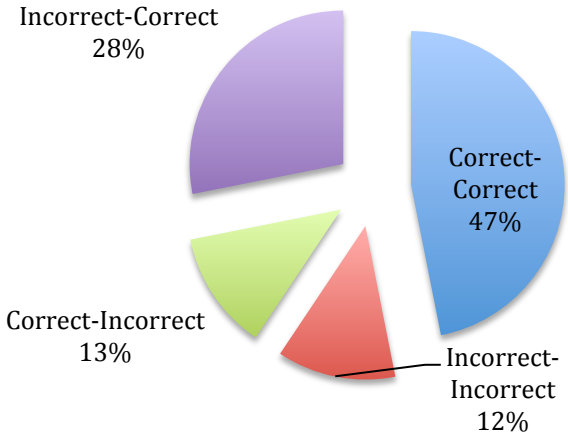
Distribution patterns showed that while a large minority of students knew the materials at Time 1, generally as large or larger proportions did not demonstrate knowledge until Time 2. The exception was the distribution of students' knowledge of copyrighted video materials limitations; many students knew at Time 1 that even materials available on public areas of the Internet could be subject to copyright limitations (see examples below).



Legal limits of video recording. T1 to T2.



Online videos can be copyrighted, even if they're posted in a public area. Change T1 to T2.



DISCUSSION

The purpose of this Curriculum is to teach students factual knowledge about cyberbullying and their utilization of the Internet. Students were tested to assess their knowledge at Time 1 (prior to the implementation of the Curriculum) and again at Time 2 (after the implementation of the Curriculum). Overall, the Curriculum did differ significantly between Time 1 and Time 2 and almost every lesson showed statistically significant differences between the Time 1 and Time 2 mean scores. For some lessons, it was evident that the majority of children did not know the materials at Time 1. For other lessons, equal numbers of students knew and did not know the materials at Time 1. The Time 1 data suggests that students may vary greatly in their knowledge about these topics. Very few items showed high levels of knowledge at Time 1, which supports the need for a Curriculum such as this one. Further, no items showed low levels of knowledge at Time 2, which supports the Curriculum's efficacy. The lessons that were not statistically significant generally had higher proportions of students who knew the topic at Time 1, and thus there was less change by Time 2. But regardless of their status at Time 1, it was evident from the analysis that many students could benefit from the Lessons in this Curriculum.

The results of this pilot strongly suggest that the Curriculum is effective in its goals, but there are important limitations to consider. First, while it could certainly be argued that learning alone is never a bad thing, this study did not directly measure if the Curriculum reduced cyberbullying or cyber-conflict behaviors. A future evaluation of this Curriculum could ask students if they believe that their increased knowledge will have any impact on their cyberbullying behaviors. (Measuring cyberbullying directly is almost certainly impossible. Self-report is the only viable option for this largely undetected behavior.)

In addition, this study is limited in its time span. It only considered short-term changes in knowledge, and did not measure if the changes were retained over a longer period of time. Presumably, the longer the period of time, the greater the impact upon behavior.

Finally, this within-subjects pre-test post-test design, utilized in this quasi-experimental study, is clearly not as strong as an experiment which utilizes randomized assignment to experimental and control conditions. The quasi-experimental design utilized here is essentially a compromise that enabled us to evaluate the impact of the Curriculum, but our ability to draw definitive, absolute conclusions is limited as a result. One limitation is the possibility of maturation – that the children simply matured during the test period and it was the "growing up" that accounted for the change between Time 1 and Time 2. However, the possibility of maturation was mitigated here by keeping the time period of the pilot study quite short (about 12 weeks). Theoretically, it's also possible that another variable in the schools changed at the same time as the Curriculum, and that this other variable accounted for the change observed. However, this second variable would have had to explicitly teach the concepts covered in this Curriculum, and this is so unlikely as to be truly implausible. Realistically, most adults and children today are often ignorant of the concepts taught here, and therefore ill equipped to provide a broad, widely available

secondary source of specific education on several school campuses.

Recommendations:

- The Curriculum appears to significantly improve the cyber-skills of children in Grades 9-12 (High School);
- We do not have data on children in other grades (e.g., utilizing these lessons in Grade 6, 7 or 8);
- Schools utilizing the Curriculum are urged to review it carefully and resolve questions in the teaching faculty *prior* to implementation (a Training Day for the Curriculum will be held at the Massachusetts Aggression Reduction Center at Bridgewater State University);
- Schools using the Curriculum are strongly encouraged to utilize the online digital lessons provided therein; finally,
- Schools are encouraged to contact MARC with any questions or concerns about the usage of the Curriculum.

Appendix A. Time 1 & Time 2 means of variables.

Grade 9 Variables.	privacypre	.06
	privacypost	.87
	upsettextpre	.29
	upsettextpost	.96
	sextpressurepre	.48
	sextpressurepost	.87
	reportabusepre	.51
	reportabusepost	.90
	whatiscyberpre	.19
	whatiscyberpost	.74
	allippre	.27
	iptrackpost	.95
	allippre	.27
	whatisippost	.97

Grade 10 Variables	onlinefriendspowerpre	.53
	onlinefriendspowerpost	.91
	strongpwpre	.19
	strongpwpost	1.00
	controlfriendspre	.53
	controlfriendspost	.91
	bombprivatepre	.78
	bombprivatepost	.88
	copyrightpre	.59
	copyrightpost	.75
	conflictpre	.22
	conflictpost	.50
	phishingpre	.38
	phishingpost	.72
	crimepre	.09
	crimepost	.94
	noprivacylawspre	.25
	noprivacylawspost	.84
	freespeechpre	.53
	freespeechpost	.72

Grade 11 variables.	cookiespre	.27
	cookiespost	.88
	videorecordpre	.50
	videorecordpost	.90
	youngriskpre	.56
	youngriskpost	.83

	publicpicspre	.51
	publicpicspost	.71
	constantpostspre	.90
	constantpostspost	.97
	maprivacylawpre	.42
	maprivacylawpost	.82
	recordaudiopre	.26
	recordaudiopost	.77
	cookiesfrombrowserspre	.06
	cookiesfrombrowserspost	.88
	twopartypre	.46
	twopartypost	.90
	whatrcookiespre	.23
	whatrcookiespost	1.00

Grade 12 variables.	trackingpre	.28
	trackingpost	.79
	targetedadspre	.52
	targetedadspost	.90
	estimatepre	.48
	estimatepost	.72
	urlpre	.28
	urlpost	.83
	smartphonespre	.34
	smartphonespost	.83
	cyberbullypre	.21
	cyberbullypost	.76
	geolocationpre	.28
	geolocationpost	.86
	vulnerablepre	.28
	vulnerablepost	.66
	phishingpre	.21
	phishingpost	.72
	tracking2pre	.38
	tracking2post	.97

The Massachusetts Aggression Reduction Center
Bridgewater State University
Bridgewater, MA 02325
(508) 531-1784
email: MARC@bridgew.edu
website: marccenter.org