# Conclusion

Ledin, George Jr. (2005). Not teaching viruses and worms is harmful. *Communications of the ACM, 48*(1), 144.

Up until recently, anti-malware has been responsive, not preventative. Solutions for malware attacks have always come after, or as the victims might feel: too late. As we have seen in going over the history of malware and malware attacks those that seek to prevent vulnerabilities and have largely had to wait until a vulnerability is exploited before it can be identified and fixed. The ‘good-guys’ always fall behind those developing malicious software and will continue to if the issue continues to be address as it has been in the past.

<examples where this has been the case>

The most significant barrier to this has been demonstrated as the fear of danger. Many feel that teaching how malicious software is developed will lead to its students using such knowledge to develop more viruses or worms, or any other malicious code. Similar fears have, in the past, prevented development in medical science, most notably with the ban on dissection of human cadavers for research. Within the computer science field itself that barrier existed around cryptography but has since been overcome and is one of the things commonly taught in classes on security. Often times however these classes are still elective and amount to mostly history classes without any examination of actual source code.

This fear can be overcome, and should be. It is of vital importance that we overcome it. Other sciences, like chemistry, have students conducting experiments with microorganisms and hazardous substances. This knowledge could be used for wrongdoing, and that is certainly a risk, but one that is mitigated by the supervision and oversight within those courses. Students are given this knowledge with the explicit understanding of the use of knowing how biological viruses spread. Knowing how things like West Nile, or Ebola, work and being taught how to develop similar organisms leads to creating vaccines. This is the very foundation of epidemic prevention. There is almost no such work being done in computer science.

Another hurdle to progress is the fear of complicity. Is teaching students how malicious code is made considered aiding and abetting should one of those students go on to use that knowledge to commit crimes? The same could be said of our previous examples with chemistry and biology. Should educators and institutions be held liable should students use the lessons to commit crime? Most people would probably disagree, an individual’s choice to abuse knowledge taught in an ethical context does not reflect on the educator as an accomplice, nor on the importance of continuing to educate in the face of such possibilities.

Due to the lack of education and the fear of “arming” students with knowledge that could be used for nefarious purposes many universities and other education institutions are ill-equipped to handle teaching this subject. Most educators have been through the same system as their students, and lack the same skills the students will lack when they complete their courses. This lack of knowledge and experience on the part of educators and institutions makes them poorly equipped to teach such subjects. This final barrier is one that could be overcome much easier should the first two be dealt with.

So, what can be done? What are our hopes for the future?

The tearing down of discussed barriers needs to happen before any meaningful progress can be made. The fear of teaching potentially damaging things to students is an outdated one. In other fields, most notably within the science community, this fear had been dealt with years ago. It must be noted that in spite of the science community itself have overcome this fear there are still many in the public that misunderstand the purpose of such education, which is a result of the public themselves not being educated in the reasons why such research and learning is important. The hope is that going forward, as the understanding of computer science grows and becomes more commonplace, similar to medicine, the education of students in how computer viruses work will be more easily accepted.

Once the fear of ethical abuse of the imparted knowledge is dealt with, the fear of legal complicity will also fade. It is important to understand that in computer science, as with the study of medicine, biology, and chemistry, the educators must teach from an ethical standing. They teach these courses so that students may better learn how malware works, and be that much better equipped to deal with issues when they arise. Should a student choose to use the knowledge for nefarious purposes it does not reflect on the educator, but solely on the student that made the unethical decision.

Educators and institutions should be able to acquire resources required to teach malware more in-depth than vague explanations of what malware is and does. Students should have access to see the source code of various viruses, worms, and other malware. They should be taught how these are created and how to create them. From here they should be challenged with how to stop them. They should be taught in a safe environment and under supervision. They should be taught the ethical and moral responsibilities of security-minded software development.

While education certainly plays a major role in the defense against malicious cyber-attacks, that defense is not the only benefit. As more people are educated about malware and understanding how what it does becomes more common the general public can be better equipped to handle the issue. The general public can be educated in better practices in regards to security. Like with public health where the average person understands the importance of daily hygiene like washing your hands to prevent the spread of disease, coughing or sneezing into the crook of your elbow, or even wearing a mask to prevent potential air-borne contamination, the average person can develop smarter practices when using computers. Such as not opening an unexpected email from an unexpected source, not clicking any links in an email, not downloading software from unofficial or unverified sources, staying away from risk-laden sites, and better password management.

Work being done by such educators as John Aycock and <other educator> should be championed and mimicked. Education focusing on malicious software should become more commonplace and those willing to teach it given resources to do so in safe environments and with full supervision.

## KEY POINTS

* History has shown a lack of preparedness to prevent attacks
* Fear of teaching “unethical knowledge” is a major roadblock
* Other roadblocks include legal complicity and lack of preparedness of educators and education institutions
* In order to progress we need to overcome the first fear, like the sciences have done
* The other roadblocks will follow, legal complicity must be guaranteed to be “impossible” should a violation of the ethics taught in the course occur
* Educators and institutions must be allowed proper resources to teach
* Resources to create a safe environment with proper supervision, and the tools to reinforce the ethical approach of “learning thy enemy”
* Look to current educators tackling the issue and championing them as appropriate to encourage more widespread education of such topics