Chris DeVisser

ICS4UE

Mr. Wilhelm

**Ethical Computing**

One issue that is happening in our board right now involves user privacy and personal information, as well as identity theft. I’ll get right to it. Are you in school right now? Are you logged onto something such as Facebook? If you are, did you know that a student could be sitting somewhere in the region, happy because a teacher’s Facebook account credentials were just obtained?

The sad fact of the matter is that what I just described is very possible, and proven to work[[1]](#footnote-1). Due to the lack of security, a student could spread a virus around the WRDSB network, undetected, and wait for the perfect moment to strike. This allows any student to do whatever he/she wants on any infected account, whether it’s to keylog it, or to masquerade as it. Private information, such as that found on any website that one might log into at school, as well as one’s identity, are both up for grabs.

At this point, the only two things that can stop a person with the knowledge to do such things are changes that prevent this from happening, and ethical computer use. Unfortunately, for my friends and me, we’ve given up on the former. I can assure you that the school board is well-aware of these problems, but as far as I am concerned, they simply do not care. The most serious issue has been remedied, but not much else.

Sure, then, we could print without using print credits. We could delay the library printers from printing until anyone who needs to print something is late for class. We could steal passwords and pose as other people. We could bring the entire network to a halt. What stops this from happening is ethicality. With great power comes great responsibility. That responsibility is based on your morals to keep things feeling like everything is right and proper. The decision not to cause a serious impact on anyone comes out of respect for them. Others don’t deserve to suffer just because somebody finds something that they have the ability to do to that person.

Many possibilities that can come to one’s mind of what to do with an infected network require some kind of programming. It’s up to the programmer to realize what something they are creating has the potential to do. Even if they wouldn’t use their program maliciously, others might. The truth is that almost every rogue program’s basis can be used for good. Keylogging doesn’t have to be about stealing passwords. I, myself, have considered whipping up a keylogger to allow me to recover something I was writing when it unexpectedly disappears, which happened to me recently when a website logged me out in the middle of writing. It’s computer ethicality that must be relied on to make the right choice about how to create and use software. Viruses have created a whole new market in network and end-user security, but both use very overlapping foundations in their code.

For the people who cannot be swayed through computer ethicality, other measures must be taken. Much of what a student can do should not even be possible in the first place. By implementing protective measures against these threats, it disables those who would use something maliciously from actually doing so. A clear, unambiguous Acceptable Use Policy with well-defined consequences is also key to guiding students down the right path. If both ends work together, computer ethicality is something that could be viewed much more highly than it is, and I would not have to worry about whether somebody could use what I know against me at school.

1. No actual Facebook hacking was attempted, but the same concept can be applied. [↑](#footnote-ref-1)