

Computer ethics

[Technology](#), [Computer](#)



You are not going to get the last word in. Even if you respond with kindness, you are not going to get the person to see the error of their behaviors.

Recognizably if you receive any very specific threat via any electronic form, you can consider notifying the appropriate law-enforcement officials. Know that unless the threats are very precise, D traceable, and reliable, they will likely not be able to help you. The police will almost surely just tell you not to respond in any way. Remember, the cyber bully is looking for attention in any shape. Even if you write back to them with an e-mail that contains nothing but a question mark, which will be plenty to keep them entertained (McLaughlin et al. , 2012). In addition, to ignore insulting emails, instant messages or other postings from cyber bullies. Try changing the settings of any instant messaging programs to allow specified friends only.

This will prevent any bullies from being able to personally attack you while you're online. Switch any social networking profiles to private and only add people you actually know and are friends with. Contact the site's moderator if a cyber bully sends you threatening private messages, or if you see unauthorized postings with your photograph or personal information on his page. This type of behavior is usually a term of service violation, and the site will delete the page and ban the bully. Change your passwords if a cyber bully has hacked into any of your online accounts.

At no time tell anyone else your passwords because you never know if they use them against you. Switch surnames or email addresses to make contacting you more difficult (McLaughlin et al. , 2012). Governmental legislations that website administrator of the event. Most local laws do not cover cyber bullying as such, but do cover bullying in general. More and

<https://assignbuster.com/computer-ethics/>

more school districts are adding cyber bullying policies to their overall bullying policy to help prevent the ever-increasing level of teen suicides associated with cyber bullying (McLaughlin et al. , 2012).

The last example of potential computer ethics issue is computer hacking. Several see the moral issues involved as cut and dry, some consider ethical breaches only when laws have been broken and others believe certain types of hacking ethically sound and some types as ethically questionable.

Techniques to prevent computer hacker's attack can be investing in a good anti-virus program. Norton Anti-Virus or MacAfee Anti-Virus is a leader in virus and spare protection. There are also free anti-virus programs online, such as BAG, which can keep your computer safe as well.

The best part of these programs is they allow you to run virus and spare sweeps at the click of a mouse and get rid of any suspicious for you within minutes. Turn on your firewall. This computer protector should automatically be on at all times, but if you have taken it down for any reason, enable it as soon as possible. Upgrade your passwords. Cracking pass codes is the easiest way for hackers to get into your personal accounts, and it's the easiest thing you can prevent. Clear your cookies and cache regularly.

Whether you're an avid Internet surfer, or you just browse on occasion, your computer will automatically store cookies to remember every site you visit. For the most part, cookies and cache are just harmless memory eaters, but some hackers design them to attack computers (Mali, 1996). Other facts to consider in debates of ethical hacking include the costs related with security checks even when no alterations or harms have occurred. Countless believe

the high amount of youth contributors and factor this into ethical decisions, believing the concealment linked with hacking makes crimes more likely to happen than they would outside of hyperspace.

One-way that people can understand actions for unethical behavior is considering the legitimate. Also, the Governmental legislations that could be enacted against this type of attack could be United States Credit Fraud and Abuse Act prohibits deliberately accessing another 's computer system when it threatens the financial well-being of an individual or business to reveal state secrets, upset international communications, defraud, cause damage or aid extortion. States have their own laws as well. Including financial penalties, imprisonment, and probation for NY illegal computer hacking (Mali, 1996).