Fighting Cyber and Biological Threats

Everybody has heard the word virus and often it is associated with a computer worm. A biological virus is an extremely tiny infectious agent. First, however, viruses aren't even living organisms at all. They're not even living, but they have some very significant characteristic which differentiates them from more inert material.

The first characteristic to look for when studying biological viruses is an ability to replicate itself. If a biological virus can replicate itself and cause infection in a way that replicates itself (and can survive in such an environment), then it is acting like a virus. Viruses only replicate themselves, but in such massive amounts, this makes them exceptionally difficult to detect and keep track of. As such, viruses often hide behind the identity of another file or program. Sometimes a virus is on a disk, but most often it hides on a removable disk or other media used to store information. Viruses are particularly insidious because they do not always manifest themselves in the way that we expect, and often cause unexpected and damaging results.

A second characteristic to look for in a biological virus is an ability to spread. Although it is impossible to catch a biological virus, it is very easy to spread pathogens. Think about it: all forms of bacteria, fungi and viruses spread through contact. (Think of the cold: if you cough or sneeze in public, you can run the risk of spreading some bacteria or fungus to those who catch your cough or sneezing. Of course, many people who get colds often do not develop infections.)

When looking at outbreaks of biological virus infections and how they occur, it is important to remember that there are three basic types of outbreaks: malware, cyber attacks and natural viruses. Malware generally refers to viruses that actively exploit a computer system without the consumer or user permission; cyber attacks are conducted with the intent of obtaining unauthorized access to data or systems; and natural viruses are designed to harm or destroy a computer system. Of these three types, malware is the most common and is what you usually come across when you try to find out more about malware.

A malware infection, when installed, can cause serious problems for your computer system. Once it has been installed, it will perform all sorts of hidden activities on your PC without your knowledge or consent. These activities can include changing your homepage, browser homepage, setting your desktop wallpaper and toolbars, and installing additional software programs. Because of the malicious nature of these activities, it can be difficult to track malware infections and to stop them. Some malware spreads itself silently by changing your homepage, browser homepage and toolbars, and using various executable files and codes to spread across your PC.

Some people say that you can avoid malware infections if you just get rid of bad files and delete junk on your PC. This is true, but that doesn't mean you'll be completely virus free. It's possible that the bad files won't be noticed, because sometimes a file will re-appear after being deleted. Other times, it may not re-appear at all. But as we know, the human mind can only remember things that have a feeling of familiarity, so even if a file

disappears it could reappear within minutes or hours, and that's when your computer gets infected.

The best way to avoid having to deal with biological virus outbreaks is to prevent them. You should do your very best to keep your computer as clean as possible. Regularly scan for viruses by using an online scanner, and if you're unsure whether a file is virus free, then delete it. Don't touch anything that you don't know! If you've downloaded music or movies from the Internet, then make sure you let the software recognize that it was downloaded. And protect yourself by downloading software that helps you remove potential viral threats before they even have the chance to attack your computer!

A clear distinction between cyber threats and biological threats needs to be made in the fight against the misdeeds that lurk online. But unfortunately, our governments are doing little more than attempting to fight fire with fire. Unfortunately, when it comes to cyber threats, all efforts are simply a waste of time. That's why the Czech Republic has taken steps to develop its own cyber security firm known as CDPE - Cyber Security and Public Opinion. Only time will tell whether that effort is strong enough to stifle the advancing biological threat.