The Hacker Attacker

By Gregorio Lobo

In today's world many people are being hacked by criminals that seek to benefit from other people's fortunes. Furthermore, an increase in better technology not only helps consumers live their lives in an easier way, but also assists hackers to come up with new ways to conduct criminal acts. As a result, victims do not know that their private information or things have been taken until the incident occurred. Therefore, to minimize the threat of hacking, computer software should be created to protect victims from thieves seeking their electronic belongings. This computer software called The Hacker Attacker should be able to do three important things: alert, protect, and report.

First, the Hacker Attacker should be easily accessible via download or commercial stores. There are many virus protection programs that help users to prevent their computers from harm of Trojan horses and worms, but there is no such program easily accessible to people that alert the user when they are being hacked. Furthermore, the Hacker Attacker should be considerably low cost in order for major parts of the computer user population to buy. Since many hackers will be affected by this software, they will try to buy it themselves and try to find ways to bypass the software or manipulate it for their own purposes. As a result, there should be constant upgrades to this program to keep hacking as low as possible.

The main feature of the Hacker Attacker is to alert the user while being hacked. The software will detect a non-registered user entering a personal or business computer and alert the person or company using that machine. This alert will indicate the user the hacker's location via IP address and the information that the criminal is trying to steal. The alert will also display other valuable information such as the time of the hack and the victim's name. Once the alert happens, the software should set the machine in a protective mode. This mode allows the computer to protect itself from the hacker by conducting a series of protective routines. Depending on the type of hack the software will implement a different protective measure. For example, if a hacker was trying to steal personal information such as social security numbers or passwords to access online banking, the software will conduct a scrambler of the numbers and passwords. Every second, the social security number or password will randomize making the information virtually impossible for the hacker to obtain. Another example would be to conduct a series of barriers or firewalls to prevent a hacker from entering a secured PC.

The last thing that the Hacker Attacker should do is to report the hack and hacker to proper authorities. For instance, while the hack is going on and the software set the computer in a protective state, the alert will check the IP address and send the information to the closest location that handles these types of crimes. Then, the authorities will go to the location that was given and apprehend the criminal. This example can be view as firefighters on call for a house fire. The authorities could separate internet crime unit placed in every city, which will help reduce the time to catch the hacker.

In conclusion, the Hacker Attacker will solve the world problem of hacking. Identities will no longer be stolen, money will no longer be magically transferred to random bank accounts, and computer usage will dramatically increase due to a feeling of safety. Furthermore, the Hacker Attacker not only will protect people from criminals, but it will create jobs. These jobs include the computer engineers to help design and upgrade the Hacker Attacker and also the new crime unit to respond when an incident occurs. Ultimately, the Hacker Attacker will not only help maintain privacy, but also keep the entire electronic world safe.