Tecno-Tips

Cybercrime and Your Computer Health

By Antonio Hernandez

The malicious intrusions in computers and networks have increased dramatically during the past ten years. Although this issue is not new, what is new is the damage that these intrusions could have on the user. During the early days of personal computers, the files on diskettes and the computer's hard drives could easily be infected with "computer viruses" that came in different forms to obstruct the computer's operations. The transmission was connected to the use of a file infected with the virus and, although this contamination upset the regular operation of the computer, it could be easily corrected using antivirus computer programs. Most of the time, these virus intrusions were not critical to the computer's operations and generally did not compromise the integrity and well-being of the user of the computer.

The connectivity of computers to networks, the use of the internet as a browsing tool, and the wide popularity and use of electronic mail as the preferred mechanism for communication opened the field for new and more dangerous types of intrusions. These new types of threats not only put the operation of the computer and the associated network at risk, but it could also compromise the integrity and the financial operations of people and businesses.

The risk of intrusions has increased due to the different types of mobile platforms or devices exchanging information with computers and the wide use of social media portals for exchanging or communicating information, including personal and private information. Remember that anything you upload on any portal or website on the Internet and any electronic message you send can be retrieved or accessed by experts known as "hackers." Not only that, but these things will remain forever in cyberspace.

In the past, Windows-based computers were the object of virus attacks due to their wide use in the business world. Today, virus attacks also affect Apple computers. Linux-based computers have less risk of being targets of intrusions.

To illustrate the risk and the potential damage that intrusions may have on computers, systems, businesses, and individuals, we will present different categories of intrusions based on the intended objective and expected outcome. Some of those intrusions are based on virus infestations, others are based on "social engineering" tactics.

Social engineering, in the context of computers and information security, is the psychological manipulation of people for divulging confidential information such as accounts, usernames and passwords, credit card details or bank account numbers, and personal identification or social security numbers. This fraudulent mechanism of obtaining information can be done through computer communications (mostly emails) or by any other mechanism, such as phone calls.

In computers, one of the most common forms of social engineering is known as "phishing." Phishing is the attempt to obtain sensitive information, often for malicious reasons, by disguising oneself as a trustworthy entity in an electronic communication. Phishing is typically carried out