# VIRUS PREVENTION

# The Tele Comm Method

A computer virus is a computer program that can copy itself and infect a computer. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, adware, and spyware programs that do not have the reproductive ability. Malware includes computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software, including true viruses. That being said, the bottom line is that it is all bad. These unwanted programs can slow down or stop a computer, steal data, and wreak havoc with entire computer operations.

So, how do you "protect" yourself from viruses? At Tele Comm we do not concentrate on "protection", but rather we concentrate on "prevention". It may not be possible to protect from all viruses, because there are new ones constantly being released, and even old ones can morph into new configurations. It is possible, however, to prevent a virus from getting onto your computer. Considering most viruses are invited onto your computer, prevention is all about safe computing. In addition to the obvious rules such as never opening an email from an unknown sender and never going to social or news web sites, here are the five Tele Comm rules for safe computing:

1. **DEPERSONALIZE THE COMPUTER**
   Remove all fuzzy animals, sticky notes, pictures, decorations, and personalized background screens and screen savers. The computer must be viewed as a tool that is used to perform work for the office; work that generates income for the company and ultimately for the employees. This view of the computer will eliminate the temptation of performing personal tasks on the computer, and thus eliminate exposure to personal sites that are more likely to contain harmful information.

2. **ESTABLISH OWNERSHIP**
   The computer belongs to the company, just as any desk or chair belongs to the company. Periodically rotation of computers among users may help to make this point, and further eliminate the possibility of potentially harmful personal information from being stored on the computer.

3. **CONFIGURE ALL COMPUTERS WITH IDENTICAL BACKGROUND AND SCREEN SAVER**
   Establish a "company background" and "company screen saver" and put it on all computers. It may be the company logo or just a plain color, but it should be the same on all computers.

4. **MAINTAIN A LIST OF APPROVED SITES**
   This list of approved sites should be limited to just those sites used to conduct the company's business. It may be updated periodically and should be kept in the browser bookmarks of all computers. The "home" site for the browser should be the same on all computers and must not be a popular site such as "YAHOO", "MSN", "AOL", or any other site that is filled with links. Instead it should be the company's web site or the most commonly used web site.

5. **MAKE ACCESS RULES**
   The rules should state that access to social sites, personal email, or news and information sites is prohibited.

For those offices that want to provide employees with "non-company" Internet access, either an additional inexpensive computer can be purchased and dedicated to employee access, or a wireless hotspot can be established for access by employee owned portable computers, such as notebooks, tablets, netbooks, and smartphones. Any connection for this purpose must be attached to a separate Internet connection that is isolated from the main office Internet connection.