

Computer Viruses: Impact, Prevention, and Recovery

All POS systems have some form of exposure to the Internet. Many systems utilize high-speed connections for credit card transactions and other business critical activity. *Every* system has users who use the Internet at home or at school and might bring files to work. Whether by design or by accident, these activities infect computer systems with viruses every day.

Impact

Computer viruses are now commonplace and increasingly damaging. The following statistics are from an organization that tracks virus outbreaks:

- ∅ There are about 70,000 classified viruses, with about 1,200 new types discovered every month.
- ∅ It is estimated that viruses cost businesses approximately \$55 Billion in damages in 2003. The same calculations were done in 2002 and 2001, at \$25 Billion and \$13 Billion, respectively.
- ∅ The W32/Mydoom virus (2004) succeeded in infecting 1 out of every 12 emails posted worldwide.

Who is at Risk?

The systems at highest risk are those that have internet access attached to their local retail network. Most viruses arrive through email attachments, but they can also arrive by downloading files, browsing the internet or simply using a diskette from home.

Classically, virus 'authors' have wanted the greatest impact possible and, therefore, they have written the virus specifically to impact the most common computers, those that are Microsoft Windows based. More recently though, viruses have targeted Apple, Linux, handheld PDA computers and cell phones.

Prevention

There are three basic forms of prevention: Isolation, Perimeter, and Saturation:

Isolation - The only 100% effective method of virus prevention is isolation. If internet access is absolutely required, then limit it to one computer which is not connected to any other computer or network. Of course this limits the functionality of that one computer; it cannot print to network printers, it cannot access a POS system, make price changes, etc... Antivirus software should be running and kept current on this computer. While extreme, the isolation method offers the highest level of security against viruses. However, it is not suitable for customers who import batches and other data through the Internet.

Perimeter – The perimeter method designates specific computers on the local retail network for internet access, with those machines running antivirus software. In theory, this method is effective because it guards the doorways to a local store network. It also minimizes cost because it reduces the purchase of antivirus software. However, this method does not protect files brought in on floppies and CDs. There is also a risk that a user will modify the settings of their unprotected computer to allow internet access, thus bypassing the perimeter protection. This method is preferred for stores with only a few computers.

Saturation - The saturation method protects all computers on the network by running antivirus software on every computer, whether they have internet access or not. An existing computer acts as the antivirus server, monitoring the other computers and distributing virus updates. This method is preferred for stores with five or more computers (including Windows-based registers).

Best Practices

Using anti-virus software is the most effective method of protection, but it is not 100% effective. In order to enhance software protection, we recommend the following practices:

- Ø Never open email from an unrecognized sender. Delete it immediately.
- Ø Never open an email attachment unless you are expecting it and have high confidence in the sender.
- Ø Invoke and enforce policies on the personal use of store computers.
- Ø Back up data nightly to multiple tapes/drives.
- Ø Watch for unexplained messages and sudden reduced performance even after rebooting. These are the initial danger signs of a virus.
- Ø Antivirus software is licensed and must be renewed periodically, typically yearly. Do not allow your license to lapse.
- Ø Periodically check the results of antivirus scans to verify that the software is working properly.

Recovery

Antivirus software will usually take care of viruses automatically. In some cases, however, an expert may need to work with the software. The longer a virus is on a computer, the more damage there will be. In extreme cases a computer will have to be wiped clean and reloaded. Generally speaking, repair from virus damage is not covered under NCBP service contracts. The keys to a quick recovery are quick detection and good data backup.

Your Next Step

Contact your NCBP representative for a risk assessment and recommended protection.