

Protecting Intellex from Viruses

What is a computer virus?

A computer virus is a program created specifically to invade computers and networks and wreak havoc on them. The mischief caused can be very minor, such as causing a funny image or cryptic message to be displayed on your screen, or it can do some serious damage by altering or destroying files.

What is a worm?

Worms are very similar to viruses in that they are computer programs that replicate functional copies of themselves (usually to other computer systems via network connections) and often, but not always, contain some functionality that will interfere with the normal use of a computer or a program. The difference is that unlike viruses, worms exist as separate entities; they do not attach themselves to other files or programs. It is valid to say that a worm can infect a vulnerable computer without any user action like opening an email or visiting a web site as long as another computer on the network is infected with the worm. Because of their similarity to viruses, worms are often also referred to as viruses. A well-known example of a worm is the MSBlaster worm, which invaded millions of computers.

What is a Trojan Horse?

Named after the wooden horse the Greeks used to infiltrate Troy, a Trojan horse is a program that does something undocumented which the programmer intended, but that the user would not approve of if he or she knew about it. According to some people, a virus is a particular case of a Trojan horse, namely one which is able to spread to other programs (i.e., it turns them into Trojans too). According to others, a virus that does not do any deliberate damage (other than merely replicating) is not a Trojan. Finally, despite the definitions, many people use the term "Trojan" to refer only to a non-replicating malicious program. An example of a Trojan horse is W32.DIDer. This virus has been found on the computers of users who have downloaded the popular file-sharing program Grokster.

What is the most common way a virus attacks?

The most common modes of attack are via email, infected networks, and Web sites. Email can be dangerous when an infected email message is received, an attachment is sent or when an email the attachment can be activated when you execute it is opened or executed. The network can be infected with worms that surface when another infected computer connected to the network transmits infected packets that attack the local network for vulnerable hosts. Web sites you visit can contain "spybots," a small program that installs on your computer and takes it over, using system resources to send information about your computer, Web sites visited, or send data to information banks that can be used for marketing purposes.

Is Intellex vulnerable to virus attack?

Intellex has a very limited vulnerability to attack by computer viruses and worms. Most viruses and worms take advantage of standard data communication applications like email applications and web browsers to attack a computer. Intellex runs a dedicated application and all communications through the network use a proprietary interface to that application. When an Intellex is used for its intended purpose: When used for its intended purpose, there is almost no chance of virus infection. This is due to the fact that although Intellex in reality is very similar to a standard PC, it is not used at all like one.

1. There is no email access, no Web browser, and scarcely any access to the desktop. There is no email access which prevents attack through maliciously formed email or attachments.
2. There is no file sharing. There is no web browser nor is there any access to World Wide Web sites.
3. The user has restricted access to the Windows desktop which prevents installation of other computer programs which could be contaminated or reside on contaminated media.
4. There is no file sharing which prevents access to the file system.
5. The Server and Messenger services are disabled which prevents access to the system via a network connection. Users do not interact with anything but the Intellex interface itself.

Intellex is vulnerable to some types of attacks because of the reliance on the Microsoft Windows operating system. There are worms that can attack vulnerabilities in the operating system through a network connection just by being connected to the network. It is necessary that a computer that already infected by the worm be connected to the same network. The only protection against these attacks is to remove the

vulnerabilities through installation of updates from Microsoft. A listing of security updates that are applicable to Intellex can be found on the American Dynamics World Wide Web site. The only possible way an Intellex can become infected with a virus is if you exit Intellex to the underlying Windows operating system and install software or connect to a network, using the Intellex system as a regular PC. Intellex is not designed to be a regular PC and should not be used as one.

Another potential vulnerability of Intellex is through the use of infected media (floppy disks). This can be avoided by using new or scanned disks whenever an upgrade is installed or image exported.

What about Anti-Virus software?

Anti-virus software programs can be an effective way to protect network connected computers from virus attack but they have limitations when used on Intellex. The only real vulnerability in Intellex that they can protect is the use of infected media. Most other types of attack are best protected by other means.

Advantages of Anti-Virus Software

- Automatically detects attack and identifies known viruses.
- Protects against attack from network, email, and infected media.

Disadvantages of Anti-Virus Software

- The continual background scanning uses system resources (CPU and memory) which can affect Intellex performance.
- Anti-Virus software can only detect viruses that it recognizes. The data file must be continually updated.
- Anti-Virus software does not address the system vulnerabilities that permit attack by worms. It only alerts that a worm is present.

How do I keep Intellex safe from viruses?

The Intellex operating environment has been preconfigured for maximum security against viruses. Server service is disable, for example, and thus the ability to inadvertently copy viruses to Intellex. However, underlying operating system vulnerabilities may be discovered and OS updates may need to be installed. If this is the case, you must exit Intellex and install the OS update, thereby rendering Intellex temporarily vulnerable to viruses. The American Dynamics Web site provides guidance on which security patches and updates apply to Intellex. You also have the option of installing anti-virus software to protect Intellex.

Recommendations

- Do not use the Intellex for email, World Wide Web access, or general computing applications.
- Do not install any software that is not approved for use by American Dynamics.
- Do not change the operating system configuration.
- Do not enable the Server or Messenger services in the operating system.
- Do not share the hard drives on the Intellex across a network.
- Always verify that any media used to update the Intellex software is free from viruses. When downloading software from the American Dynamics Web site and copying to removable media for transfer to the Intellex, always use a PC that is free from viruses.
- Always use a firewall if the network is connected to the Internet. Open only the ports necessary for Network Client access.
- Always control physical access to the Intellex to prevent unauthorized personnel from changing the software or operating system configuration.
- Monitor the American Dynamics web site, www.americandynamics.net, for up-to-date information on virus protection.

How do I get the latest Intellex virus and security information?

Monitor the American Dynamics web site, www.americandynamics.net, for up-to-date information on virus protection.