Mark Crootof
Final Draft
Internet Security: Viruses, Worms, and Adware
1701 Words

BASICS

Overview

$ After deciding to computerize a facility, it is important to consider if the practice wants to communicate with the outside world through the internet.
$ There are many advantages to such communication, and many dangers.
$ Having a website will allow countless potential clients to learn more about a practice. Being able to access other websites for information will help doctors and their businesses, as often much of this data is cutting-edge medical knowledge. The internet also allows for the transferring of information (radiographs, blood results, digital pictures of lesions or videos of behaviors and gaits) to people all over the world. Sites, such as VIN and sites connected to the veterinary universities, provide vast databases to assist with complicated diagnoses.
$ The internet, however, is a very large and dangerous place for the unwary, but a few precautions should allow the average user to have a wonderful time surfing the net without worry.
$ There is no such thing as a completely safe and secure computer or computer site, as almost every major company (including the government) have had their systems hacked. If someone can get past these top-notch security systems, someone will be able to get into one at a veterinary practice.
$ That someone, however, has to know about you and your computer, and there must be a reason they would want to hack your system. These unlikely situations, combined with an average security system, are generally enough to ensure that you will have a safe site.
$ Firewalls, anti-virus programs, and different passwords and levels of access for different staff members are three major precautions that a facility can implement to protect the computer system. It is also helpful to follow accepted good computing practices.

Terms Defined

$ Adware. Program/software that installs itself on a computer without the knowledge of the user. Like spyware, these programs are often a companion to valid software downloaded from the internet. As the name suggests, adware often plays a role in advertising: it collects information about the user, based on which websites he or she frequents, and uses this data to display advertisements that pander to the user's interests.
$ Cookies. Messages given to a web browser by a web server. The main purpose of cookies is to identify users. Websites that use cookies often request information from viewers, which is then packaged in a cookies and sent to the web browser. The browser stores the message and then sends it back to the server whenever the user returns to that website. This information is used to present a user with custom webpages; for example, instead of seeing a generic "Welcome!", the user will see a welcome page with his or her name,

such as “Welcome, Juliana!”

- $ Firewall. A device that limits traffic on a network and controls everything that goes in or out of a computer. This device will reject non-valid programs; however, the firewall does need to be taught what types of programs the user wants to accept, or else it will reject everything.
- $ Hacker. An individual, or group of individuals, who attempt to break into programs or networks that are restricted. Once in a restricted program, the hacker can cause damage to the program or network. This damage takes many forms, ranging from simply changing minor information to installing viruses, worms, or other dangerous software that will travel between computers and cause damages and erasures.
- $ Host. A computer that is connected to a network, such as the internet. Each host has a unique IP address.
- $ Internet. A global network connecting millions of computers. Each internet computer, called a host, is independent. Its operators can choose which internet services to use and which local services to connect to the internet.
- $ IP address. This is a specific number that serves as an identifier for its computer.
- $ Internet Security. A term that is determined by (1) how badly a hacker would want to access your system and (2) what procedures and how much money you are willing to spend to make this process more difficult.
- $ Password. A combination of letters and/or numbers that is unique to the user and controls the accessibility of a computer and/or program and/or network. A password can easily be changed by the user. The more frequently a password is changed, the more secure the network.
- $ Pop-ups. Little windows that will come on a viewer’s screen to provide requested and/or unsolicited information. Often used as advertising gimmicks.
- $ Spam. Information, especially e-mail, that is considered not useful, irritating, inconvenient, worthless, or damaging for the user.
- $ Spam filter. A device that removes many types of spam, keeping them from infiltrating the user’s computer or e-mail inbox..
- $ Spyware. Program/software that covertly gathers information for the user’s internet browsing for the purpose of advertising. Like adware, these programs are often bundled with honest software products that are downloaded from the internet. It transmits user information, such as browsing habits, to its source.
- $ Trojan Horse. A destructive program that pretends to be a benign application. Unlike viruses, these do not replicate themselves.
- $ Virus. A program or piece of code that is loaded onto a computer without the user’s knowledge and runs against his or her wishes. Viruses can, and usually do, replicate themselves; often, they will be programed to send themselves to other sites. To do so, they require information from the host computer. Viruses are manmade, and it is relatively simple to create a virus that will replicate itself. They tend to use up some or all of a computer’s memory, which can slow down or stop the system.
- $ Web browser. A software application used to locate and display web pages.
- $ Worm. A program that replicates itself over a computer network and usually performs malicious actions, such as using up a computer’s resources or shutting the system down. Worms carry their replication information with them: unlike viruses, they do not need data from the host computer.

OPTIONS AND ISSUES

Firewalls

- $ Firewalls act like a guardian at a gate: they check everything that goes in or out of a computer network.
- $ They are often found within the operating system that is supplied with software programs. For example, Microsoft's XP program contains an excellent firewall. Such programs will often require a process called "enabling" before they can become functional.
- $ All firewalls require a certain amount of time and training before they will recognize the difference between the benign and malicious programs.
- $ Most security programs will offer a firewall as part of a package, and it can be added to other components of the chosen program.

Anti-Virus Programs

- $ Anti-virus programs are commercially available to everyone.
- $ The two most common ones for small businesses, such as veterinary facilities, are Norton Anti-Virus and McAfee Anti-Virus. Both offer virus scanning, firewalls, anti-spam programs, and privacy programs. They are both well-regarded programs, and either one should provide an adequate level of security for the novice user.
- $ When one purchases a computer, one of these two programs will often be included in the software package.
- $ Regardless of which program is used, make sure that there will be regular automatic updates available. These should be automatically sent to the computer, and will keep the program knowledgeable on the latest viruses.
- $ An anti-virus program can be set up so it automatically scans all files (and hence all information) on a computer on a regular basis. Scans can also be manually initiated.
- $ Many anti-virus programs can be downloaded for free on the internet, but some will also offer additional software that can be purchased. Examples include privacy and anti-pop-up programs.

Passwords

- $ Never use personal items, such as birthdays, house numbers, telephone numbers, et cetera.
- $ The less a password resembles anything intelligible, the more secure it will be.
- $ The more frequently a password is changed, the more secure the network.

Good Computing Practices

- $ In general, be careful while surfing the internet. If you are unsure of a site, don't enter it.
- $ Before opening new web sites, attempt to ascertain if they are real sites with information you are seeking.

- $ Only open e-mail from people or institutions with which you are familiar or from whom you are expecting communications.
- $ Avoid deals that are too good to be true. They are.
- $ Some of the free or cheaper internet programs will increase the chances of exposure to spyware, adware, and spam.
- $ There are some programs, such as Spybot, available on the internet that will search a computer for spyware and adware, identify any such programs, and delete them.
- $ Unfortunately, even if everything is done correctly, it is still possible to receive unwanted information, but sticking to the guidelines outlined above will minimize the spam on a computer.

CAUTIONS

To understand how a Trojan horse, virus, worm, adware, or spyware could sneak into a system, consider the following scenarios.

- $ Your website receives e-mail regularly, most of which is from clients with whom your staff is familiar. One day, however, you get an e-mail from an unknown: according to the subject line, perhaps it is a would-be client or a drug company that can save your practice thousands of dollars. A staff member opens it. Now, this could be an ordinary, harmless e-mail, or it could contain one of the aforementioned nasties that could serious damage your system. A good anti-virus program would inform you of a danger or remove the virus, but adware and spyware can still sneak by.
- $ When a product, such as a necessary software program, has a licensing agreement, it may contain spyware or adware. It may even mention this in the agreement, but due to the length and legalese, most readers scroll down the webpage and accept all conditions unknowingly. Not only does this allow annoying programs into your system, it does so legally.

MISCELLANEOUS

Recommended Reading

- $ CERT Coordination Center. Home Network Security. 2001. Available at www.cert.org/tech_tips/home_networks.html. Accessed July 11, 2004.
- $ Claymania Creations. Anti-Virus and "Security" Products. 2001. Available at www.claymania.com/anti-virus.html. Accessed June 12, 2004.
- $ Network Associates Technology. McAfee Homepage. 2004. Available at www.mcafee.com. Accessed June 13, 2004. Website for McAfee anti-virus program.
- $ Symantec Homepage. 1995. www.symantecstore.com. Accessed July 11, 2004. Website for Norton anti-virus program.

Author

Mark Crootof DVM
608 Rt 29
Middle Grove, NY 12850