

Journal of

INDUSTRIAL TECHNOLOGY

Volume 15, Number 3 - May 1999 to July 1999

Computer Crimes: How to Avoid Falling Victim

By Dr. John A. Marshall

KEYWORD SEARCH

*Internet
Legal Issues*

Reviewed Article

The Official Electronic Publication of the National Association of Industrial Technology • www.nait.org

© 1999



Dr. John A. Marshall is the Internship Coordinator for the Department of Technology at the University of Southern Maine. His areas of specialization include Power and Energy Processing, Electronic Control Systems, Plant Layout/Material Handling, and Industrial Distribution.

This is the final article in a two article series designed to encourage safe Internet utilization by identifying common computer crimes frequently encountered today. Internet access is becoming an essential requirement in a variety of curriculums. In fact, it is an excellent educational and research tool well suited for many Industrial Technology courses. Dangers do exist, however, for those who access the Internet. Educators need to be aware of these dangers and include precautions in courses that encourage Internet utilization.

This article provides insights and “safety instructions” designed to prevent Internet users from becoming Internet victims. Surfing the Internet is exciting, valuable, and very informative. Taking the time to identify potential dangers should be an integral component in any curriculum.

Introduction

The first article in this series began by identifying five of the most common types of computer crimes experienced today. After the brief overview, the first article explored two common types of computer crimes: fraudulent schemes and computer viruses.

This article picks-up where the first left off and investigates three additional computer crimes frequently encountered by novice Internet users. These remaining three computer crimes involve programs that steal sensitive information, hackers accessing and stealing sensitive databases, and computer hardware theft. All Internet

Computer Crimes: How to Avoid Falling Victim

By Dr. John A. Marshall

users must be aware of the dangerous and fraudulent activities that occur each day on the same Internet that students and professionals use as learning tools.

Programs that Steal Sensitive Information

The Deeyenda Plague. A new type of computer virus is receiving much attention as it spreads across the Internet community. The higher levels of attention results from the nature of this virus and the potential security risks it poses. Instead of a destructive Trojan virus (like most viruses), this virus referred to as Deeyenda, performs a comprehensive search on the computer, looking for valuable information, such as email and login passwords, credit cards, personal information, etc. The Deeyenda virus also has the ability to stay in memory while running a host of applications and operation systems, such as Windows 3.11 and Windows 95. This means that when a login and password are sent to the server, the virus can copy it and send it out to a pre-programmed address. The following message is being spread throughout the Internet, including USENET posting, EMAIL, and other Internet activities.

**FCC WARNING !!!!! - DEEYENDA
PLAGUES INTERNET**

There is a computer virus that is being sent across the Internet. If you receive an email message with the subject line “Deeyenda,” DO NOT read the message, DELETE it immediately! Some miscreant is sending email under the title “Deeyenda” nationwide. If you get anything like this, DON’T DOWNLOAD THE FILE! It has a virus that rewrites your hard drive, and can steal sensitive information.

Another reason for the warning is that the Deeyenda virus is virtually undetectable. Once attacked a com-

puter will be unsecured. Although it can attack any operating system, this virus is more likely to attack those users viewing Java enhanced Web Pages (Netscape 2.0+ and Microsoft Internet Explorer 3.0+ that are running under Windows 95). Researchers at Princeton University have found this “plague” on a number of World Wide Web pages and fear its spread. These researchers suggest the above warning be advertised, “for we must alert the general public of the security risks”.

Don’t Open That File. In addition to the credit card scams, many AOL users also have been sent e-mail recently by con artists trying to get their system passwords. The messages offer such things as a free pornographic picture or a piece of software that will boost a computer’s performance. To get the gift, the user must open a file that is attached to the message. When the file is opened, it starts a program that collects the subscriber’s account name and password, and sends it back to the hacker. This type of “Trojan Horse” program is frequently sent to subscribers who use one of the large Internet service providers.

Computer security experts warn users not to open attached files unless they know the person who sent the message. “People need to be as skeptical in the online world as they are in the off-line world. Just because it’s coming over a computer and it’s got a nice-looking electronic image, that doesn’t mean it’s official” (Medine, in “Online”, 1997).

“This is a serious problem that’s growing exponentially,” said Richard Power, an analyst with the San Francisco-based Computer Security Institute. “Criminals are becoming even more clever at manipulating people in the online world” (Power in “Online”, 1997).

Con artists have long used phones, the mail, and face-to-face pitches to wheedle personal information out of people. E-mail, however, represents a new and potentially easier medium to commit such crimes.

"It's relatively easy for fraud artists to look like legitimate companies," said David Medine, associate director for credit practices at the Federal Trade Commissions, which investigates e-mail fraud. With e-mail, Power said, "You don't have to worry about masking your voice or putting on a disguise" ("Online", August 31, 1997).

Man-in-the-Middle Attack. The "Man-in-the-Middle Attack," known as a spoof, occurs when a user visits a booby-trapped web page. Once visited, this site can travel with the user as they access other legitimate sites. Prevention is simple. Be sure to directly access any location where sensitive information may be transmitted. Three steps to insure this are:

Step 1: Carefully type the URL into the open location field of the browser.

Step 2: Add a bookmark to the site as soon as the browser arrives there.

Step 3: In the future, only use the bookmark to access that site.

Periodically review entries in the bookmark file to be sure they do not refer to intermediate web sites. An example of an intermediate web site is as follows:

This is a normal URL: <http://www.acme.com>

This is a questionable URL: <http://www.xyz.com/www.acme.com>
In the questionable address, notice how the URL ends at the same place (acme.com) but travels through a third server (xyz.com) to arrive there. Bookmarks like this should be deleted (<http://www.schwab.com/SchwabNOW/SNNav/security.html>).

Browsers Allow Hackers and Marketers Access to Your Computer.

Chris Sprague, a college student, was surfing the Internet recently when a hostile computer program jumped off a Web site, and attacked his computer.

The rogue program took control of his PC, and shut it down. A similar program could have done far worse - it could have damaged his computer permanently, stolen personal information or commanded his computer to make long-distance phone calls (Blom, 1997).

The software that Sprague and almost everybody else uses to surf the Web - known as a "browser" - is becoming a door that swings two ways. Browsers take Web surfers to the on-line world. Potentially, they also bring hackers and corporate marketers into personal computers (Blom, 1997).

"Most people go out and surf the Web and they think nothing is coming back at them unless they ask for it. That's not correct. Most of the attacks on the Internet come through your browser" (Leavy, 1997). Browsers regularly hand out information about individuals to online sites. Browsers quietly compile information on the users surfing habits, and it files data on the computer. Basically, all stored information could be compromised.

And, in a few still-rare cases, Web browsers allow hostile programs to jump uninvited onto the computer's hard disk. Once there, the programs can peek into the files or command the computer to perform actions such as shutting off, sending electronic mail to a location of its choosing or dialing the phone (Blom, 1997).

Web browsers, such as Internet Explorer and Netscape Navigator, have always given out a certain amount of information about a users on-line activities. Web site operators know what time the user visits their page, the computer operating system, the Internet service provider, where the surfer came from, and where they went next. In some cases, these browsers may even supply the users e-mail address. An e-mail address, coupled with other common databases, gives them home phone numbers and mailing addresses.

In the past, Web surfers had to consciously download programs and then order them to run. People could weigh the value of each program, the reliability of the Web site they were visiting, and the risk it posed of introducing a virus to their computer.

Now, however, the programs hit their computer running (Blom, 1997).

Cookies. "Cookies" are small information files that site operators add to the user's browser and, in some cases, to the hard drive of users computer. These files contain information about the type of pages that have been viewed on a company's site, Internet spending habits, and any password used to access the site. This information makes it easier to log into some sites that are visited frequently, and to navigate around Web pages. Cookies also provide marketers with information that they use in trying to promote their products.

When visiting a web site, the site operator's computer will locate these cookies and use the information to tailor the experience. For example, the site operator might show products of potential interest by flashing them on the screen. Or it may allow access to the site without asking for a specific e-mail address or password again. Users can be warned about cookies heading toward their computer by changing some preferences in both Netscape Navigator and Internet Explorer. In the latest versions of Navigator, go to network preferences, protocols, and check the box for warning about cookies. In the new Explorer, go to view, options, advanced, and check off the warn-before-cookies question.

"Browser manufacturers are working hard to make their products more secure," said Mulligan, at the Center for Democracy and Technology. The problem is that hackers and marketers also are working on new techniques. The user also can empty out the cookies file by safely deleting it anytime they want. It grows back with each new cookie the computer accepts (Blom, 1997).

Hackers Accessing Sensitive Data Bases Credit Data on 100,000 Peopled

Cracked. Federal agents reported that by using the online name "Smak," a hacker was able to infiltrate an Internet service provider and glean credit and personal information on more than

100,000 customers (Zamora, 1997). According to an FBI spokesman, the hacker broke into the operating system of a San Diego company that provides links to the Internet, and then used a device that snoops for customer information. Undercover agents arrested the hacker after arranging a meeting at San Francisco International Airport to pay \$260,000 for 100,000 credit card numbers with credit limits that ranged up to \$25,000 each (Zamora, 1997).

Password Theft is Child's Play. A 15-year-old boy's name is the latest addition to the U.S. Secret Service's list of computer hackers. Police say the boy was irate that his Internet service provider recently raised its prices. He got even by stealing names and passwords from other customers and using them to log onto the system free of charge (Blom, 1997). The boy was enjoying his free access when other customers began noticing unusually high charges on their bills. Charged with aggravated invasion of

computer privacy, the case will be handled in juvenile court. A greater number of hackers are young computer-trained teenagers who don't understand the consequences of using their knowledge for illegal purposes (Blom, 1997).

Conclusions

The five types of computer crimes presented in this series represent the types of challenges that face an information society dependent on computers. The cost and inconveniences caused by these crimes is huge and escalating each day. Criminal delinquents and ruthless con artists have developed acute computer skills, and are using them in a very creative manner. The Internet is their new frontier.

All Internet users should be aware of these types of events and techniques. Educators who encourage Internet use among students may wish to include these precautions in their discussions. The insights and "safety instructions" discussed here have been designed to

prevent Internet users from becoming Internet victims. Surfing the Internet is exciting, valuable, and very informative. Taking the time to identify potential dangers should be an integral component in all curriculums.

References

- Blom, E.(1997, March 17). Beware: Web Surf Has Risky Undertow, Portland Press Herald, pp. 1A, 8A. Information on Internet Security, Downloaded on 1/19/97 <http://www.schwab.com/SchwabNOW/SNNav/security.html>
- Leavy, P., in Blom, E.(1997, March 17). Beware: Web Surf Has Risky Undertow, Portland Press Herald, p. 1A.
- Online, as in Life, Cyberscams Netting the Unwary.(1997, August 31). Maine Sunday Telegram, p.11A.
- Zamora, J.H. (1997, May 24). Hacker Got Credit Data on More Than 100,000 people, FBI Says, Portland Press Herald, p. 6D.