Journal of
INDUSTRIAL
TECHNOLOGY

Volume 15, Number 2 - February 1999 to April 1999

Internet Crimes Encountered By Novice Surfers

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

Internet Crimes Encountered By Novice Surfers

By Dr. John A. Marshall

John 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. He was recently awarded equipment grants from Siemens Energy & Automation and SMC Pneumatics totaling $135,000.00.

Purpose

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

This discussion will begin by identifying five of the most common types of computer crimes experienced today. After the brief overview, this first of two articles will explore the two crimes most frequently encountered by novice Internet users: fraudulent schemes and computer viruses. The second article will investigate the remaining three computer crimes which are programs that steal sensitive information, hackers accessing and stealing confidential databases, and computer hardware theft. It's unfortunate, but the reality of the situation is that mean and fraudulent individuals inhabit the same Internet that students and professionals use as learning tools.

Overview of Five Common Types of Computer Crimes

Fraudulent Schemes. The most popular Internet rip-offs today are fraudulent schemes, or scams, that have been developed to fleece even experienced surfers. For the criminal element, Internet fraud is an opportunity to make a lot of money. Con-artists are showing a great deal of computer savvy and creativity as they hit the surf running.

There is a sense of credibility when a user sees something on the Internet because we have begun to trust the technology and benefit from it. Couple this with an ever-increasing number of naive surfers, and we arrive at a multimillion-dollar national problem.

What we must remember is that the Internet is a crowded marketplace and we need to be just as careful there as we would be in the world's biggest city.

Computer Viruses. A second plague that is terrorizing Internet users are viruses. These viruses can arrive as interesting email messages but when opened, attack and destroy computer programs and files. Every time users surf the Internet, share a floppy disk, or open an email, they risk a virus infection. Three to six new viruses are being discovered every day. Sooner or later, all computers will be exposed to these infections.

Programs That Steal. A third "crime" becoming popular involves computer programs that are automatically downloaded to the hard drive while visiting web sites. These programs, referred to as "cookies", can send "sensitive" information back to web sites that have been visited without the user's knowledge or consent.

Hacker Crimes. The fourth type of "computer crime" involves hackers

Table 1. Computer Crimes

1. **Fraudulent Schemes on the Internet**
   - Email Message Encourages You to Make a Toll Telephone Call
   - FAX and Voice Mail Encouraging Toll Call
   - Web Site Changes Your Internet Provider Resulting in Toll Charges
   - Web Pages that Trick Users into Revealing Sensitive Information
   - False Name/False Internet Address and Product Misrepresentation
   - Top Five Computer Scams
2. **Viruses that Damage and Destroy**
   - The Internet Worm
   - Join the Crew
   - We Will Cyber Bury You
3. **Programs that Steal Sensitive Information**
   - The Deeyenda Plague
   - Don't Open That File
   - Man-in-the-Middle Attack
   - Browsers Allow Hackers and Marketers Access to Your Computer
   - Cookies
4. **Hackers Accessing Confidential Data Bases**
   - Credit Data on 100,000 People Cracked
   - Password Theft is Child's Play
   - The United States Pentagon Defense Computers
5. **Computer Hardware Theft**
   - Masked Men Armed with Guns

breaking into databases and stealing confidential information such as credit card numbers and passwords. Even the United States Pentagon has become the victim of hacker attacks. They average 250,000 attempted attacks per year with more than 60 % penetrating their systems ("Heavy-duty Hackers", 1988).

Hardware Theft. We end our discussion with a fifth, and growing concern, related to the increase in violent crimes involving the theft of computer hardware and software.

Table 1 highlights the five most common types of computer crimes encountered by novice surfers. We will begin our discussion by looking at Fraudulent Internet Schemes.

Fraudulent Schemes on the Net

Email Message Encourages You to Make a Toll Telephone Call. In this internet-based scam, which is growing in popularity, users receive an E-mail that strongly requests a telephone call to a specific phone number. Typically subject lines include "ALERT" or "Unpaid Account," often with a messages similar to the example below. *"I am writing to give you a final 24 hours to settle your outstanding account. If I have not received the settlement in full, I will commence legal proceedings without further delay. If you would like to discuss this matter to avoid court action, call Tom Murray at Global Communications on 1-809-496-2700."*

A few minute telephone call to their number frequently results in a two hundred-dollar long distance charge on your phone bill. Similar messages are also arriving on FAX machines and being left on voice mail. The area codes below have frequently been used for this purpose.

242	Bahamas
473	Grenada
345	Cayman Islands
246	Barbados
664	Montserrat
284	British Virgin Islands
264	Anguilla
876	Grenada
784	St. Vincent/Grenadines
767	Dominica
758	St. Lucia
268	Antigua & Barbuda
441	Bermuda
787	Puerto Rico
868	Trinidad & Tobago

In a recent university example, a professor was urged to call a long-distance number to clarify information included in an upcoming "Who's Who in Science" publication.
The price of this professor's ignorance would have been twenty-five dollars per minute, the fee charged by a Caribbean telephone company for calls to its 809 exchange. Con artists are employing all possible techniques to get people to call the 809 exchange and to keep them on the line. The scammers get a cut of the phone charges, which run as high as $1,000 per call.

Wayne Persons, a computer programmer for the University of Maine System, received an e-mail message from the scammers last month. A company calling itself Global Communications threatened in the message to sue him unless he called their office immediately. The phone number given was in the 809 exchange, which Persons did not recognize but which actually works similarly to an American 1-900 number. As a result of a warning message Persons received from a friend, the call was never made. Other targets of the scam nationally have been paged with an 809 telephone number or faxed a letter demanding that they call a number beginning with that exchange.

If someone makes the call, an automated system on the other end of the line tries to keep them on the phone as long as possible to run up the bill. It either gives the person a long-winded recorded message or leads him or her through a maze-like voice mail system (Blom, 1996).

It is important to prevent becoming a victim of this type of scam, since trying to fight the charges afterwards can become a real nightmare. Legally, a toll call was actually made. Complaints to both the local phone company and the long distance carrier will result in being told that they are simply providing the billing for the foreign company. The victim will end up dealing with a foreign company which argues that they have done nothing wrong.

Web Site Changes Your Internet Provider, Resulting in Toll Charges. A third form of this scam lures customers with the promise of erotic photographs and ends-up costing them thousands of dollars in overseas phone charges.

Internet visitors to three sites on the World Wide Web were told they could access erotic photographs by downloading a free software program. Unknown to the customers, the program cut them off from local Internet providers and reconnected them to a number assigned to Moldavia, an eastern European country that borders Romania.

The calls then were routed to a Canadian site that charged the much higher Moldavia phone rates while the photos were transferred to the user's computer. Phone charges, up to $3 a minute, continued to mount until the computer was turned off ("Internet Scheme Shut Down",1997).

Web Pages that Trick Users into Revealing Sensitive Information. The electronic mail message recently sent to America Online subscribers looked official enough. Titled "Important AOL Information" and bearing the signature of the company's Member Services department, the message provided an update of the online computer service's efforts to fix its busy-signal problem.

At the end of the note, subscribers were asked to jump to a World Wide Web page - which featured a letter from AOL Chairman Steve Case - where they were asked to enter their name and address as well as their home phone and credit card numbers to update AOL's new computers. The unsuspecting subscribers were actually providing a cyberthief with new credit card account numbers.

This scam is the latest in a series of increasingly bold and sophisticated online ploys to wrest personal information from AOL subscribers and Internet users in general. Although law enforce-

ment officials say they have no way to tally the cost of such crimes, industry specialists estimate it is costing consumers millions of dollars a year.

AOL subscribers have been barraged with several messages in recent months that aim to swipe their credit card numbers. Among the tactics have been offers for free time on the service and a request to re-enter billing information to confirm a new payment plan, company officials said.

AOL isn't alone. Such scams recently have been tried on subscribers to other online services and on people who have direct connections to the Internet. AOL has been especially attractive to those seeking to commit fraud because of its size - it has more than 8.5 million subscribers - and the fact that many of its customers are online neophytes. By virtue of the fact that AOL is the largest online service, it provides the largest pool of potential victims.

AOL officials say they investigate reports of credit card fraud and report incidents to law enforcement agencies. But the company concedes it can do little to squelch the scams other than alerting subscribers not to part with personal financial information online.

The come-ons, however, can be remarkably smooth. A message sent to AOL subscribers sounded much like AOL's recent television spots and official correspondence with customers. "As you know, the number one priority for all of us at America Online continues to be meeting our obligation to provide you with the best possible service ("Online," 1997). The note went on to mention "the development of a new server which offers a higher system capacity."

The note than asked the reader to click on a highlighted section of text to "read in depth about the steps we have taken" and to "complete the required update of your information on our new servers." Clicking on the text sent users to a Web site outside the AOL service, where they were asked to type in their personal information ("Online," 1997).

False Name or Address and Product Misrepresentation. Concern about junk e-mail has mounted as more and more businesses try to make money off the Internet. Sending mass volumes of e-mail is vastly cheaper than traditional mass mailings. A mailing list of Web users can cost as little as eleven dollars per million names. Many companies have begun advertising and promoting their products via low cost e-mailings. This has led to network bottlenecks that have slowed the flow of information across the Internet.

FTC officials plan to focus on two types of scams: businesses that use a bogus name or Internet address, leaving consumers with no way of stopping the junk mail because their messages bounce back from the false addresses, and junk mailers who lie to consumers in an effort to lure them into investment, business opportunity or to other scams ("FTC Goes After E-Mail Fraud", 1997).

Sometimes, scammers offer to sell computer-related equipment such as memory chips or sound cards and then either deliver substandard goods or nothing at all. They sell software that is supposed to allow people to work from home but that really has no commercial value. The crooks offer deals that seem too good to be true, and their deals turn out to be just that (Blom, 1996).

Top Five Computer Scams. The following are the top five Internet-related scams identified by the National Consumers League during the past two years:

Pyramid schemes: Con artists promise on their Internet sites to pay big dividends to people who send money to their offices. Dividends are claimed to come from other people who put money into the system. A few early investors in the pyramid see cash, but most lose all their money.

Internet-related services: People don't deliver the Internet services promised and paid for, such as the design of a personal or business Web site or Internet access accounts.

Equipment sales: Crooks don't deliver the computers or related equipment paid for. Usually includes memory chips, mother boards and sound cards. In a variation on this, the criminals provide goods but of substandard quality or power.

Business opportunities: Con artists sell business opportunities or franchises using unreasonable predictions of profitability and other misrepresentations. Buyers are usually unable to make enough money to cover the original investment.

Work-at-home offers: Many have a high-tech link and may require purchasing company software or work processing programs. After making the purchase, any work submitted for reimbursement will not meet the con artists' "standards" (Blom, 1996).

Viruses that Damage and Destroy

Every time a user surfs the Internet, shares a floppy disk, or opens an email, they risk a virus infection. Three to six new viruses are being discovered every day. Sooner or later, all computers will be exposed to these infections.

How can the user protect their system from mutating viruses? Install and keep current an active antivirus program such as Norton or McAfee. Also, always buy legal copies of all software used. Be very cautious about using other individuals disks in your system. It is also suggested that periodic backups be made of the hard drive in the event that the system does become infected.

Viruses can be of the stealth, polymorphic, encrypted, boot sector or the macro type. New macro viruses include the following names: "alien", "atom", "badboy", "birthday", "chaos", "dark", and "dogies" (Norton, 1997). Below, we will discuss three common viruses, the "Internet Worm", "Join the Crew", and "Returned or Unable to Deliver".

The Internet Worm. Coursing through arteries, replicating along the way, edging into new sites to wreak havoc, the virus at first seemed like any other - a harmful toxin, but one that eventually would be defeated by the host's defense mechanisms. This, however, was a new, more powerful poison, and it would capitalize on the system's weaknesses, infecting and re-

infecting as it meandered through the host (McNeeley, 1997).

The "Internet Worm", as the virus came to be known, slithered into thousands of computers connected to our national information infrastructure. Created by Cornell University student Robert T. Morris Jr., it infected more than 6,000 systems, jamming hard drives and erasing valuable information before being cured in November 1988 by engineers at the University of California at Berkeley and at Purdue University in West Lafayette (McNeeley, 1997).

This was the first time the Internet and the malicious aims of "crackers" - computer gurus looking to create havoc at someone else's expense - made the mainstream national news. It wouldn't be the last (McNeeley, 1997).

Join The Crew. A very devastating email virus that is becoming popular is titled "Join The Crew". If opened, this virus attacks the computer's hard drive and erases everything on it. Join the Crew is a relatively new, malicious virus that not many individuals know about. IBM made information on this virus public by Brown (personal communication, January 26, 1998).

"Returned or Unable to Deliver". This virus will attach itself to your computer components and render them useless. Do not open or even look at any mail with this title. Immediately delete any mail items with this topic. America On Line has indicated this is a very dangerous virus and that there is no remedy for it at this time (Brown, personal communication, January 26, 1998).

We Will Cyber Bury You. Russia's military looks like an empty shell. However, behind the scenes, Russia's military leaders are shaping a strategy that one day could pose a threat to the West: focusing its limited resources on R&D for "information Warfare."

Western analysts say that Russia is anteing up and working on viruses and other high-tech wreckers that can attack an adversary's computers. These wreckers have the capacity to destroy computer systems that operate everything from the financial systems to communication networks (including telephones) to utility grids.

Moscow's stepped-up R&D program is a backhanded compliment to America's state-of-the-art military technology that performed so well in the Persian Gulf War against Iraq's Soviet-made weapons (Crock, 1997). "It is only a matter of time" before critical U.S. computer systems face major attack, said Robert Marsh, the head of the President's Commission of Critical Infrastructure Protection (Attacks Inevitable, 1997).

"It is only prudent that we take action to close the door on those opportunities," commented Marsh. The panel is expected to make recommendations on how the government and private sector can make vulnerable systems more secure (Attacks Inevitable, 1997.).

Conclusions

The reality of the situation is that criminally delinquent individuals inhabit the same internet as students and professionals. "The Internet is the new frontier for con artists, the evolution of fraud" (Blom, 1996). Cyber-fraud is a multimillion-dollar problem nationally, with criminals regularly sending out e-mail solicitations for services that consumers pay for, but never receive.

This first article, in a two article series, identified six different types of "computer crimes" which are growing in occurrence. Two of these crimes, fraudulent schemes and computer viruses were thoroughly investigated in this article. The subsequent article will delve into the remaining four computer crimes that are frequently encountered by novice Internet users. The purpose of these articles is to better prepare educators and students to take measures against the common types of computer crimes that are plaguing the Internet today.

References

Attacks on U.S. Computers Inevitable, Official Warns. (1997, June 19). Portland Press Herald. p. 7A.

Blom, E.(1996, November 17). Scams Lurk on Internet Screens. Maine Sunday Telegram, p. 1B.

Blom, E.(1997, March 17). Beware: Web Surf Has Risky Undertow. Portland Press Herald, pp. 1A, 8A.

Crock, S.(1997, April 21). We Will Cyber-Bury You. Business Week, 17, p. 6.

FTC Goes After E-Mail Fraud. (1997, June 31). Portland Press Herald, p. 12B.

Heavy-duty' Hackers Attack pentagon Computers. (1998, February 26). Portland Press Herald. p. 4A.

Internet Scheme Shut Down.(1997, February 20). Portland Press Herald, p. 5A.

Lat, E.C.(1997, May11). Cargo Thefts Latest in Computer Crime. Maine Sunday Telegram, p. 11.

Leavy, P., in Blom, E.(1997, March17). Beware: Web Surf Has Risky Undertow. Portland Press Herald, p. 1A.

McNeeley, T. D. (1997, February). Hackers, Crackers & Trackers. The American Legion, 142, 34-36.

Norton (1997). Anti Virus Program. Symantec Corporation.

Online, as in Life, Cyberscams Netting the Unwary. (1997, August 31). Maine Sunday Telegram, p. 11A.