NASW-NC Newsletter

Published 10 times per year by NASW-NC.

Newsletter Production by
PUBLICATIONS UNLTD ◆ Raleigh

Messages from Cyber-space

Therapy on the Internet

Stephen M. Marson and Sara Brackin, Pembroke State University

THIS IS A THREE PART SERIES THAT ADDRESSES a quickly emerging area of social work practice psychotherapy on the Internet. Our first installment addressed basic Internet cultural and values. In Part II, confidentiality is acknowledged as a key component of normal social work intervention. An important question emerges, "What about confidentiality and the Internet?" In part two, we examine the concept of "confidentiality as a misnomer" and important technical actions that must be addressed to comply with the NASW Code of Ethics. In our third installment, we'll address the question, "What's happening now?" That is, how are current psychotherapist offering services over the Internet, what kinds of services are being offered, and what are the implications for social work private practitioners.

Confidentiality as a Misnomer: Part II

As stated earlier, general principles of ethical behavior relative to confidentiality are applicable to social work practice on the Internet. That is, when one is practicing clinical social work in a mental health center, one is ethically and legally mandated to take "reasonable precautions" to secure confidentiality. When practicing on the Internet one must continue to maintain "reasonable precautions" to secure confidentiality. However, "reasonable precautions" on the Internet are grounded in technological knowledge of the human motivation for "hacking" and of cyberspace security. Thus, confidentiality on the Internet is a misnomer. The issue of reasonable precaution of maintaining confidentiality, is actually an issue of security. Briefly, this means that traditional standards of confidentiality cannot be considered as the sole basis for "reasonable" clinical practice on the Internet.

The prerequisite to understanding Internet security is developing an appreciation for the human motivation to hack. Ask a successful burglar the following question, "Do you have any desire to break into a mental health center and randomly read charts?" The answer to this question is an unequivocal "*No!*" Why? Burglars are purposeful. At the risk of serving prison time, randomly reading mental health charts is an absurd objective.

— continues on page 6

REPRINT:
The North Carolina Social Worker Newsletter.
Volume 21, Issue 6 , June/July, 1996.

Ask a successful hacker the same question, and the answer is a resounding, *"Yes!"* Why? "To test my skills against a sophisticated security system." Most hackers have no desire to read charts or do damage. The prime motivation to test one's skills is well-documented.

The authors of this article ask the same question of themselves. "Do I have a desire to break into a mental health center and randomly read charts?" In an honest but disappointing reply, we discovered that we too had the motivation to hack. The next question is, "Would we do it?" We came to the honest conclusion that the ethical standards we embrace would lead us not to hack a mental health data base. The interest exists, but ethical standards are the key to computer security and confidentiality. Thus, any computerized security system is effective only to the degree of the ethical standards embraced by the primary users.

An individual's mindset is tightly related to the concept of establishing a security system. When establishing a security system, one must think like a hacker and not merely embrace the technological security strategies that have been successfully employed. It is often said that, "for every computer security strategy, there is a corresponding method to override it." Thus, after one has established a security system one must ask the question, "What information must I have in order to break into the system without security clearance?" The reply should be a list. If one is not able to create a list, the security system is woefully inadequate.

Unlike traditional concerns of confidentiality, social work practice on the Internet encompasses at least seven technical protocols. These include but are not limited to: encryption, password selection, security of commercial vendors, logging in and out, special concern for women, and fingering. With the progression of time and technology, basic security methods improve but will never become fail-safe.

Encryption

Hidden from most users is the openness of e-mail transmission. When e-mail is transmitted it often follows a pathway which is routed through several different computers. Each time a transmission is routed in such a manner, the message can be stopped and accessed. The process is similar to mailing a postcard. Any postal employee that services the postcard can read it, copy it and distribute the content without the sender or receiver knowing. However, the probability of such an occurrence is highly unlikely. The effort takes time, skills, and a purpose. Thus, e-mail transmissions are a bit more secure than a postcard — except when the information is sensitive and there is someone who wants it! For example, Oliver North deleted all incriminating e-mail evidence regarding the 1987 Iran-Contra affair. However, by employing a sophisticated utility, the FBI was able to uncover the deleted e-mail that lead to his downfall.

Most transmissions do not require special care. However, it is clear that any transmission exchanged between a client and a therapist must be encrypted. While it is true there are ways to breach security or decrypt messages over the Internet, it is no different from the physical world. As long as the therapist makes reasonable attempts to ensure confidentially they cannot be held liable for computer crimes. Many software packages and services are available that make e-mail messages hard to decode without the proper authority.

Most people think of confidentially as what the therapist knows about the client. In dealing with intervention over the Internet, the social worker should be reminded that theirs is not the only copy of the communications between client and therapist. The actual word for word interaction may be up for scrutiny by the entire interested population if the therapist is sued. This is enough to scare many therapists away from this type of intervention. When dealing with several therapists using one e-mail address there will have to be a way to separate each message and allow only the intended therapist to access their clients messages. It would also be wise to erase (and write over) the file after making a copy and placing it in a more secure location.

Password Selection

The first line of security is the password. Most hackers know that novice users do not understand the concept behind the password. *Passwords are suppose to be secret!* Hackers have computer programs that automatically attempt all the words found in the dictionary. Such a program includes a protocol to use proper names, birth dates, television shows, movies, addresses, auto license numbers, dog names and addresses — forward and backwards!

Basic Rules For Establishing A Password

Do not use a password that can be found in any data base. Memorize a password and do not share it with anyone. Use a mixture of numbers, letters, symbols, and punctuation. Use both upper and lower case letters. Lastly, passwords must be changed frequently. The standard for highly secured information is once a month.

Security of Commercial Vendors

Some commercial vendors [i.e., CompuServe, Prodigy, and America Online] are more secure than vendors that operate a UNIX-based system or UNIX shell [i.e., Netcomm and Well]. Hackers have a difficult time breaking into secured areas in a non-UNIX based system because program architects have built an environment that is menu driven with a limited number of options. However, any loose cannon system operator can bypass the menu. Thus, as stated earlier, an Internet environment can only be as secure as the ethics of the people who have the skill to hack around it.

The reasonable alternative for a secure link to the Internet would be a private and direct access to the Internet. Although it is extremely difficult, individuals with a private SLIP or PPP accounts [direct and private access to the Internet] are not totally secure. A thoughtful hacker can capture transmissions at the point of entering and exiting the port. Key point: The only person that would pursue such a strategy would be one who *knows that important messages are being transmitted and these* messages are worth the time and the effort to capture. Who would make such an effort? A detective who is collecting incriminating evidence for a divorce hearing! Therapists are often subpoenaed in divorce cases. An attorney with access to e-mail transmissions will not admit he has access, but he will know exactly what questions to ask in court. With current technology, neither the therapist nor the client will be able to confirm that security has been breached. However, one way to catch such an invader is to include incriminating disinformation in some of the transmissions. This is the strategy that was successfully employed by Rudy Baylor in John Grisham's novel entitled, *The Rainmaker.*

Logging In and Out

As a security measure, develop the habit of observing the "Last Login" screen. Most computer programs that link to the Internet provide information that identifies the time and date of the last login. Such information can be used to identify if someone else has gained access to confidential information. In addition, monitor your 'last command.' When prompted to do so, most computer programs will identify the last command initiated by the user. These two strategies are not only useful for security of Internet files, but also useful for an office PC. Student workers can have access to a professors computer in which exams are housed. A student can easily hack into a test bank.

Special Concern for Women

Telephone companies warn female subscribers to not list their first name in phone books. The same security measures should be taken on the Internet. Women are often bombarded with random males. Using one's first name as part of a user identification is considered a very bad idea.

Fingering

The FINGER command is commonly found on all UNIX systems. It offers information about the user. Hackers use the FINGER command to determine the frequency and time of logins. The FINGER command can be used to identify the most vulnerable account—the inactive account. Some users are not aware of the FINGER command. Others may be aware, but not know that the information can be changed. Within Internet environments in which much information must be secure, it is wise to control information available via FINGER.

In part III of this series, we'll address the issue of how current psychotherapist are offering services on the Internet. The prime question becomes, "What are the problems and implications for social work private practice?" Part II outlined some technical features that are required to assure a reasonable level of confidentiality that goes beyond our present professional training.