IT: SECUR IT

Don't ask, don't tell *or* Yeah, but . . .

The issue of safeguarding SIGNET-D passwords comes up time and time again, with the Department's Operational and Security groups attempting to raise general awareness as to why this is such an important issue.

There are normally two issues associated with passwords, and most employees are familiar with the first one. This is the concept of safeguarding your, or corporate, data. Your password ensures that only authorized people can have access to your data. The other less well recognized concept, is that your passwords uniquely identify you to the system and, therefore, provide integrity to the system by ensuring that system events can be traced back to you. In other words, if the system says you did something, it's a provable fact because your user ID and password were used. As the Department and the world seems to be moving increasingly towards e-mail as a means of official communication, it's vital that our systems have impeccable integrity.

If I know your password, I can logon as you and send e-mail to anybody in the Department on any tasteless or unpleasant subject I can think of. If I know your password, I can logon as you and read all your e-mail. What if I know your password, and logon as you to send a sensitive document to *Frank* magazine via e-mail? or manage to gain access to the SIGNET-D servers and erase whole chunks of data? I'm sure you get the point.

There is a very simple guideline popularized several years ago by U.S. President Clinton on a military issue that can be applied to the safeguarding of passwords: **Don't ask, don't tell.**

From a **confidentiality, integrity and availability** perspective (the big three computer security concerns), there are very few valid reasons to ever tell anybody your password or to ever ask anybody for theirs. Very few.

❶ Yeah, but my co-worker has told me to give him/her my passwords in case I'm ever absent and he/she needs access to my files and e-mail.

Don't ask, don't tell. Important e-mail dealing with divisional business should be delivered to, or at least cc'd to, your division's organizational e-mail account, not your personal one. That's why these organizational mail accounts were created. Your clients and correspondents should be so advised. Important divisional files should not be stored on your personal H: drive, where only you have access, but perhaps in your division's directory on your I: drive, or in a directory on your local C: drive where they can be accessed by others without compromising your password. That's why I: drives were created, and why you have a local C: drive.

A restriction exists in ICONDESK whereby if more than 255 messages are waiting to be accepted by your e-mail account (because you're on holidays, TD or otherwise away from the office), anybody who sends a subsequent message to you will get a cryptic "MTA Congestion" error returned to them and will have their e-mail bounced back. If you are a "light" e-mail recipient, and can't imagine getting anywhere near 255 messages accumulating in your e-mail account while you're away, you can simply arrange to have your e-mail forwarded to somebody else. See the Corporate Application "Profiling|Profil" or contact your SIGNET-D Systems Administrator for details. [Editor's Note: see also "Summertime Tips," *Connexions* No. 3/96, July 29, 1996, pp. 9-10.]

If you are a "heavy" e-mail recipient, and can envision 255 messages accumulating during your absence, you may want to give consideration to giving your e-mail password to an extremely trusted colleague. Should you take this unusual step, we cannot stress enough the importance of changing your password immediately upon your return. [Editor's Note: This modifies point 2. in the article, "What happens to your messages when you are away?", *Connexions* No. 3/96, July 29, 1996, pg. 5.]

Note that this limitation of 255 messages does not exist with divisional organizational mail accounts, which is why they are the preferred destinations for official e-mail.

Continued on page 6 ▶ ▶ ▶