



January 2008

Unprotected Computer User ID and Password

Your password allows access to many computing and information resources. The password, along with a user identification (user ID), validates your identity as an authorized computer user on a computer system or network. Your validated identity is then used to control your activities within the system or network, areas which are potentially limited to authorized users, or groups of users, based on a need to know.

Case

Diane was authorized by her group leader to take a work laptop so she could work from home. Since Diane eventually started to have difficulty typing on the laptop, she requested and was approved to switch the laptop for a desktop computer for home use. Her organizational computer security representative created an account on the desktop computer for Diane but he failed to check for sensitive information left by the previous owner. Diane returned the laptop and took the desktop computer home. A few weeks later, one of Diane's children asked if she could use the computer for her schoolwork since the family did not own a computer. Diane logged in and allowed him unauthorized and unsupervised access to the internal network. Soon another child was also using the computer for schoolwork. Diane knew she was not supposed to give her user ID and password to anyone, but she gave them to her children so they could log in without bothering her. The children began to use the computer and Diane's work user ID and password at will. They routinely downloaded Internet files and used unauthorized peer-to-peer software.

Security Concern

Diane violated DOE and local policies by giving her children her work user ID and password. Doing so put the entire internal network at risk. Diane's children could easily have downloaded viruses, worms, Trojans, and other malware (malicious software) that could have affected almost every computer system at the site. Additionally, a review of the computer's hard drive revealed a sensitive file that had been left by its former owner. Diane's children could have had unauthorized access to that file or made it vulnerable to unauthorized access by others. A forensic review of the hard drive revealed that the file had not been accessed while the computer was issued to Diane.

Causal Analysis

- Weaknesses in the process for approval and management of use of government property allowed Diane to take home the improperly sanitized computer.
- Diane willfully violated DOE and site policies prohibiting the sharing of user IDs and passwords.

(Note: Proper approval and documentation of the take-home computer were issues in this matter but are beyond the scope of this CSI.)

EVER WONDER WHAT EVENTS
LEAD UP TO A
SECURITY INCIDENT?
CSI CAN UNRAVEL THE
CLUES.

CSI:
CONTEMPLATING
SECURITY
INCIDENTS

EXPLAINING WHAT A
SECURITY INCIDENT IS
AND HOW IT UNFOLDS.

Defense Nuclear Security Lessons Learned Center

Sharing Experiences to
Ensure National Security



Corrective Actions

- Written justification is now required before workers are allowed to take government computers off-site.
- Diane's group reviewed all off-site computer use and conducted a wall-to-wall inventory of all computer equipment.
- Diane's group evaluated and revised the requirements for sanitizing take-home computers.
- The organizational security computer representative was retrained to ensure sensitive information is properly removed or protected on take-home computers.

Infraction

Diane was issued a security infraction for sharing her user ID and password when she knew doing so was a violation of local and DOE policies. Diane offered no excuse or justification for sharing her user ID and password aside from convenience. The security computer representative was not issued an infraction because the lack of clear procedures for preparing a computer for off-site use led him to believe someone else had sanitized the computer.

Lessons Learned

- Obtain management approval and ensure proper documentation before taking government property off-site.
- Your user ID and password are *valuable data* that protect your computer system and other systems at work.

Do Not Share User IDs or Passwords With Anyone!

References

- 1) DOE CIO Guidance: <http://cio.energy.gov/policy-guidance/guidance.htm>