

# Why Have a Lock If You Leave the Door Open?

October 2007



## ON CYBER PATROL



We humans are very resourceful creatures. When faced with a threat we are able to create innovative, effective ways of protecting ourselves. Back at the dawn of time when humans were stalked by prowling predators, they leaned to build a roaring fire at the mouth of the cave to keep the threat at bay. Yet that fire needed to be strategically placed and well maintained to be useful. Let it die out and there was a good chance someone became a midnight snack for a creature with very big teeth. That's why it is always amazing when somebody decides that a proven security device is inconvenient and devises a way, sometime a very resourceful way, of circumventing it.

Then and now security devices and procedures are only effective if used fully and correctly. In today's cyber world, we are still trying to protect the information cave and the resources inside. There are countless security procedures – system passwords, CACs (common access cards) – that keep our information safe from the modern version of roving predators. Yet some people find it too much trouble to have to reenter a password or reinsert a CAC when their computer has timed out.

One inventive fellow actually created a device that moved his mouse when he was away from his desk so that the screen wouldn't lock. It saved him precious seconds when he returned by not having to log back in. Now that took some creative thinking and solid engineering skills. Yet his misapplied resourcefulness opened the door to unauthorized access. The results of this kind of breach can be found on a regular basis on the local news and daily security briefings.

The use of CACs is designed to eliminate many security risks by reducing the need for multiple and ever-changing passwords. Yet they are only effective if used as designed. Left in a computer with a device that prevents the computer from locking is inviting trouble. Whether the computer is in a secure building, a forward base in the desert or in a local coffee shop, we need to keep our data secure. By making it possible for unauthorized and potentially dangerous people to access sensitive data in the name of saving a few seconds of effort puts personal identity, sensitive data and perhaps even the well-being of other Army personnel and their families at risk.

When somebody circumvented security devices designed to protect him or her in prehistoric times, it usually only thinned out the gene pool. Now thwarting these devices for personal convenience creates more risk than simply being mauled by a cave bear. It opens the door to potentially catastrophic data loss and compromise that could put soldiers' lives in danger.

The On Cyber Patrol © cartoon and supporting articles are created and made available by the U.S. Army's Office of Information Assurance and Compliance, NETCOM, CIO/G6. For more information on the OCP program or to submit ideas for upcoming cartons/articles contact [oncyberpatrol@hqda.army.mil](mailto:oncyberpatrol@hqda.army.mil).