Password Changes? We Don't Need No Stinking Password Changes

Reflecting back on the just completed effort to change all university passwords (most for the first time ever); I remember four issues being raised consistently regarding this effort.

The most common issue heard was why we are changing passwords in the first place. The answer is twofold. First the office of the auditor general for the state of Illinois has been on the University even before my arrival to institute password changes across all University systems. I suspect that this was as a result of the 2006 security breach in which over 200,000 then current and former students, faculty and staff records were compromised. Secondly, up until Thursday October 15th we were one if not the only major Illinois University that did not change passwords regularly. That all changed between October 15th and October 28th 2009 as over 16,000 WIU passwords have been changed.

The second issue and the one needing the most attention was that this effort should have been better communicated. Without question this and other University wide efforts both technical and non technical can and must be better communicated. In many ways we should be judged by how well we communicate. I can accept that.

The third most common question or concern I got was how I am going to remember my password without writing myself a note and sticking it on my computer monitor. For this I offer the following three possible solutions.

> Technical approach: The use of a product like **Password Safe** (see passwordsafe.sourceforge.net) to keep track of your many passwords including password changes. Utilities like Password Safe securely keep track of many passwords by protecting them with a single very secure password. Of course it's a big problem if a single very secure password is divulged resulting in the potential disclosure of the keys to your online kingdom.
>
> Technical approach for the rest of us: Back in April of 2008, I wrote a security and privacy newsletter article titled "Hello Help Desk, I Can't Remember My Password" in which I discussed an approach to remembering even strong complex passwords. Go to (www.wiu.edu/security/awareness.php) to view this newsletter and other cyber security awareness items.
>
> Non technical approach: After changing your password every 90-120 days, write yourself a note and keep it in your wallet or purse. Of course be aware that, according to Javelin Strategy and Research, lost or stolen wallets and purses are the number one method used by identity theft thieves to gather identity information.

The final common issue raised as part of the effort was why I need to change passwords on up to three systems depending on my relationship with the University. My quick answer is because of historical reasons (uTech supports Ecom and WIUP while AIMS supports STARS) and lack of funding. However, I do think this question warrants additional debate and I encourage and support

any effort to bring Single Sign On to the University for everything but systems holding sensitive or compliance data.

Now I would be remiss if I did not acknowledge and thank the many dedicated men and women of uTech and AIMS without which efforts like this would still be just pipe dreams from the security ivory tower.

Regards,

Michael Rodriguez
Chief Technology Security Officer
Western Illinois University

"The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something nonrandom like 'Susan.' And if it's random, like 'r7U2*Qnp,' then it's not easy to remember." — Bruce Schneier