Mountain Computers™ Inc. Newsletter - November 19, 2011

The Best Place in Nevada to take your PC & Business for over 5 years and running!

COMPUTER SECURITY – PART I of X

A request came in this last week to write about USER IDs an Password Management. Today, the basic rules of login IDs aka usernames are simplified so a human can remember it. The associated password policies are strong enough to be remembered without some degree of difficulty. The threat that computer hacking programs are used to attempt dictionary attacks is just a basic ploy. The real threat are no passwords on administrative accounts. The secondary real threat is password length and complexity; long enough to not be easily hacked with a dictionary brust force attack method. Social engineering is an option to bypass 4 digit pin authentication but we must remain strong to the premis of "motif". Why does someone want to hack your account? If my name is Joe Black working at ABC company.com, typically an organization will give me a username jblack and email jblack@abc-company.com . The password can be hand created or generated using a password generator. IT freaks will use the latter, and IT admins friendly to users will provide something random enough and generic enough so a normal person can function. The password policies past 15 iterations will be annoying at best and relevevant. If the employee type is staff or management this approach works correctly but the need to be strong at any level is relevant. Low level access penetration is the goal of hackers in order to gain higher level access. Strategic staff and higher levels of engineering and management and security personnel require extremely strong userids and passwords. Enough about high levels of security - those people know the risks of their account protection. Getting back to basics, there are a few computing desktop and server scenarios to consider in basic user ID and password management. 1) Single computer assigned to single user. 2) Single computer assigned to multiple users. 3) Computer lab of computers available to multiple users. 4) There is a server farm with one administrator accessible to one to many servers. 5) There is a data center cage with multiple vendor 1u to 5u systems within and supervised access. The variety of configurations are finite and we can take 30-40 pages to describe the risks and present the solutions; however, let us approach the risks from the beginning level to the intermediate. When a computer stands alone and not on a network, the best security is a physical door with a lock and key. If the office is compromised the next computer needs to be physically locked to the floor / desk or wall to avoid theft. If that is not the goal, the access to the computer hard drive and external storage are the next level of risk. If there is no hard drive nor external storage, then the username and password to the dumb terminal (beehive) or cloud thin clients the next level of threat. So, is the username and password taped inside a drawer, under the keyboard, inside a notepad or journal sitting on the desk? Please make sure that is not the case. -- Next week - More about this.

Ps. Do you want to know the masssive secret of password security that even the security experts don't know?

BUILD TO ORDER PC - PART VI

This Saturday, let's re-review motherboards. I love to look at motherboards and I love to look at what they can do for me and my company, and in doing so my customers. If I don't like it, my customers won't like it. Simple truth. The real benefit of a motherboard is the functionality, expandability, guarantee of performance, and warranty behind it to make sure the cost associated warrants the protection guaranteed. Gigabyte more than 5 years ago offered lifetime motherboard warranties akin to Intel/AMD processor and Crucial Memory lifetime warranties. Those G-boards worked forever for me and Crucial never failed me. Dozens of those G-boards we used in past builds and passed on to customers without incident. Those are great odds! Now my latest endeavor is the P5G41 board as a mainstay; an affordable LGA775 chipset. My next step is a core i-series board that I can offer that has longevity to 2014.

Mountain Computers Inc.
490 E 8th St.
Reno, Nevada 89512
Office (775) 287-9552
Technical Support (775) 324-3524
Office Hours: Mon-Fri: 8am-5pm
Lunch 11x-12x
Saturday 10am to 2pm

GO GREEN
PC-TUNE UP!

Newsletter designed using Scribus - Open Source and Free