[princi_elem] Student passwords

From : Peter Tromba <tromba@4j.lane.edu>	Tue, Aug 28, 2012 04:33 PM

Sender : princi elem-bounces <princi_elem-bounces@4j.lane.edu>

Subject : [princi_elem] Student passwords

To : princi elem <princi_elem@4j.lane.edu>, princi midd <princi_midd@4j.lane.edu>, princi high <princi_high@4j.lane.edu>

Cc : Brad New <new_b@4j.lane.edu>, Laurie Moses <moses@4j.lane.edu>

Hello Principals,

I am writing this note to you to provide background and request feedback regarding student passwords for email and the internet. My goal is to roll out this plan for the beginning of the school year and I need your conceptual understanding of the issues and support for the letter and the spirit of this proposal before I go beyond your group and engage the attention of office staff, the TSS's, teachers, etc.

The first thing to understand about this issue is how seemingly simple yet stupefying complex it is. Our work in network services, which has included a ton of research and thought into "identity management", shows us that there are no easy answers and that this topic bedevils school districts and universities nationwide.

We have broken the problem down into parts:

1. How do we get the initial passwords out to students.
2. How do we make sure that user passwords are easy to remember and hard to figure out.

To answer Part 1, we can either use an initial password that is something the kid already knows and the school has on file, or we can assign something random and send those randomized passwords in some form to the building. We do not believe that we have the systemic capability to assign random passwords and get them to each student. When we thought about printing them, sending them out in spreadsheets, etc, every solution we came up with looked like a workload problem at the buildings. With regard to using an initial password based on something on file, the only element in the student record that we know for sure and that does not change is the mealtime number.

Therefore, our recommendation is NO CHANGE to initial student passwords.

The key to answering part 2 is to have the users change their passwords to something they can remember and that is harder to figure out than the mealtime number. This is also what we should be training students to do in general.

Therefore, our recommendation is that students be required after a certain number of days to change their initial password. If they do not, the only place they will be able to go on the internet is the password change page. Further we recommend the following rules for passwords for students based on level:

K-2: 4 characters (e.g. 1235 or cat5 or clam)

Grades 3-5: 4x4 characters (e.g. 1234-abcd or fred-9999 or 4567-0001)

Grades 6-12: same as current staff stringency (One capital letter, numbers and letters, etc)

Finally, we will be implementing over time some targeted restrictions for student accounts to critical district resources that should not result in any change for the user experience in the buildings, but that will make our network more secure.

If you support NO CHANGE to the initial assignment of passwords and a MANDATORY CHANGE to initial passwords after 30 days or so, you need do nothing. I will take your silence as support. If you do have issues/questions with this, please let me know as soon as possible.

Thanks,

peter.

P.S. On the topic of password and security, be prepared for another email from me to all staff. While student passwords are a complex problem, weak student passwords are not and have not been a major source of network insecurity. The issue we have in 4J relating to passwords and security is a staff issue to which all of us must attend.

Peter Tromba
Director of Technology
Eugene Public School District 4J
541-790-7777