E-TIP
Educational Technology Integration Pointers

Vol. 24

USER NAMES AND PASSWORDS

As Digital Citizenship Week 2018 comes to a close, it is important to remember that not just students, but everybody needs to make sure their accounts are secure. Much like we lock the house and take the key when we leave, we need to lock our online accounts and make sure that no one else can access them when we are done. This can be accomplished through good user names and strong passwords.

USER NAMES

User names (or screen names) are your online identity. As such, they shouldn't reveal much about your real identity. This is especially true for children – information on the Internet should be limited to only what is absolutely necessary.

When creating a user name, don't use any part of your real name, birthdate, addresses, or phone numbers. This will help prevent people online from identifying who you really are and where you live. Make user names easy to remember, but not related to your personal life. In addition, before choosing a user name, try typing it out in all capital letters to make sure that it doesn't spell anything inappropriate or misleading. Finally, remember that this is representing who you are online, and so you want to make sure it is a good example of what you stand for.

MATH WARNING!
Bonus E-Tip: Math Behind Password Security

If your password uses lower-case and upper-case letters, numbers, and symbols, there are 94 possible characters in a password. This means that, for a one-character password, there are $94^1 = 94$ options for a password. For a two-character password, there are $94^2 = 8{,}836$ potential passwords. If you use eight characters, there are $94^8 = 6{,}095{,}689{,}385{,}410{,}816$ (over six quadrillion) possible passwords.

Find more E-tips at https://goo.gl/qPn7bN.

PASSWORDS

Complex passwords are the best preventative measure for keeping hackers out of your personal accounts. The best way to create a secure password is to make something that is easy to remember but is also unique. Although it is important to use numbers in a password, avoid using phone numbers, addresses, or birthdays – it's best to use a random sequence of numbers that is not identifiable. In addition, the longer a password is and the larger variety of characters used, the harder it is to crack.

Most websites require a password to be at least 8 characters. If this 8 character password is a combination of letters, numbers, and symbols, it would take a computer roughly 9 hours to figure it out, according to howsecureismypassword.net/. The longer a password is, the more secure it is. One tip for creating longer passwords that are still memorable is to switch symbols for letters that look like them. For example, the password **password** (instantly cracked) can be made more secure by using $, 0, @, and P instead of s, o, a, and p to form the password **P@$$w0rd** (9 hours). If you add quotes to the beginning and end (**"P@$$w0rd"**), it becomes even more secure and will take about 53 years to crack.

A final tip on secure passwords is to change them regularly – every six months or so. The newest version of Google Chrome helps you with this, by creating long, secure passwords and saving them, so you don't have to remember them, but they can be changed at any time.

Sources:

Byrne, Richard. "Good Reminders About Password Security." *Free Technology for Teachers*, 7 Oct. 2018, www.freetech4teachers.com/2018/10/good-reminders-about-password-security.html.

"What Are Some Good Rules for Screen Names and Passwords?" *Common Sense Media: Ratings, Reviews, and Advice*, Common Sense Media, www.commonsensemedia.org/privacy-and-internet-safety/what-are-some-good-rules-for-screen-names-and-passwords.