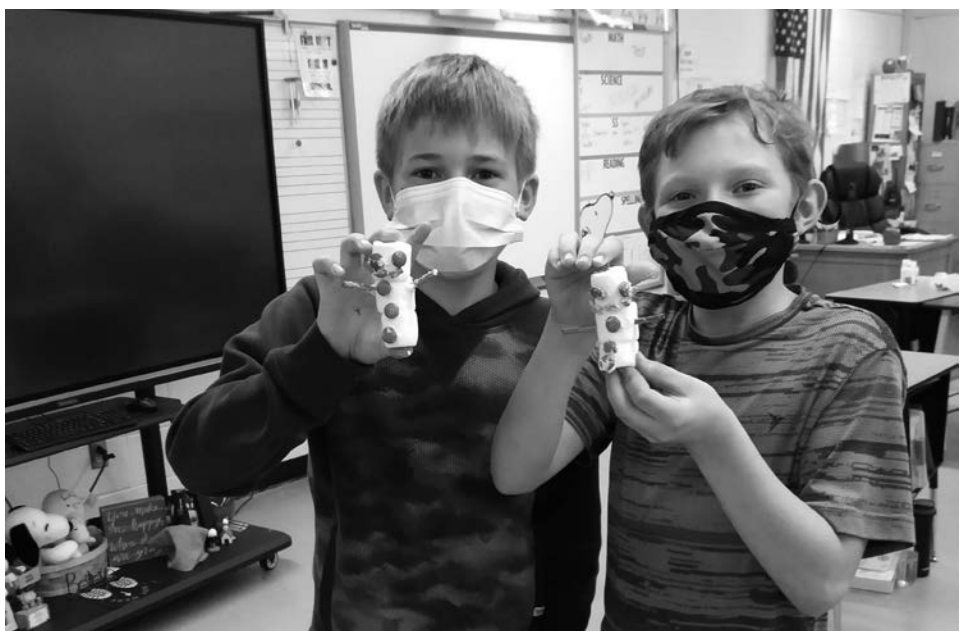
Let's Make a Snow Twin

Brandon Fourth Grade Teacher Sandy Kuik

Celebrating the last day of winter had more meaning this year as the fourth graders at Brandon School got busy building snowmen indoors! Their usual materials of snow, sticks, rocks, and scarves were swapped out for marshmallows, pretzels, M&M's, and fruit roll-ups as they worked with a classmate to make a snow twin. That sounds like a breeze, doesn't it? Well, it wasn't quite that easy. What made this learning activity unique, and quite difficult, was that partners were behind desk dividers and had to rely only on verbal directions during the build to create a snowman that was as close to their partners as possible. No peeking was allowed! This blind build served as a culminating activity for the communication unit of the new Social Emotional Learning curriculum. It gave the fourth graders the opportunity to practice effective strategies used when communicating with others, known as boosters, and to avoid bloopers, the roadblocks that interfere with the ability to work effectively in a cooperative learning activity. Building a snow twin involved a variety of critical thinking skills. Partners had to do a lot of listening, some negotiating, and a great deal of collaborating. Creating these snowmen twinsies definitely challenged the fourth graders to use the communication skills they learned during our SEL time. It also happened to result in quite a tasty treat! The most difficult part of this activity, according to some of the fourth graders, was understanding exactly what their partner wanted them to do. The most fun part, as expected, was eating their creations!

Addison Grade and Mallory Parks work on their communication skills as they try to make their snowman twins.

Alisabeth Perr and Pyper Witthun proudly share their snowman twinsies.



Finnley Frank and Cody Keating show their snow twins right before they enjoy eating them.

Tech Tip of the Month

Submitted by the RBSD Technology Committee

Hackers, Data Privacy, and Protection

Being aware of the possible dangers online is the first step to protecting your information and keeping your computer safe. Updating your computer and browser, being aware of phishing scams, using unique passwords, being leery of attachments, usb drives, and downloads, and finally, installing antivirus software that has been deemed "top ranking" are all ways to protect you and your family while online.

How do hackers target and attack computers? Hackers create and use programs called **Malware**. Malware is a catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, fake security software, and ransomware. Below are the definitions to help distinguish between the different types of Malware:

- Viruses - potentially the most destructive - can do anything from erasing the data on your computer to hijacking your computer to attack other systems, send spam, or host and share illegal content.
- Spyware - collects your personal information and passes it on to interested third parties without your knowledge or consent. Spyware is also known for installing Trojan viruses.
- Adware - displays pop-up advertisements when you are online.
- Fake security software - poses as legitimate software to trick you into opening your system to further infection, providing personal information, or paying for unnecessary or even damaging "clean ups".
- Browser hijacking software - changes your browser settings (such as your homepage and toolbars), displays pop-up ads, creates new desktop shortcuts, and shares personal preferences to third parties.

What can you do? In the past, it was recommended that users install antivirus software on their computers. Unfortunately, some of the antivirus programs have opened a "back door" to those conducting espionage, launching destructive attacks, and hijacking important data or personal information. Don't worry, there are antivirus programs that have been proven to be effective. One such program is Windows Defender. Windows Defender has been ranked as one of the top four performing programs by the independent IT security institute AV-TEST. One of the best things about Windows Defender is that it is free to Windows 10 users, whereas the other programs need a paid subscription. Some of the other top scoring programs include F-Secure Safe 17, Norton Security 22.17, and Kaspersky Internet Security 20, all of which have a subscription that will need to be purchased.

You should drop the "passWORD" and create a "PassPHRASE."
A password is typically composed of not more than 10 letters or symbols, or a combination of both. It could be a string of random symbols such as "B@3!&O$$" or just a word like "sunshine", or a combination of both such as "B3aut1ful!". On the other hand, a **passphrase** is longer than a password, contains unrelated worlds, and does not necessarily need to contain characters or symbols, but can in order to be more universally compliant. An example of a passphrase would be "Shoeplaygroundhoneybee*".

Why are passphrases better than passwords?

1. Passphrases are easier to remember than a random of symbols and letters combined together. It would be easier to remember words from your favorite song or your favorite quotation than to remember a short but complicated password.
2. Passwords are relatively easy to guess or crack by both humans and robots. The online criminals have also leveled up and developed state of the art hacking tools that are designed to crack even the most complicated password.
3. Satisfies complex rules easily. By following the use of punctuation, upper and lower cases in Passphrases, you will also meet the complexity requirements for passwords.
4. Major OS and applications support passphrase. All major OS including Windows, Linux and Mac allow pass-phrases of up to 127 characters long so you can create a longer passphrase for maximum security.
5. Passphrases are next to impossible to crack because most of the highly-efficient password cracking tools break down at around 10 characters. Hence, even the most advanced cracking tool won't be able to guess, brute-force or pre-compute these passphrases.

A passphrase should be at least 16 characters long as well to ensure its maximum security. With this new strategy of using a variety of passphrases in all your important accounts and websites, maintaining anti-virus software, and becoming familiar with ways hackers target victims, you can now enjoy a fully-secured online experience.

Sources:

Humphries, Matthew. "Windows Defender Achieves 'Best Antivirus' Status." PCMAG, PCMag, 6 Aug. 2019, www.pcmag.com/news/windows-defender-achieves-best-antivirus-status.
Natarajan, Ramesh. "Password Vs Passphrase: Here's 5 Reasons to Use Passphrase." Password Dragon – Free, Easy and Secure Password Manager for Windows, Mac and Linux, www.passworddragon.com/password-vs-passphrase#:~:text=So why is passphrase better,a short but complicated password.