HEALTH AND SAFETY

NECSD NEWSLETTER

DECEMBER 2021

IN THIS **ISSUE**

HEALTH AND SAFETY **COMMITTEE UPDATE**

The latest committee meeting included a recommendation to install additional door alarms at our high school campus with the future possibility of additional schools as well.

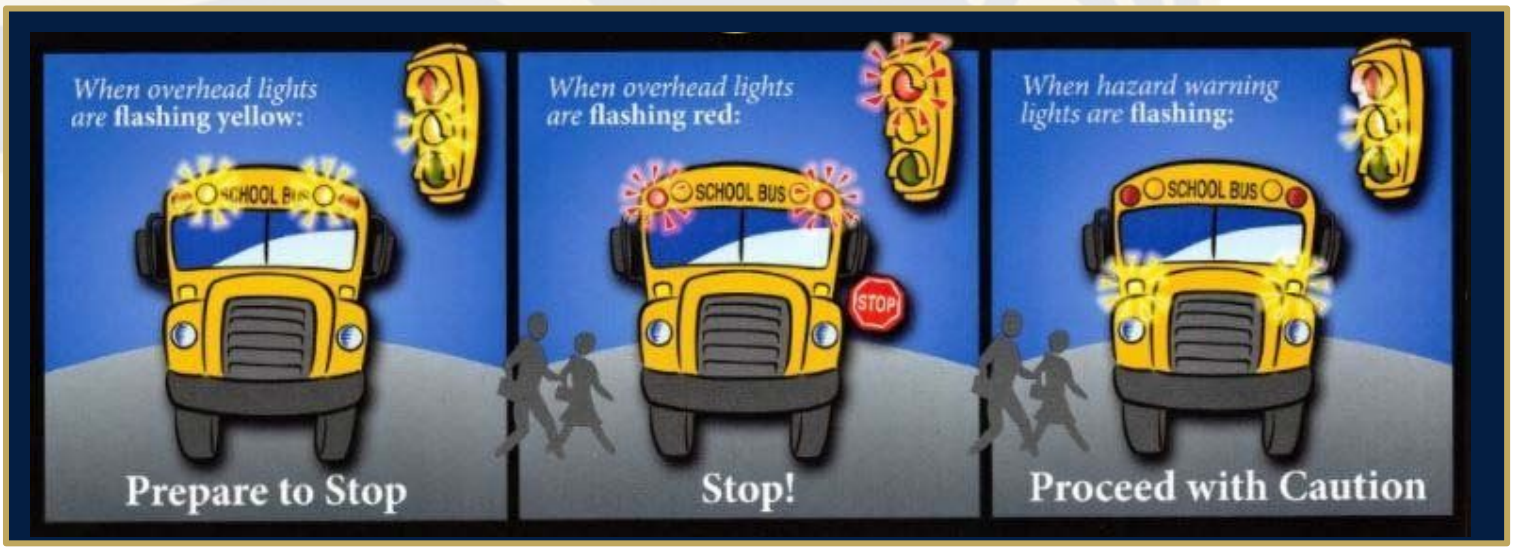
INTRODUCTION

Monthly newsletters are being designed to provide the schools and community with the knowledge and resources necessary to continuously improve the safety of our school environments. Each issue will feature specific topics to inform and guide readers of the district's or schools safety compliance and practices. We recommend that you read this publication to stay abreast of what is happening as well as some resources to connect self, home and school to collectively keep our educational learning environments safe.

INTERAGENCY TASK FORCE

A newly created Interagency School Task Force convened to leverage our community resources to support youth development. Developing a comprehensive plan that identifies effective, evidence-based strategies to address positive youth development requires the involvement of law enforcement, school administrators and staff, and other key community and school stakeholders. We will meet once a month for the remainder of the year once we have developed an action plan to discuss and plan supports for our youth in the area of youth development and violence prevention, intervention, and suppression.

BUS SAFETY REMINDER

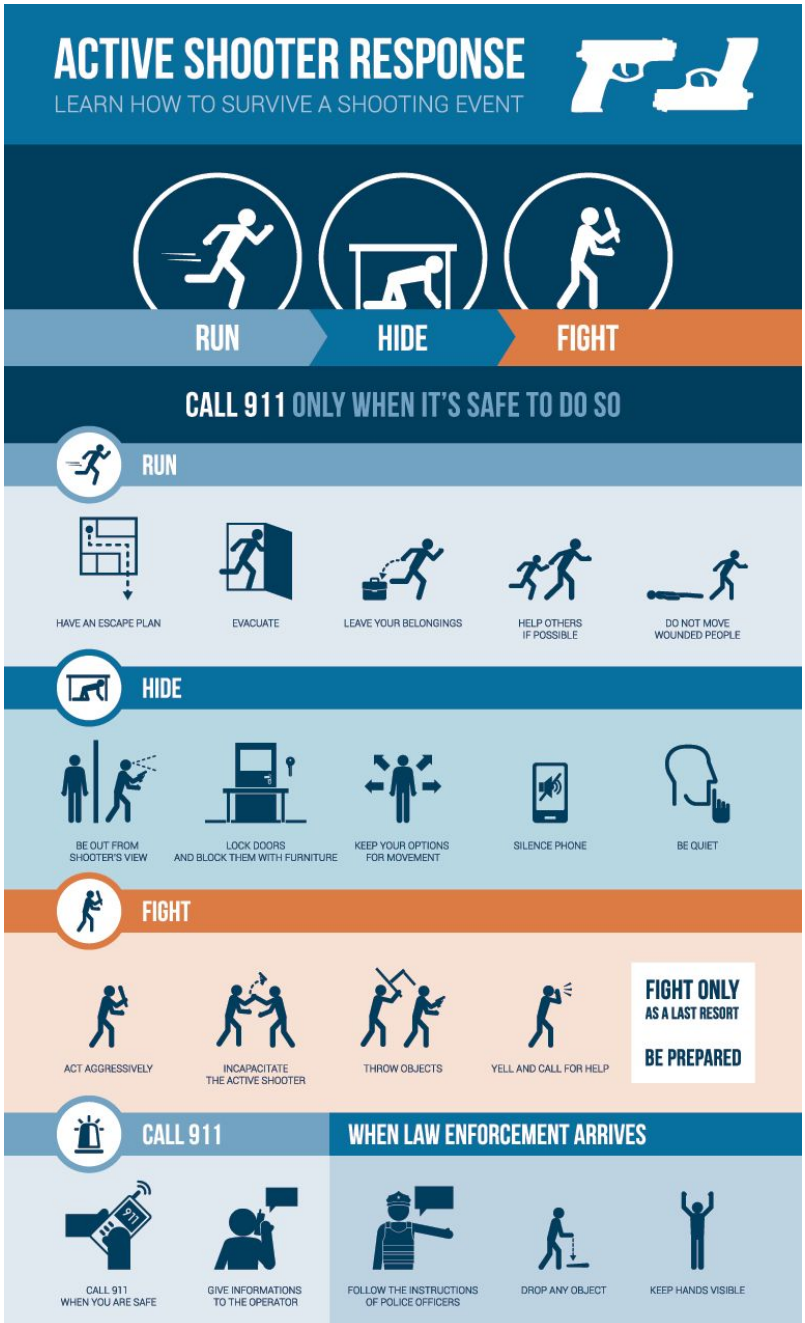


HEALTH AND SAFETY NECSD NEWSLETTER

DECEMBER 2021

ACTIVE SHOOTER SITUATIONS

Be aware of your environment and any possible dangers. Take note of the two nearest exits in any facility you visit. If you are in an office, stay there and secure the door. If you are in a hallway, get into a room and secure the door. As a last resort, attempt to take the active shooter down. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her.



TIP: REPORT SAYS SCHOOL SHOOTERS ARE NOT IMPULSIVE (https://bit.ly/3lOYaTx)

CALL 911
WHEN IT IS SAFE TO DO SO!

9 CRITICAL WARNING SIGNS OF VIOLENCE

Here is our list of nine potential warning signs* that can signal an individual may be in crisis or need help:

1. **Suddenly withdrawing from friends, family and activities (including online or via social media)**
2. **Bullying, especially if targeted towards differences in race, religion, gender or sexual orientation**
3. **Excessive irritability, lack of patience, or becoming angry quickly**
4. **Experiencing chronic loneliness or social isolation**
5. **Expressing persistent thoughts of harming themselves or someone else**
6. **Making direct threats toward a place, another person, or themselves**
7. **Bragging about access to guns or weapons**
8. **Recruiting accomplices or audiences for an attack**
9. **Directly expressing a threat as a plan**

HEALTH AND SAFETY NECSD NEWSLETTER

DECEMBER 2021

CYBER SECURITY

These days, people use countless passwords for many daily activities and tasks. These passwords protect your most sensitive data, whether that is financial data, health data, or just your favorite family vacation photos. Because passwords are so important, criminals are always working to capture, compromise, or otherwise gain access to passwords to get to things that they shouldn't. So how can you create stronger passwords and better safeguarding techniques for all of your important logins?

First, you need to understand how passwords can be hacked, then you'll know how to create stronger passwords. Follow along below as we cover what you need to know about password hacking and crucial password protection tips to keep your important information safe.

HOW CAN PASSWORDS BE COMPROMISED?

There are several ways that passwords can be compromised:

- **Brute Force Attack:** A brute force attack is when an attacker tries a very large list of possible passwords, such as words from a dictionary, to try and guess the right one. This is why using words not found in the dictionary and a combination of letters, numbers and symbols is a good idea.
- **Credential Stuffing:** Credential stuffing is when an attacker takes a large list of usernames and passwords from a data breach and tries them against other services, like banking websites, to determine if those passwords were reused and thus provide access to the account. This is why it's important to not reuse your passwords, especially on important websites like banking, etc.
- **Hash Cracking:** Hash cracking is when attackers gain access to a database of stored passwords that have been hashed, which is a way of obfuscating the password. They then attempt to reverse the obfuscation to get the original password. The longer and more unique the password the harder it is usually to crack. This is why long, unique passwords are important.

GOOD PASSWORD HYGIENE

With so many ways to compromise passwords, it may seem like it is impossible to protect your password and keep it safe. That is definitely not the case! By consistently engaging in a few password security tips and account best practices, you can dramatically reduce the chance that your accounts will be compromised:

- ***Use strong passwords**: Use long passwords or passphrases that are complex and combine uppercase letters, lowercase letters, numbers, and symbols. The best passwords are long (more than 16 characters) and completely random.*
- ***Never reuse passwords**: Use a separate password for each service you use.*
- ***Be careful where you enter your password**: Beware of entering passwords on websites that don't show the lock indicating that traffic is encrypted, opening links that you get via email, and working in untrusted wireless networks.*

Mr. Matthew Tindall
Director of Safety & Security

Email:
mtindall@necsd.net

Phone:
845-563-3429