Greater Southern Tier BOCES

Digital Citizen News - February 2018

The Newsletter of the GST BOCES Digital Citizenship Initiative - Volume I - Issue 6 - February 2018

Digital Security - it is for your protection!

Your knowledge of digital security should focus on four key areas

1. Protecting yourself and your information (data)
   - Use secure password practices, do not give out personal information to people without confirming their credentials
2. Protecting any hardware, software, and networks that you use (at home, at school, on public WiFi, etc.)
   - Use antivirus software. Scan and remove malware. Do not open suspicious emails or files.
3. Protecting your school district computers and network
   - Protect school, library, or business computers and devices with the same good habits that you would use for your own equipment.
4. Protecting your communities (where you live, and work or online communities that you are part of)
   - If you use social media and participate in online communities, be as aware of your own safety and security as you would be in real life. Report suspicious or improper activity.

Some Really Awesome Security Tips

You should use STRONG PASSWORDS for all of your online accounts. Learn how to create and store them.

Where possible use TWO-FACTOR AUTHENTICATION for added security.

Check website addresses to see if they are secured by HTTPS instead of plain HTTP.

Do not open email messages that look suspicious or are from people that you do not personally.

In this issue we explore the topic of:

DIGITAL SECURITY

This newsletter is certified as 100% Authentic by GST RIC Digital Security Team

DIGITAL SECURITY VOCABULARY TIME

PASSWORDS - TWO-FACTOR AUTHENTICATION - ENCRYPTION - HTTPS

WHAT IS A STRONG PASSWORD? A STRONG PASSWORD is one that cannot be easily be guessed by a human, or easily decoded by a computer. You can increase the strength of the password by making it longer, and by using different types of characters (uppercase, lowercase, numbers, and symbols).

WHAT IS TWO-FACTOR AUTHENTICATION? Authentication factors fall into three categories, which include:

1. Knowledge factors - something the user knows, such as a password, PIN or shared secret.
2. Possession factors - something the user has, such as an ID card, security token or a smartphone.
3. Inherence factors, more commonly called biometrics - something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. TWO-FACTOR AUTHENTICATION requires using a combination of these factors to authenticate or to reset a password.

WHAT IS ENCRYPTION? ENCRYPTION is the method by which text or data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key.

WHAT IS HTTPS? HTTPS stands for Secure HyperText Transfer Protocol. All of the information that is sent between your browser and the https:// web site is encrypted using a unique encryption key so that it cannot be decoded by people trying to spy on you.

Check this Out >> **16.2%** of HIGH SCHOOL students reported being ELECTRONICALLY BULLIED within the last year. View the graphic at https://globaldigitalcitizen.org/bullying-cyberbullying-infographic

ENCRYPTION IN ACTION		
The starting text	Encrypt it using a "key"	The result
"This is a test" Try encrypting your own text at **https://encipher.it/**	"0123456789" This is a very simple key (only 7-bits) Some encryption schemes use long keys (imagine a 248-bit key)	"EnCt23018e2ca206fea8a14546d0cb678da80d1e9bc443018e2ca206fea8a14546d0cnYj/oPiBPADTtE4LUVoHF6hWCv2p1FJ9A8zK5ZUtNH6XAiU9IwEmS"

The University of Toronto researches Internet security and human rights.

THECITIZENLAB https://citizenlab.ca/

Helping to Develop the "Filter Between The Ears"

Attorney and child advocate **Parry Aftab** advises that parents work on developing their child's "filter between the ears." Some general guidelines:

Limit kids' leisure time online to under an hour and a half a day, including time spent text-messaging via cell phone.

Talk to kids about the dangers of offline meetings with strangers who have contacted them via the Internet.

Use software to filter inappropriate sites for young teens.

Keep young kids off social networks and dating sites.

Consider giving kids more leeway on the friends they can accept on chat, IM, or as e-mail buddies, but ensure that you know their offline identities. No friends of friends.

Filter or block image searches, which can be a way around many filters.

Block peer-to-peer technologies and teach kids not to download pirated software, movies, or music.

Password theft is a problem at this age, so teach kids to guard passwords.

Try to keep the computer in a central location, and watch kids' behavior with interactive devices such as cell phones and interactive gaming gadgets like Xbox Live. If these devices include parental controls, as Xbox Live does, use the controls. But be aware that even with the controls in place, these games can be risky for young teens because they enable users to chat with strangers.

Source: https://www.cnet.com/news/developing-safe-and-smart-internet-citizens/

DIGITAL SECURITY HELPLINE

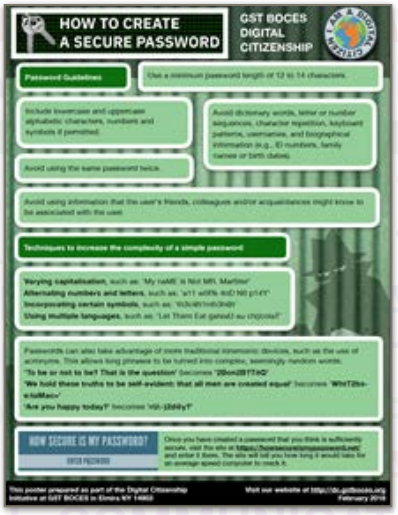
accessnow

If you're at risk, we can help you improve your digital security practices to keep out of harm's way.

If you're already under attack, we provide rapid-response emergency assistance.

https://www.accessnow.org/help/

GET THIS MONTH'S DOWNLOADABLE RESOURCE



This month you can download a printable PDF poster about Creating a Secure Password.

We hope you enjoy it.

http://go.gstboces.org/dc-180201