Digital Citizen News - November 2018

Volume 2 : Issue 03 - November 2018

Greater Southern Tier BOCES

UNDERSTANDING YOUR DIGITAL FOOTPRINT

:: HOW THE INTERNET SEES YOU ::

> "What if, instead of avoiding social media in school altogether or focusing solely on the negative aspects, we teach students how to leverage it to connect in positive ways and build a digital footprint that reflects their best selves ..."
>
> Susan M. Bearden @s_bearden

What is a digital footprint?

Whether you realize it or not, every time you go online you leave behind "footprints", the traces of where you have been and what you have done.

How does this happen?

All computers/devices that connect to the Internet are given a unique address called an IP address. Any messages sent on the Internet have a source address and a destination address. Routers, switches, servers can track, and log or record these addresses.

Browser software is able to save "cookies", small bits of information", to your computer and then read those cookies the next time you connect. Retailers may use them to keep track of purchases that you have made so that they can offer you new products and special deals that are customized just for you.

Google collects data on every search that you make, and on every item that you click on to view. If you have a Google or Gmail account and you are logged in when you do a search, your searches are linked to your profile information which may include your age, your gender, and your location.

On Facebook every item that you view, every link you click on, and anything you may "like" are combined together with your list of friends and friends of friends to create a picture of who you are, and what things you are interested in.

Is this digital footprint a bad thing?

Not necessarily. It may be very convenient that a web site knows your preferences when you need to reorder an item, or that the response to a search is tailored to the information you might want to see most. The only time that the footprint may be a problem is when an item that you wanted to keep private is shared by a third party.

Who owns/controls the info in your footprint?

Most the site privacy agreements grant the site owner the right to record and use the information they collect about you.

Some companies are becoming more sensitive about customer needs, and allow you to control what information they can record and use. Apple Computer recently introduced a portal that lets customers view what data the company has linked to them and to their accounts.

What should I do about my digital footprint?

The first thing that you can do is to be aware of what information companies are collecting about you. Read the user agreements carefully.

Sites like Facebook allow you to link other accounts and programs to your Facebook account. Be aware that when you link these things together that they will be sharing your information as well.

Sign Up to receive this newsletter in your email inbox

Scan this QR code with your phone, or go to http://go.gstboces.org/dcnews-signup in your browser.

More Information about Digital Footprints continues on the next page and on one of this month's free printable posters.

UNDERSTANDING YOUR DIGITAL FOOTPRINT

Some tips for Managing Your Digital Footprint

1. Use Privacy Settings

Most companies are aware of customer's privacy concerns. Read their privacy policies and make use of any settings that they give you to limit the spread of your information.

2. Don't Overshare

The only sure-fire way to avoid digital footprint trouble is for to keep quiet about anything you wouldn't want to be shared with everyone in town. If you don't share it - it can't be used against you.

3. Google Yourself

You may be surprised what you find. It is also good to know what others may find about you.

4. Monitor Linked Accounts

While it may seem more convenient for you to link accounts together, be aware of the information that they may share about you.

5. Use A Secondary Email

When you are setting up accounts or requesting information you may want to use a second email account. This may limit spam and other information sent to your main account.

6. Sending Is Like Publishing – Forever

Every time you send a message, post, or picture, you're publishing it the same way CNN does a news story. And the internet never forgets.

7. Use Digital Tools To Manage Your Footprint

Disconnect (Disconnect.me), DoNotTrackMe (Abine.com) and Ghostery (Ghostery.com) are examples of cross-platform extensions that block tracking cookies and give users control over site scripts.

Some Links on Digital Footprints

Internet Society Tutorial on **What is a Digital Footprint?** http://go.gstric.org/203-footprint1

Virtual Library on **What is a Digital Footprint?** http://go.gstric.org/203-footprint2

TeachThought on **Managing Your Digital Footprint** http://go.gstric.org/203-footprint3

Safe YouTube

Watch & Share Safely

GIVE THIS SITE A TRY!

Youtube can be a great source for videos on all kinds but the advertising and follow up videos can be unpredictable. You are never sure what will pop up, and if you are projecting this in front of a class of children that can be embarrassing!

http://safeyoutube.net has a solution to this - it allows you to enter the URL (address) of a video on Youtube and it creates a short URL where you can watch the video presented in a safe, ad-free view, as well as a few other features like being able to share your shortened URL on social media.

Note: Not all videos work with SafeYoutube (some videos are restricted from linking to other sites), but it works for many of them, and saves you the embarrassment from something inappropriate popping up in front of your students.

http://go.gstric.org/203-safetube

Are there any Benefits from Unplugging?

Unplugging encourages people to actually talk to each other.

Unplugging forces students to look you in the eye.

Unplugging can give students a challenge.

Unplugging helps you connect to different learning styles.

Unplugging encourages students to think outside of the box.

More thoughts about unplugging …
http://go.gstric.org/203-unplug

A NEW DEFINITION FOR YOU

DENIAL OF SERVICE

A **Denial of Service** attack is typically accomplished by flooding the targeted machine or network resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

An example of this would be attacking a network firewall with so many requests for access that it no longer can allow legitimate traffic to pass to or from the Internet.

source: **http://go.gstric.org/203-DOS**

FREE RESOURCE

RANSOMWARE Hostage Rescue Manual

from **KnowBe4**

A company that "enables your employees to make smarter security decisions every day."

The Rescue Manual is a 20-page PDF document that defines ransomware, techniques to avoid ransomware, and how to handle it if your machine becomes infected. The PDF is free but the page does ask you to register to download it.

The KnowBe4 web site also has a section of other free tools you can explore.

http://go.gstric.org/203-ransomware
http://go.gstric.org/203-knowbe4

"If you are on social media, and you are not learning, not laughing, not being inspired or not networking, then you are using it wrong."

Germany Kent, co-author of You are what you Tweet

PHISHING INFORMATION FOLLOW-UP

Last month we reminded you how phishing attempts are still on the rise. Here's some information about a new type of phishing that is spreading quickly. It is called...

Business Email Compromise

Business Email Compromise (BEC) is defined as "an exploit in which the attacker gains access to a corporate **email** account and spoofs (see below) the owner's identity to defraud the **company** or its employees of money."

In this type of attack, the attacker uses phishing techniques to steal an employee's email login and password, and then uses those credentials to send emails to others at the company trying to get those targets send to send money to an online source.

Recently, we heard of two of these attacks happening in NYS school districts.

In one case, the attacker masqueraded as a school principal and sent emails to other email addresses of real employees asking them to purchase Apple iTunes gift cards.

In the other case, the attacker compromised the account of a school business official and sent emails to the school district treasurer asking for a payment of thousands of dollars to an online vendor account.

These attackers are becoming more bold and aggressive in their attacks, and are finding ways to make their attacks seem legitimate. Please be careful with your email credentials, and don't get caught by a phisher.

According to the September issue of the Cyberheist newsletter, "The FBI stated that BEC has caused the loss of over $12 billion between October 2013 and May 2018. The best way to defend against BEC attacks, according to the FBI, is to use face-to-face or voice-to-voice communication."

Source: **http://go.gstric.org/203-cyberheist**

Finally, increasing employee awareness of email security can prevent an attacker from gaining access to the organization in the first place. Sound policies, and employees trained to follow them, can help block BEC before it starts.

Spoofing is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the person who receives it.

For more information:

http://go.gstric.org/203-BEC or

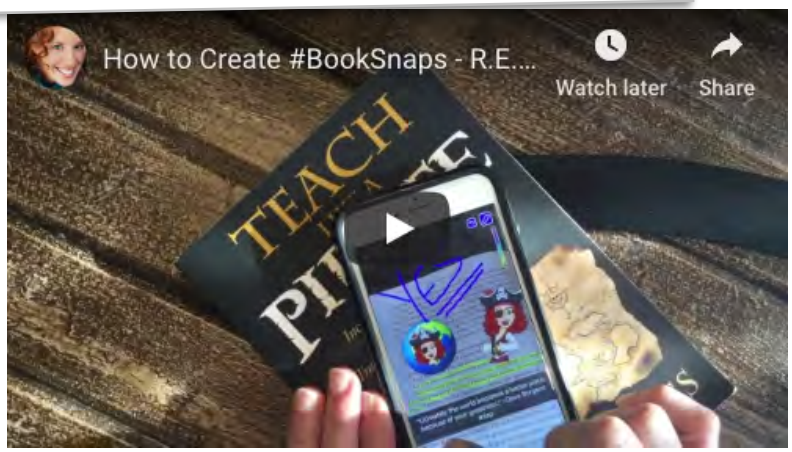
http://go.gstric.org/203-spoof

THIS MONTH WE EXPLORE #BookSnaps

What is a BookSnap?

A **BookSnap** is simply a digital, visual representation used to annotate and share reflections of any excerpt of a book or text.

#**BookSnaps** are now being implemented in nine countries from kindergarten to graduate students.



In this Youtube video, Tara Martin demonstrates how to create #BookSnaps using Dave Burgess' book, Teach like a Pirate

http://go.gstric.org/203-pirate

How do you create a #BookSnap?

1. Take a picture of the text of the passage that you want to share.
2. Annotate the image using any software that have on your computer/device.
3. Your annotations should include the author and title of the book that you are writing about, and then you can add your comments, reflections, and insights about the passage.
4. Post the image you have created and annotated to your social media site(s) to share them with others.

Share your snaps with your friends and classmates and invite them to post their own snaps in response.

Top Reasons to create #BookSnaps

- To annotate and share excerpts of the book you're reading
- To connect an idea or thought by creating a digital visual representation it. The visual representation solidifies the text content within the mind and signals the brain to retrieve the idea from memory.
- To diagram the rise, fall, and climax of the plot
- To highlight figurative language and imagery
- To notate character conflict and internal struggles
- To personally connect to the text
- To point out the main idea or a supporting argument

http://go.gstric.org/203-snapsforlearning

Apps that you can use to create #Booksnaps - more apps and info at http://go.gstric.org/203-snapsapps

SnapChat Seesaw Book Creator FlipGrid

The apps listed here are just examples of ones that can be used for #BookSnaps. It is important that before using third party applications you check their privacy and data policies for compliance with state and federal laws. (CIPA, FERPA, COPPA, NYS 2D. etc.)

We would love to see any examples of #BookSnaps that you create!
Send them with your name, grade level, and school name to dc@gstboces.org

Take Control of Your Digital Footprint

What is my Digital Footprint?

Your digital footprint is the combined total of all of your activity online. It contains every message you have posted, every site you have visited, every "like" that you have clicked, and every item that you have bought. Whether you like it or not, you are being tracked as you participate online, and your information is being used by vendors and sites

Why is it important? Why should I care?

There are two important reasons to care about the information that you leave behind you as you interact online: **Your Privacy** and **Your Future**.

People that you don't know can gather up information about you from your posts and messages. They may know your age, where you live, and what school you attend. This may lead to safety concerns for you and your family. Many families have had their homes robbed because they have posted details of their vacations online.

Recent surveys tell us …

40% of college admissions officers visit the social media pages of applicants.

52% of employers view a future employee's social media presence.

Are there things that you have posted that you wouldn't want others to see?

What can I do about my Digital Footprint?

1. Use privacy controls in apps and browsers.
2. Think before you post texts and images of yourself.
3. Be selective of who you friend and who you allow to link to your content.
4. Treat others online as you would like to be treated.
5. Don't share information that should be kept private. (Don't overshare.)
6. Represent yourself and your ideas in a positive light.

With so many eyes potentially judging you, do you think you need to clean up your digital footprint?

GST BOCES Digital Citizenship Initiative - November 2018
email us at dc@gstboces.org visit our website at http://dc.gstboces.org

So Very ThaNkfuL

for all of the Good Digital Citizens -

- who keep us safe and secure online!
- who help us keep our information private!
- who use the Internet in positive ways and make things better for all!

I AM A DIGITAL CITIZEN

GST BOCES Digital Citizenship Initiative - November 2018
email us at dc@gstboces.org visit our website at http://dc.gstboces.org

USE THIS QR CODE TO SIGN-UP FOR OUR NEWSLETTER