This month we focus on Digital Identity

Last month we focused on DIGITAL SAFETY and SECURITY. This month we will focus on DIGITAL IDENTITY which is related to safety, privacy, and security because part of controlling your online IDENTITY has to do with maintaining the privacy and security of personal information with regards to your digital life.

> ### ⓘ DEFINITION OF DIGITAL FOOTPRINT
> "the information about a particular person that exists on the internet as a result of their online activity"

In previous issues we have written about your DIGITAL FOOTPRINT, which is one of the main things that you need to be aware of as you visit web sites and use online services.

It is an identity that goes with you as you interact with search engines, vendors, social media, and informational sites. Many sites will customize the content that is presented to you as you land on their site.

Each link you click on and every item that you "like" gets added into the pool of data about you that sites can use take advantage of you as you are surfing.

Be aware of the types of data that sites are collecting by looking at their policies, and use any controls that your browser programs may allow like DNT (Do Not Track) settings.

Some sites allow you to view the data that have about you, and some may allow you to delete it.

DEMOCRAT   REPUBLICAN

DO YOU IDENTIFY WITH EITHER OF THESE PARTIES?

Are you aware that there is an election this month? We see signs, and symbols representing politicians all around our neighborhoods, and we can't turn on the TV or go online without seeing video ads, or tweets about political candidates and topics.

DO YOU FEEL THAT THESE MESSAGES ARE BASED ON FACTS OR OPINIONS? DO THEY SEEM TO BE TARGETING YOU? DO YOU FEEL THAT THEY ARE TRYING TO SWAY YOU TO CHANGE YOUR MIND? OR TO CHANGE YOUR VOTE?

When you use social media or browse through web sites…

DO YOU NOTICE ADVERTISING NEAR THE TOPS OF PAGES? OR IN THE MARGINS? DO THE ADS SEEM RELATED TO THINGS THAT YOU HAVE POSTED ABOUT? OR ITEMS THAT YOU HAVE SEARCHED?

As a digital citizen it is important to be aware of your footprint as you use sites and services, it is equally as important to be aware of sites that are trying to influence you with false information and fake claims.

BE AWARE OF SITES THAT DISPLAY INFORMATION THAT IS CLEARLY BIASED, OR IS FAKE NEWS, OR THAT TRIES TO INFLUENCE YOU.

In this time where we have been bombarded by political news and information, have you noticed:
MEDIA THAT HAS BEEN SPECIFICALLY TARGETED AT YOU?
INAPPROPRIATE PRODUCTS OR SERVICES THAT HAVE BEEN OFFERED TO YOU BASED ON SOMETHING YOU CLICKED?
MESSAGES THAT HAVE TRIED TO INFLUENCE OR PRESSURE YOU?

Whoo Are You Online?

Breaking down your Digital Identity
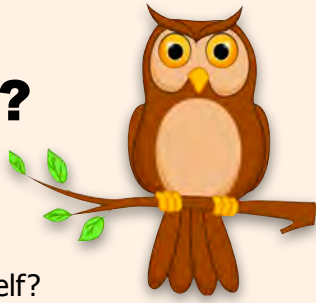
Have you ever Googled yourself?

If you answered NO, then I invite you to give it a try. Find anything you weren't expecting? Anyone who has a public presence online has something called a "digital footprint". Anything you post online (the good, the bad, and the ugly) says something about you as a person. It is up to you to decide what you want your digital identity to be.

If you use any social media (Facebook, Twitter, Instagram, TikTok, Snapchat, etc.) then you have already established a digital footprint. It is up to you to decide what you want your digital identity to look like when posting on your social media.

> It's growing. Your footprint expands as your information is copied and passed on, making it more searchable and viewable to a large invisible audience.
>
> It's not just up to you. When other people - like your friends, companies, or groups you belong to - track, post, or share information about you, it becomes part of your footprint.
>
> It's permanent. Because it's archived in a variety of ways and passed on by others, it doesn't ever go away.

Don't share something about yourself or someone else that you might later regret - you cannot take it back. Remember, something you post now could affect your future so always THINK before you post!

What's in a Signature?

Have you ever gotten an email and wondered 'who is this person'? Adding a signature to your emails helps people know who you are and your role in the school. When you send an email people may not have the information they need to adequately respond to you. For students, this means adding at least your first name and your school. For emails that go to people outside the school you would never want to include your last name or grade to stay safe. For staff that means adding your full name, title, work location, and a phone with extension. This makes it easy for people to contact you and better understand your role at your school.

The good news is that adding a signature is easy. Different programs like Office 365, Google and Outlook usually have a "Mail" tab under Options or File and then a "Signature" section where you can include a signature for both new and reply emails (these can be different). Remember – each separate device needs its own signature as these do not 'travel' across devices.

So go ahead and make your email signature as unique as you are – add a quote, your website, a fancy font – just remember to make it school-friendly. Stuck?!? It didn't work?!? You can always "Ask a Librarian" in your school for help.

LINKS TO DIGITAL FOOTPRINT LESSONS from CommonSense Education

Digital Trails (Grade 2)
What information is OK to have in your digital footprint? http://go.gstric.org/403-trails

The Power of Digital Footprints (Grade 7)
How might our digital footprints shape our future? http://go.gstric.org/403-power

Social Media and Digital Footprints (Grade 8)
How does using social media affect our digital footprints? http://go.gstric.org/403-socialmedia

Who's Looking at Your Digital Footprint? (Grade 11)
How can information you post online affect your future opportunities? http://go.gstric.org/403-whos-looking

Dear Techie Tom

ON IDENTITY THEFT

Dear Techie Tom,

I have heard so much about identity theft on the news lately and I am concerned about the safety of my information. What steps can I take to protect mine and my family's identity online?

-Billie B.

Dear Billie B.,

Identity theft is a real concern now-a-days and would be thieves are getting more creative in trying to get yours and your family's information. You can ensure that your identity stays safe by taking some of the following steps:

1. Use strong, secure passwords and try not to use the same password twice.

2. Be careful with your physical (on paper) information. Shred all documents with personal details that may arrive in the mail or through other means.

3. Never enter information like your social security number, credit card number, or any other identifiable information on sites that you do not trust.

4. Avoid opening emails, clicking on links, or attachments from people you don't know.

5. Check your credit report at no cost once a year at **AnnualCreditReport.com**, which is approved by the Federal Trade Commission, to make sure there is no suspicious activity.

6. If you suspect your identity has been stolen, you can contact the Identity Theft Resource center at 1-888-400-5530 or by visiting **www.idtheftcenter.org**

By staying vigilant, you can make sure that all your personal information says secure!

● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●

You can view more tips using our short link http://go.gstric.org/403-theft (content from **ConnectSafely.org**).

Activity Time - More Awesomeness

In the October 2020 issue of this newsletter, we introduced you to the wonderful world of **Interland**, which is a part of Google's **Be Internet Awesome** initiative.

Interland has a world called **Tower of Treasures**, where your task is to collect your personal information and save it in the tower of treasure before hackers get it!

You can play this game with no sign up at **http://go.gstric.org/403-tower**

Once you have dodged the hackers, head on over the **Be Internet Awesome Family Page** at **http://go.gstric.org/403-families** and check out some fantastic print resources and activities centering around all things digital citizenship!

GSTRIC Digital Citizenship Resources

The Digital Citizenship Committee has been providing newsletters going on four years now! Have you ever been to the Digital Citizenship website and checked out all the available resources?

The URL for the website is http://dc.gstboces.org

Browsing the website, you will find links to:

- Digital Citizenship Monthly Newsletters
- Digital Citizenship Blog
- The current 2021-2022 Calendar Contest information
- The 2020-2021 Digital Citizenship Calendar
- All student art submitted for the 2020-2021 Digital Citizenship Calendar contest
- Downloadable/Printable Resources
- GST Web Resources
- Copyright and Fair Use Resources
- Other Web Resources
- Resources from a past GST BOCES Workshop on Digital Citizenship

Currently not receiving our monthly newsletter electronically. Sign up here http://go.gstric.org/dcnews-signup

Follow us on Instagram - https://www.instagram.com/dc.gstboces/

Once you have checked out our webpage, and caught up on newsletters, send any comments, suggestions and questions to dc@gstboces.org. We would be glad to hear from you.

I AM A DIGITAL CITIZEN

digital
detective

Exploring Your Own Digital Footprint

Use this sheet to jot down sites and services that you use regularly and explore their privacy policies. What types of information are they collecting about you? Do you notice that the site customizes its content specifically for you? If your friends use the site, does it show them the same content it shows you?

searches + commercial sites:

social media:

websites that you use:

** After you have finished your investigations, share your information and what you have learned with your parents and your family, your teachers, and your classmates. And of course, you can always share it with us at dc@gstboces.org.

Visit http://dc.gstboces.org

RIC one DPS

A DIGITAL CITIZEN I AM