

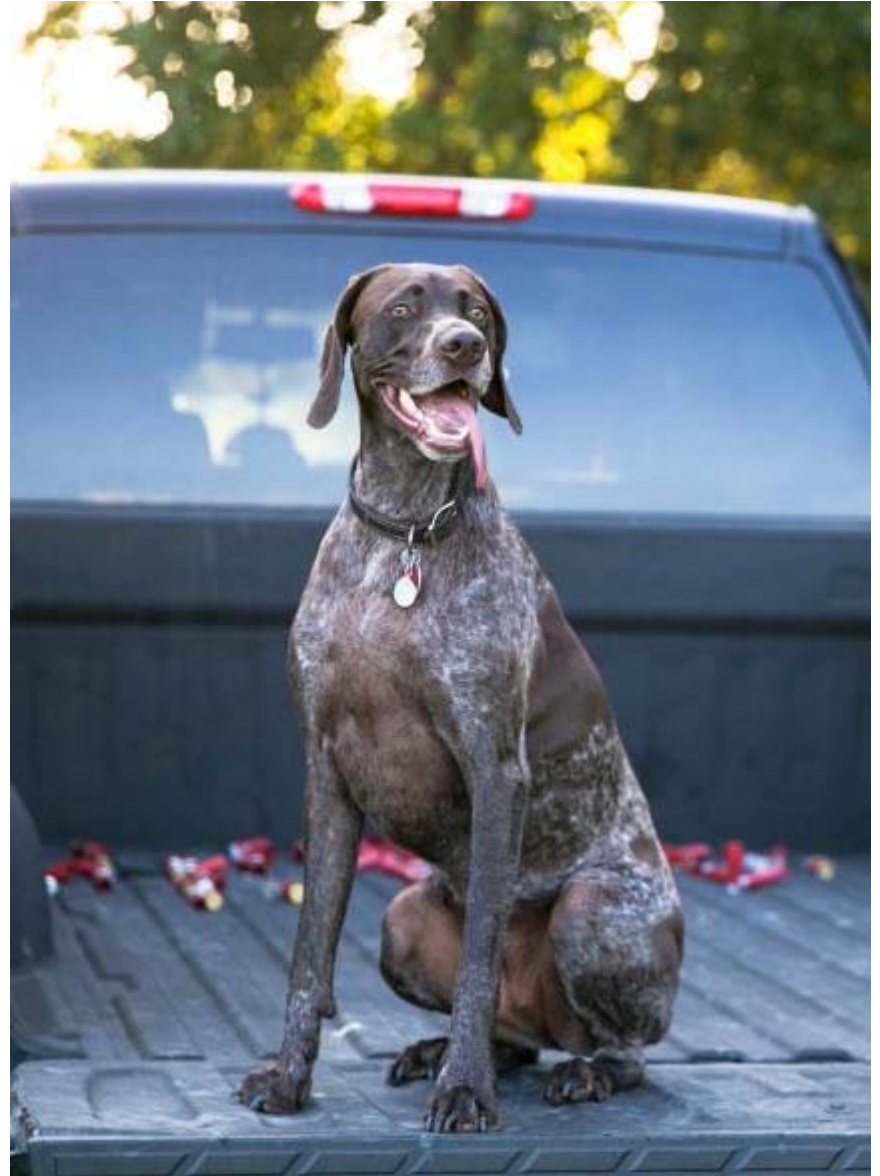


Social Media

How to Protect Yourself in an Ever-Changing Landscape

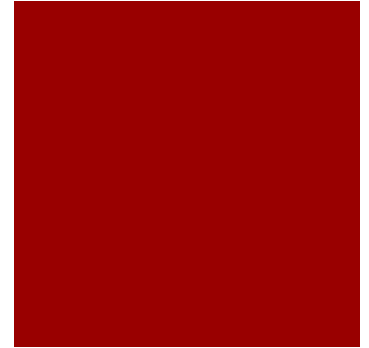
Who I Am?

- Dinah Goodson
- Grew Up in Glen Rose, Texas
- Graduated with a Bachelor of Arts in Public Relations and Masters of Arts in Mass Communications with a focus in Sports Media from Texas Tech University
- Dairy Queen Blizzard lovin', dog mom

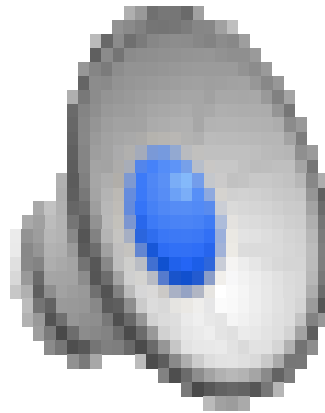


What I Do

- Content Marketing Strategist at Southwestern University.
- Which means, I'm a digital marketing professional.
 - Social Media
 - Display Advertising
 - Retargeting
 - Google Ad Words
 - Geo-fencing
 - Analytics



What's a Digital Footprint?

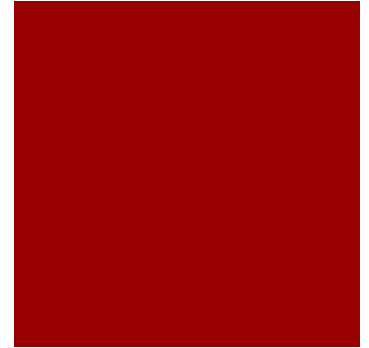


How to Avoid Marketers

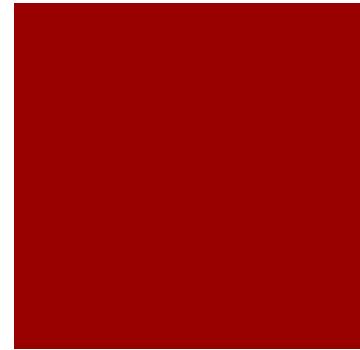
- Burn all sources of digital media now!
- Delete your cookies.
- Tell Mark Zuckelburg thank you for Facebook algorithms.



How to Avoid the Really Bad Guys!



Tip 1: Privacy Settings

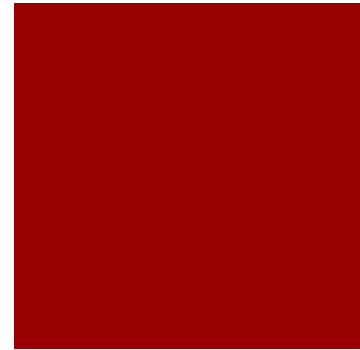


Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

Facebook

Tip 1: Privacy Settings



Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	Friends	Edit

Facebook

Tip 1: Privacy Settings



Privacy

- Photo tagging
- Allow anyone to tag me in photos
 - Only allow people I follow to tag me in photos
 - Do not allow anyone to tag me in photos

- Tweet privacy
- Protect my Tweets
- If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more.](#)

- Tweet location
- Add a location to my Tweets
- When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)

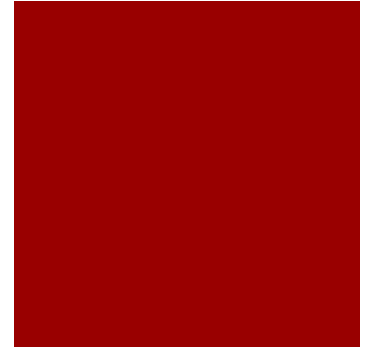
Delete location information

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

- Discoverability
- Let others find me by my email address
 - Let others find me by my phone number
- [Learn more](#) about how this data is used to connect you with people.

Twitter

Tip 1: Privacy Settings

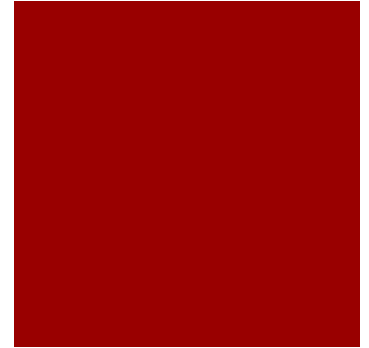


- Personalization** Tailor Twitter based on my recent website visits
[Learn more](#) about how this works and your additional privacy controls.
- Promoted content** Tailor ads based on information shared by ad partners.
This lets Twitter display ads about things you've already shown interest in.
[Learn more](#) about how this works and your additional privacy controls.
- Twitter for teams** Allow anyone to add me to their team
 Only allow people I follow to add me to their team
 Do not allow anyone to add me to their team
Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. [Learn more](#).
- Direct Messages** Receive Direct Messages from anyone
If selected, you will be able to receive messages from any Twitter user even if you do not follow them.
 Send/Receive Read Receipts
When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see receipts from other people. [Learn more](#)

Twitter

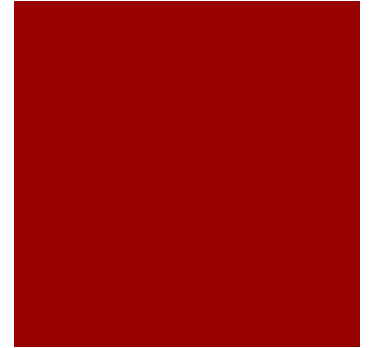
Tip 2: Beware of TMI

- The Duhs!
 - Social Security # or last 4 digits
 - Birth Date
 - Home Address or Phone Number
 - Passwords
 - PIN numbers
 - Bank account
 - Credit Card Info
- Your current location. (locations feature on social media outlets)
- Real-time photos or videos.



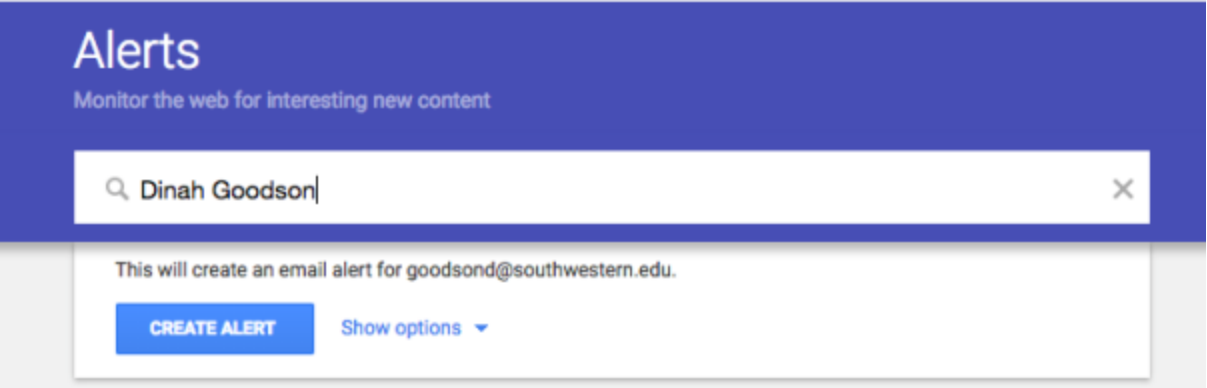
Tip 3: LinkedIn Work History

- Don't include your full resume.
- Identity thieves can use that information to fill out a loan application, guess a password security question or social engineer their way into your companies network.



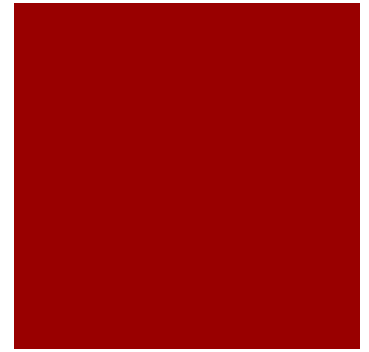
Tip 4: Search Yourself

- Check out how your profile looks to other people. See if your privacy settings are like you want them.
- If you see your name in locations you don't frequent, could mean someone else is using your identity online.
- Set up a Google alert with you name.
 - Go to [google.com/alerts](https://www.google.com/alerts)
 - Create your alert.



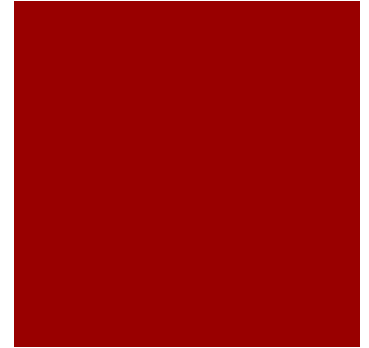
The screenshot shows the Google Alerts interface. At the top, the word "Alerts" is displayed in white on a blue background, with the subtitle "Monitor the web for interesting new content" below it. A search bar contains the text "Dinah Goodson" with a magnifying glass icon on the left and a close button (X) on the right. Below the search bar, a white box contains the text "This will create an email alert for goodsond@southwestern.edu." At the bottom of this box, there is a blue button labeled "CREATE ALERT" and a link labeled "Show options" with a downward-pointing triangle.

Something to Think About



A Child's Digital Footprint

- The average parent will post almost 1,000 photos of their child by the time they are 5.

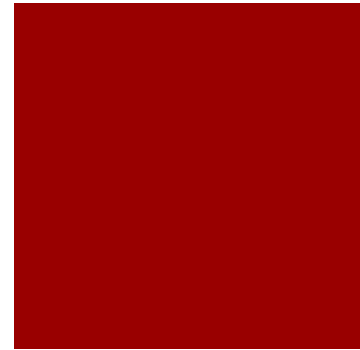


The Facts

- A quarter of parents never ask permission of people in photos before sharing them.
- Nearly one-fifth have never checked their privacy settings.
- Majority of parents who use social media (74%) say they know another parent who has shared too much info about a child. This includes:
 - Embarrassing Information
 - Personal Information that could identify a child's location
 - Inappropriate photos

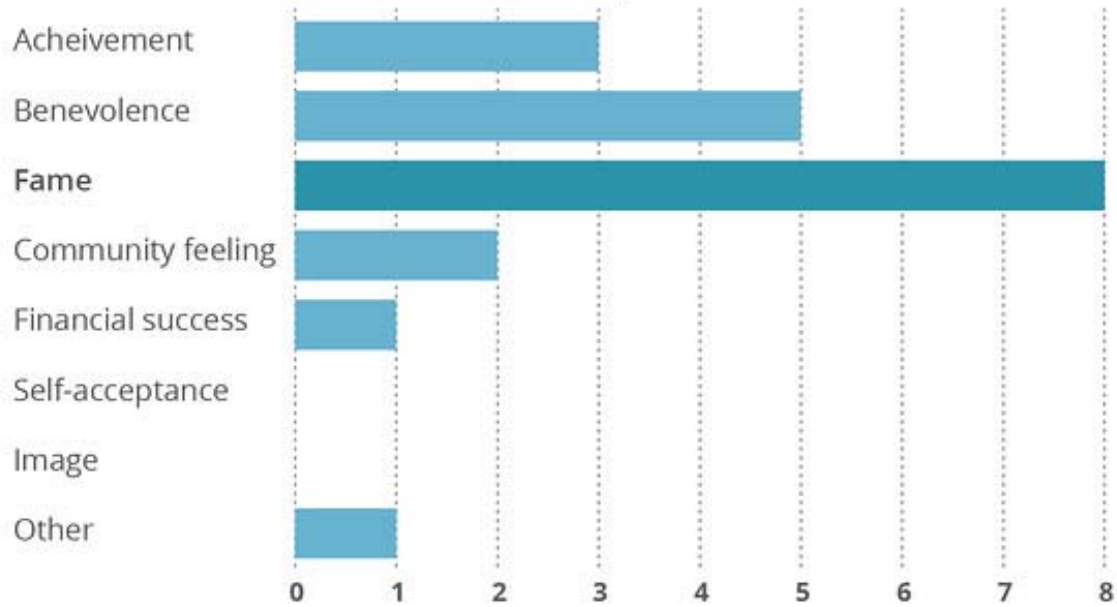


Kids Value Fame



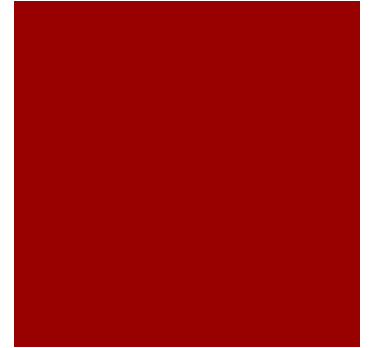
The kids want fame

These children were asked to list their future goals



Source: Yalda T. Uhls and Patricia M. Greenfield

What This Means



- Before a child turns 5, their parents have already created their digital footprint for them. They have to live with this digital footprint for the rest of their lives.
- When they are old enough, they are learning that they can post whatever they want without another persons consent.
- They are learning that likes (fame) is the most important thing.
- They could be at risk from predators.

Questions??

