

Digital citizenship and your digital footprint

1. This overview
2. Digital citizenship
3. Your digital footprint





First:

What things
contribute to
your “digital
footprint”?



Next:

How can you
take control of
your “digital
footprint”?

1. Be kind and helpful on public accounts
 2. Use privacy settings
 3. Keep a list of your accounts
 4. Don't overshare
 5. Use good password management
 6. Google yourself
 7. Monitor linking accounts
 8. Consider using an anonymous second email address
 9. At least skim the terms and conditions
 10. If you post it online, assume it is published forever
 11. Understand that searches are social
- Use digital tools to manage your digital footprint




Demonstrate good digital citizenship

Citizenship (Merriam-Webster): membership in a community, or ***the quality of an individual's response to membership in a community***

Modified to the digital world: “The quality of habits, actions, and consumption patterns that impact the ecology of digital content and communities.”






“The quality of habits, actions, and consumption patterns that affect the ecology of digital content and communities.”

What do you do to support the digital communities you are a part of?



General guidelines

- **Remember the human**
- **Act online as you would in real life**
- **Understand and follow the community rules**
- **Put your best foot forward**
- **Look for original sources**
- **Be constructive in your criticism**
- **Give people the benefit of the doubt**
- **Do not engage in trolling, harassment, or other bad behavior**
- **Report rule violations**



Your Activity	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 see the people, Pages and lists you follow?	Public	Edit
How people find and contact you	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Public	Edit
	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?	Yes	Edit
How You Get Message Requests	Decide whether message requests go to your Chats list, your Message requests folder, or whether to receive them at all.		
	Potential Connections		
	Friends of friends on Facebook	Chats	Edit
	Other people		
Others on Facebook	Message requests	Edit	
Accounts on Instagram	Message requests	Edit	

YOU decide how much information you want to share, and take control of your private information!

Browser Privacy

Enhanced Tracking Protection



Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.

[Manage Exceptions...](#)

[Learn more](#)

Standard

Balanced for protection and performance. Pages will load normally.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

Includes Total Cookie Protection, our most powerful privacy feature ever

Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. [Learn more](#)

Strict

Stronger protection, but may cause some sites or content to break.

Custom

Choose which trackers and scripts to block.



2. Use privacy settings

Run in Private Windows

Allow Don't Allow

When allowed, the extension will have access to your online activities while private browsing.

[Learn more](#)



3. Keep a list of account usernames and passwords

In a secure place
Consider simple encoding

example:

hunter2

duckhunter2

4. Don't overshare.

This includes information that is not explicitly about you



5. Use a password manager

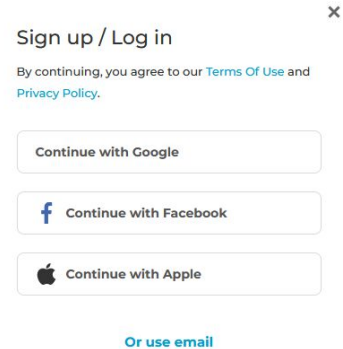
Bitwarden, KeePass, Dashlane, Keeper

6. Google yourself

You can even set an alert for your name
(<https://www.google.com/alerts>)

7. Monitor linking accounts


Convenient, but safe?







Alerts


Monitor the web for interesting new content

🔍 Create an alert about...

My alerts (2) 

"Jeremy Storly"  

jeremy.storly@cornerstonescareer.com  

- 
- 8. Consider using an anonymous, secondary email**
 - 9. At least skim the terms and conditions**
 - 10. Assume what you post online is being published forever**





11. Understand that Searches are Social

Data is harvested from every site you visit and every search you do

12. Use digital tools to manage your digital footprint

Extensions: uBlock Origin, Font Fingerprint Defender

Private (Incognito) mode

Choosing a more secure browser

THINGS TO REMEMBER

1. Private or incognito browsing isn't really private
2. If a site or app is free, then you might be the product
3. Beware of sites or users who ask for personal information

Note: The only way to totally remain private online is not to go online.

Be informed so you can take control of your footprint, not so you can eliminate it.





<https://amiunique.org/>



Learn how identifiable you are on the Internet

Help us investigate the diversity of web browsers.

This website aims at studying the diversity of browser fingerprints and providing developers with data to help them design good defenses. Contribute to the efforts by viewing your own browser fingerprint or consult the current statistics of data provided by users around the world!

[View my browser fingerprint](#)

If you click on this button, we will collect your browser fingerprint, we will put a cookie on your browser for a period of 4 months. More details are available in the [privacy policy](#)

My browser fingerprint

Are you unique ?

Yes! You are unique among the 1164010 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.



50.26%



47.57%



2.24%

UTC-6

2.88%

en

76.34%

Similarity ratio duration : 7 days 15 days 30 days 90 days All time



<https://haveibeenpwned.com/>



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(0b5e7e25e8775f7e7e80906ada4f0021_img.jpg\) !\[\]\(740312fd467f47b04cab841ab3868d83_img.jpg\)](#)

';--have i been pwned?

Check if your email or phone is in a data breach



pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

641

pwned websites

11,999,160,131

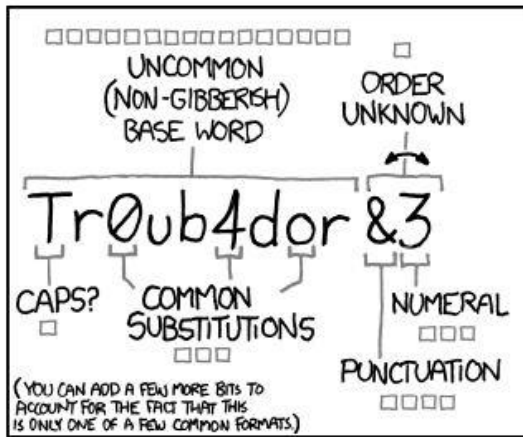
pwned accounts

115,568

pastes

227,241,349

paste accounts



~28 BITS OF ENTROPY

□□□□□□□□ □

□□□ □□□

□□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

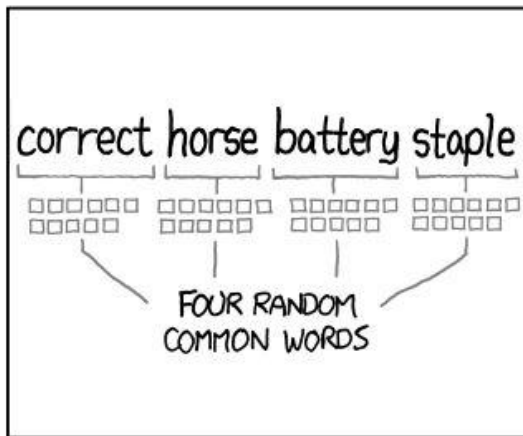
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HIGH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□

□□□□□□□□□□

□□□□□□□□□□

□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Go to <https://www.digitalliteracyassessment.org/> and scroll down until you find “Using Technology in Daily Life”