

Privacy & Security

The Digital Age



WIKIPEDIA
The Free Encyclopedia

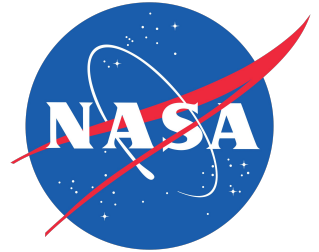


UBER

Google



facebook



Data Privacy **AND** Data Security



Privacy = the appropriate use of your data

Security = the integrity, confidentiality, and availability of your data

Questions to
think about...

How do I keep
my personal
data secure and
private?

Strong Passwords

- Complex passwords containing 8-20 characters
 - Capital and lowercase letters
 - Special characters (! @ # \$ % ^ & *)
 - Numbers
- Different passwords for different accounts

Strong Passwords

- 2 Factor Authentication

- A 2 step verification process for an added layer of security
 - Texting your phone with a unique pin
 - Calling your phone with a unique pin
 - Asking you a security question specific to you

- Password Managers

- Help manage and diversify your passwords
- Be careful...you need to keep your master password safe!

Which is stronger?

password123 or *pA\$s5%w0Rxd86#18

codehs2018 or c0#d*3HhSs!()fn

Tips:

- Limit any personal details included (birthday, graduation year, name)
- Try not to spell out full words (the more random the better)
- Don't write passwords out on apps like Notes, Evernote, iMessage, or other places your digital footprint lives

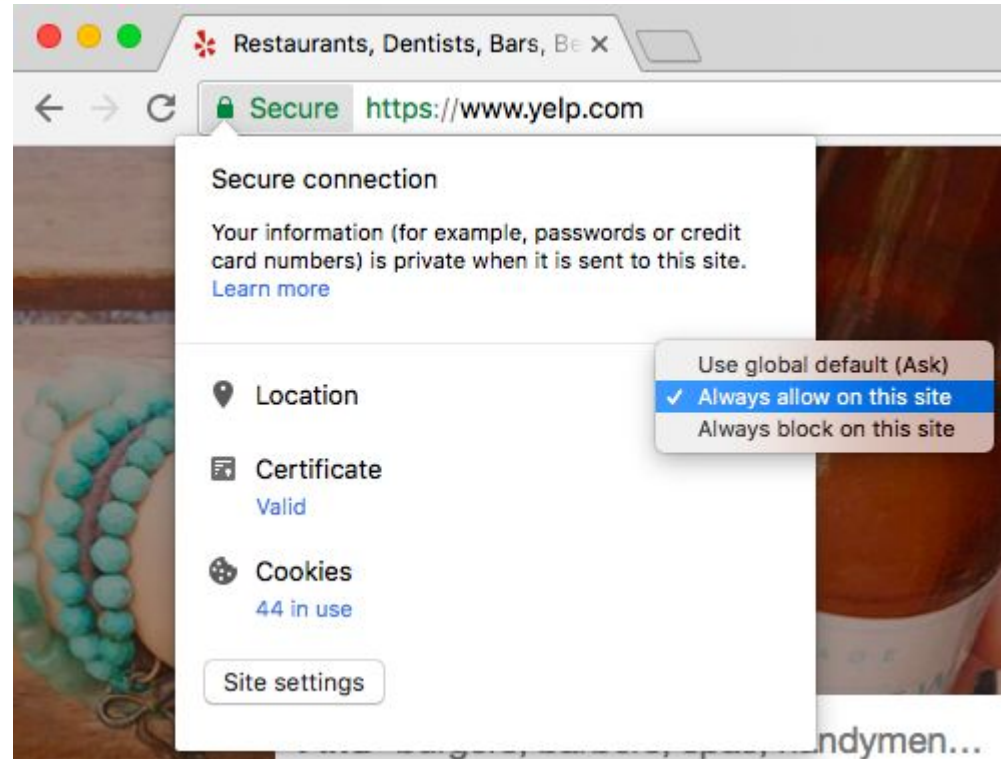
Secure Sites

- **https://**
 - **s = secure**
 - **http:// = less secure**
- Verify the URL
- Avoid lots of popups
 - 1 or 2 popups are okay
- Use your best judgment



Secure Access to Hardware

- Webcam access
- Audio access
- Microphone access
- Location access



Privacy Policies

- Legal documents websites have that disclose the ways they can store and share your data
 - Typically very long and dense documents many users do not want to read



Not all privacy policies are equal

Some privacy policies use your data to make money or to target products and advertisements at your

- Ever wonder why that watch you just Googled about appeared on your Instagram newsfeed?



Avoiding Phishing Scams

Phishing: a method to gather personal information such as usernames and passwords using deceptive emails and websites



Stolen Data: What Can Happen?

- Online impersonation on social media
- Bank account theft
- Identity theft
- Communicating inappropriately with others
- Sharing or selling your private data



Stolen Data: What to do?

- Contact a parent or IT professional at your school
- Contact a representative from the company (Gmail, School portal login, Instagram, etc.)
- Contact your bank and notify them of any fraudulent charges

Security Reminders

- Use your best judgment
- Use password best practices
- Check twice to make sure a website is secure
- Be careful when logging on to public computers
- Stay up to date on the best web security practices

CompTIA ITF+ Alignment

6.3 Summarize confidentiality, integrity and availability concerns.

- Expectations of privacy when using:
 - The Internet
 - Social networking sites
 - Email
 - File sharing
 - Instant messaging
 - Mobile applications
 - Desktop software
 - Business software
 - Corporate network
- Written policies and procedures
- Handling of confidential information
 - Passwords
 - Personal information
 - Customer information
 - Company confidential information

CompTIA ITF+ Alignment

6.5 Explain password best practices.

- Password length
- Password complexity
- Password history
- Password expiration
- Password reuse across sites
- Password managers
- Password reset process