Online Self Defense

The basics of staying safe online.

At the end of this class you will be able to...

1. Act as a good digital citizen online
2. Create strong passwords
3. Avoid cyber attacks
4. Adjust your smartphone settings for privacy and security

Digital Citizenship

Living a healthy online life

A Good Citizen...

Follows the rules and laws

Is kind and respectful

Communicates clearly

Respects the property of others

Keeps themselves and others safe

Takes responsibility for their actions

Stays informed about the world

Be a good citizen offline

and online

Passwords

Creating a set of keys for your digital house

Creating Strong Passwords

1. Create a passphrase

Examples:

- Spooky Halloween
- I love reading at the library
- Today is a great day
- Hope is the only thing stronger than fear

Creating Strong Passwords

2. Add numbers and symbols.

Examples:

- SpookyHalloween4252
- I love reading at the library*@3
- 15&Todayisagreatday
- Hope is the only thing stronger than fear67%

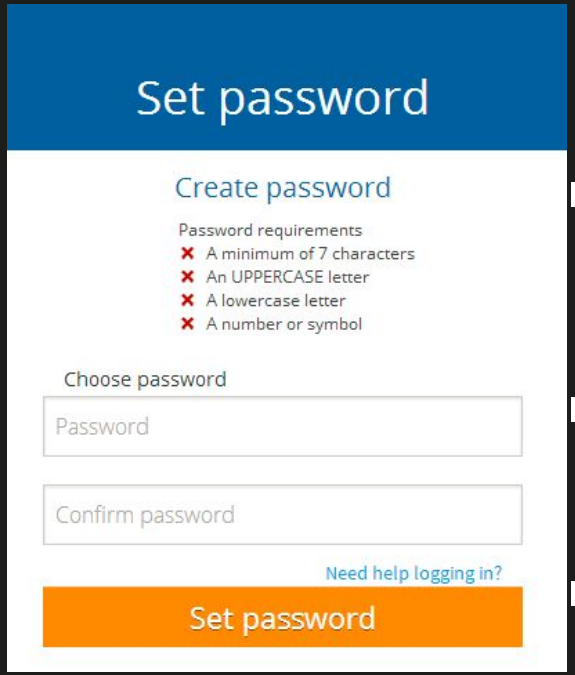
Creating Strong Passwords

3. Follow the site specific rules.

Your Password:

- Must be different from your User ID
- Must contain 8 to 20 characters, including one letter and number
- May include one of the following characters: %, &, _, ?, #, =, -
- Your new password cannot have any spaces and will not be case sensitive.

*REQUIRED FIELD

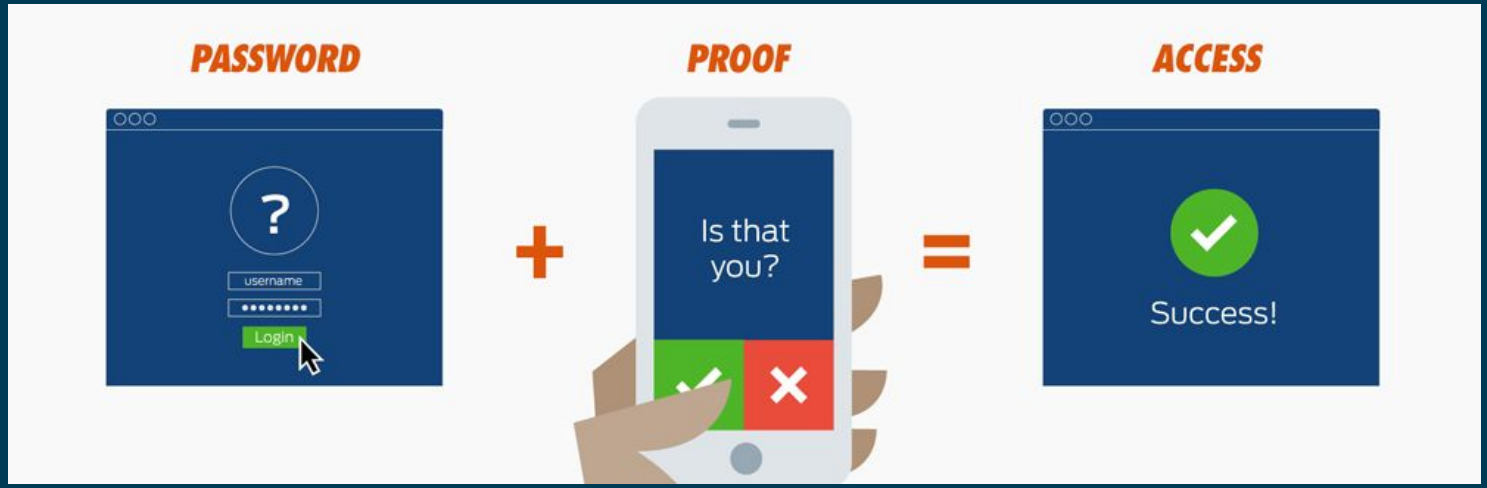


Creating Strong Passwords

Tips for Success

- Don't use personal information (street name, nicknames, children's names)
- Avoid simple words, phrases, or patterns (abcd, 1234, qwerty, password)
- Don't reuse passwords on important accounts (banks, email, taxes)
- Don't write it down where someone can find it
- Use face ID or fingerprint passwords when possible
- Use 2-factor authentication
- Use a password manager

2-Factor Authentication



Password Managers

Cyber Attacks

How to avoid phishing and malware

Phishing

- Only click on links from trusted sources
- Don't download any attachments unless you know who it's from and what it is
- Only enter personal information on websites that use HTTPS
- Listen to your gut. If the message seems out of character for the person contacting you don't trust it. Contact the person on a different platform to verify their identity.

Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted] Spam x

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>
to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

The Amazon Marketplace

- - - - - -SHOPPER/MEMBER:4726
- - - - - -DATE-OF-NOTICE: 12/22/2015

Hello Shopper: [redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

subject: Hello

from: **red.orange@aol.com via yellow.edu.ar**

to: green.blue@purple.org
Today, 4:40 AM

Hello,

Green, Are you free at the moment?

Regards
Red Orange

Sent from my iPhone

---

from: Blue, Green

to: red.orange@aol.com
Today, 5:20 PM

Do you still want to talk? Sorry, I was in a meeting.

...

---

from: **red.orange@aol.com via yellow.edu.ar**

to: green.blue@purple.org
Today, 5:20 PM

Yeah i just need you to do something for me.I am tied up right now, can you purchase itunes gift card3 pieces - $100 each? I would reimburse you when am through, Let me know also i would prefer to call you but can't receive or call at the moment with my line.

Regards
Red Orange

Malware = Malicious Software

Software designed to do damage or other unwanted actions on your computer.

- Viruses, worms, trojan horses, ransomware, spyware
- Don't download email attachments if you don't know what they are
- Don't click on links or visit websites you are unfamiliar with
- Install and keep updated antivirus software
- If infected, stop using the computer and change all passwords using a different device

Ransomware

- Mostly attacks businesses and governments
- Encrypts your information so you can't access it
- Attackers make you pay to gain access to computer again
- Spread through phishing emails, advertisements
- Backup important information


KASPERSKY lab


AVG


avast


Bitdefender

Smartphone Safety

Staying healthy when you're mobile

Getting Your Settings Right

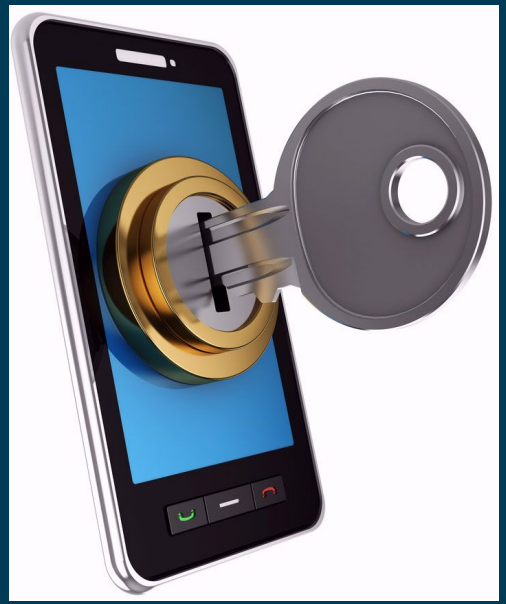
- Security
- App Permissions
- Location

Android

iOS

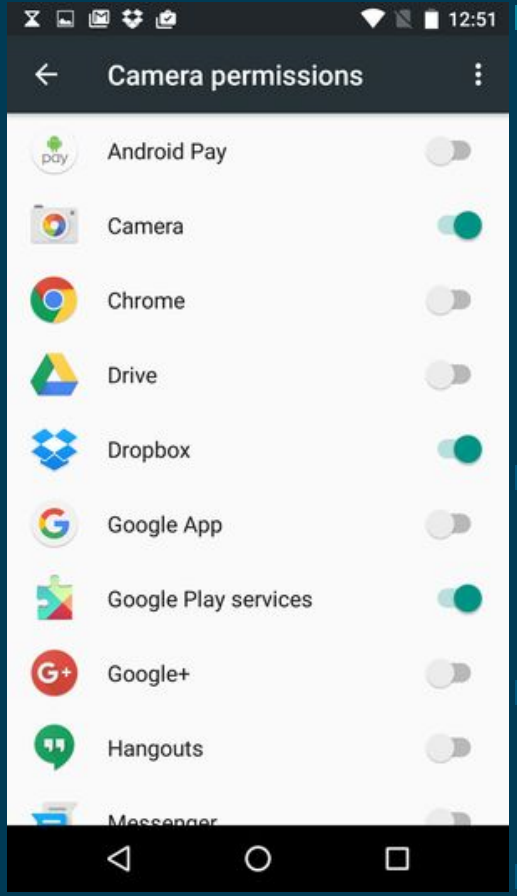
Security Settings

- Enable a screen lock password: Fingerprint and facial ID are best choices. Otherwise use 6 digit PIN.
- Enable a password on any apps with sensitive information (e.g., bank accounts, health apps, email)
- Update software and apps regularly
- Setup iCloud (iOS) or Device Manager (Android)

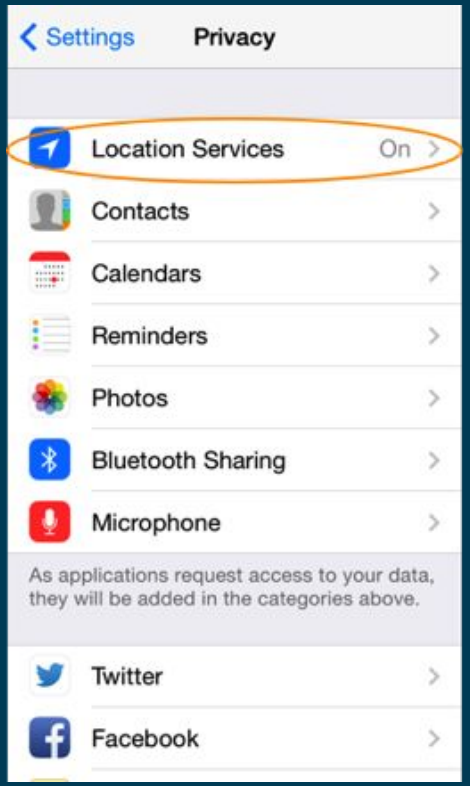


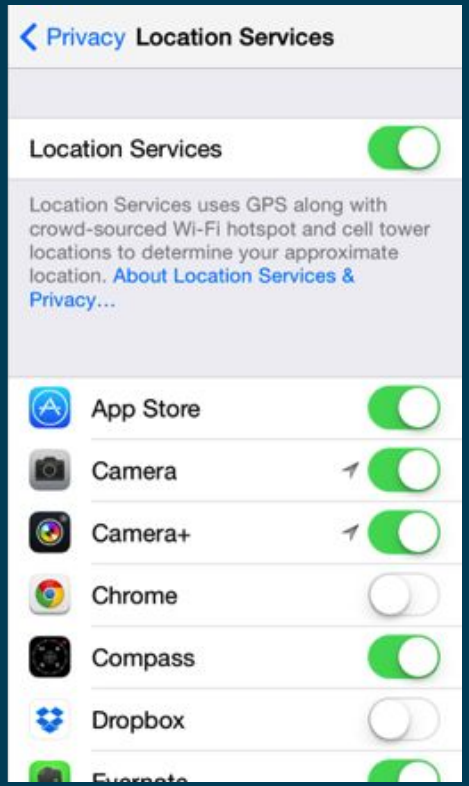
App Settings

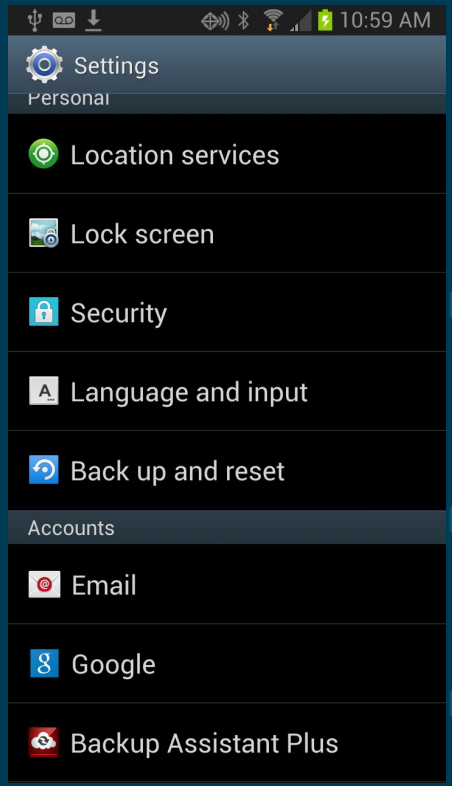
- Don't give apps an all access pass to your information
- Look at each app individually to decide if you want it to have access
- Never download an app if you feel uncomfortable with permissions
- Only download apps from authorized stores (Google Play or App Store)



Location Settings







Use public wifi with caution

Survey

Questions?

Make an appointment with a librarian!

sjpl.org/privacy

chooseprivacyeveryday.org/self-defense.pdf