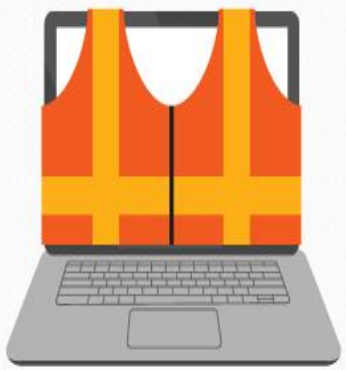


# CYBER SAFETY:

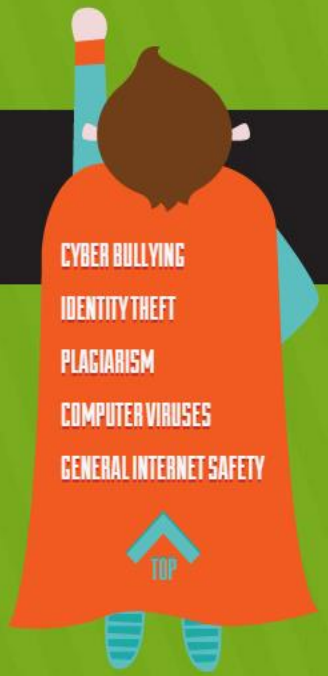
*An Interactive Guide To Staying Safe On The Internet*



## INTRODUCTION

The Internet is without a doubt one of the best resources available to us. Unfortunately it's also extremely dangerous if you aren't aware of who and what lurks behind the scenes. Everyone should know how to be safe when surfing the web, but internet safety tips and tricks are spread out all over the web without a go-to resource. Since the majority of internet scam and virus victims are students and young people, Open Colleges is a perfect place to post the very first full guide to being safe on the internet.

# CYBER BULLYING




> *"Cyber Bullying is the use of the Internet and related technologies to harm other people in a deliberate, repeated, and hostile manner."* - **Wikipedia**

## FORMS

**Whether it's posting public pictures, social statuses, or personal messages, cyber bullying takes many forms. The most popular cyber bullying tactics are:**

### 1 FLAMING

*Online fights using electronic messages with angry and vulgar language.*


*Joe and Alec's online exchange got angrier and angrier. Insults were flying. Joe warned Alec to watch his back in school the next day.*

## 2 HARASSMENT

*Repeatedly sending nasty, mean, and insulting messages.*


*Sara reported to the principal that Kayla was bullying another student. When Sara got home, she had 35 angry messages in her e-mail box. The anonymous cruel messages kept coming - some from complete strangers.*

## 3 DENIGRATION

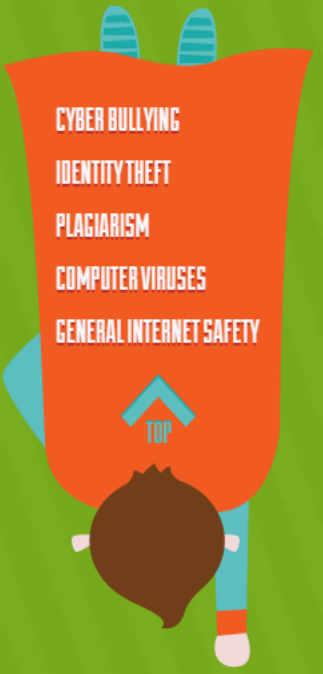
*"Dissing" someone online. Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.*


*Some boys created a "We Hate Joe" Web site where they posted jokes, cartoons, gossip, and rumors, all dissing Joe.*

## 4 IMPERSONATION

*Pretending to be someone else and sending or posting material to get that person in trouble or danger or to damage that person's reputation or friendships.*


*Laura watched closely as Emma logged on to her account and discovered her password. Later, Laura logged on to Emma's account and sent a hurtful message to Emma's boyfriend, Adam.*



## 5 OUTING

*Sharing someone's secrets or embarrassing information or images online.*

*Greg, an obese high school student, was changing in the locker room after gym class. Matt took a picture of him with his cell phone camera. Within seconds, the picture was flying around the phones at school.*

## 6 TRICKERY

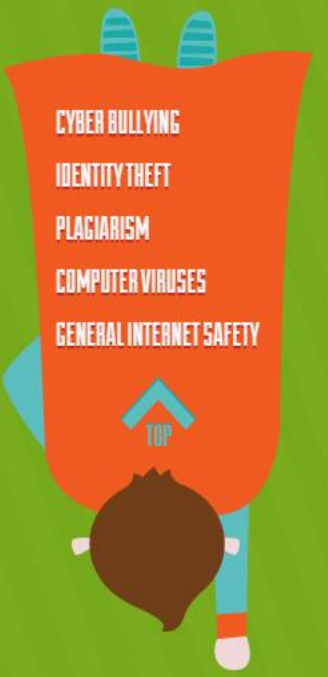
*Talking someone into revealing secrets or embarrassing information, then sharing it online.*


*Katie sent a message to Jessica pretending to be her friend and asking lots of questions. Jessica responded, sharing really personal information. Katie forwarded the message to lots of other people with her own comment, "Jessica is a loser."*

## 7 EXCLUSION

*Intentionally and cruelly excluding someone from an online group.*

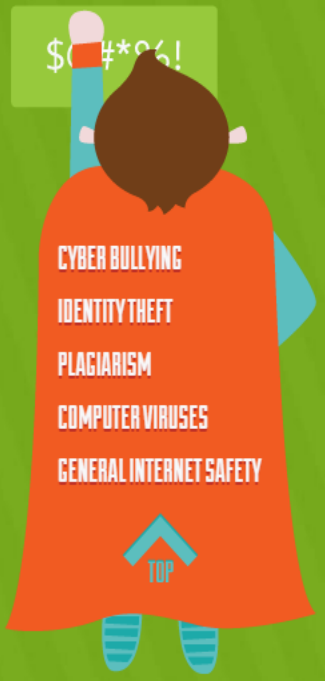

*Millie tries hard to fit in with a group of girls at school. She recently got on the "outs" with a leader in this group. Now Millie has been blocked from the friendship links of all of the girls.*



## 8 CYBERSTALKING

*Repeated, intense harassment and denigration that includes threats or creates significant fear.*


*When Annie broke up with Sam, he sent her many angry, threatening, pleading messages. He spread nasty rumors about her to her friends and posted a sexually suggestive picture she had given him in a sex-oriented discussion group, along with her e-mail address and cell phone number.*



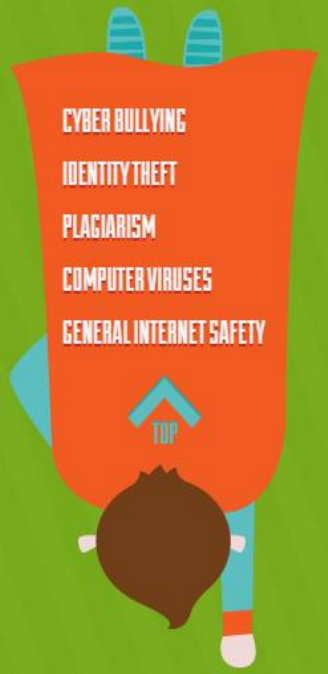

# EFFECTS

Just a handful of the effects of Cyber Bullying include:

- Undermining confidence
- Causing stress and hurtful health effects
- Affecting performance and attendance in school
- Depression and a sense of loneliness
- Suicidal thoughts

## But why are the effects so devastating?

For one, cyber bullying material can be worldwide and is often irretrievable. Bullies can be anonymous, giving the victim a sense of helplessness.

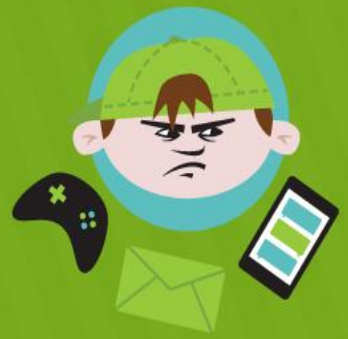



# MISCONCEPTIONS

Contrary to popular belief, **cyberbullying doesn't just happen to kids**. Bullies on the web will look for almost anyone to harass, as long the bully has someone to pick on and an audience.

While most cyberbullying takes place on instant messaging nowadays, kids are bullied almost anywhere in the virtual world.

This includes: **Chat rooms, video games, e-mail, blogs, and even over cell phones.**



Cyberbullying isn't just kids picking on other kids. If handled incorrectly, **it can escalate**

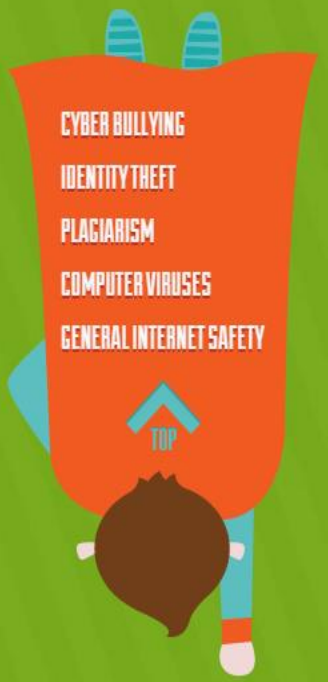
Cyberbullying isn't just kids picking on other kids. If handled incorrectly, **it can escalate from rude jokes and gossip to cyberthreats.**

# LOL > FYI > YOU'RE DEAD

Examples of these threats can include physical threats to others or be self-inflicted.

> *A group of girls at his school had been taunting Alan through IM, teasing him about his small size, daring him to do things he couldn't do. They dared him to commit suicide. He discussed this with them. The girls thought it was a big joke.*

**It's best to catch and prevent online bullying in its early stages, what may seem harmless at first can turn out to be much more.**



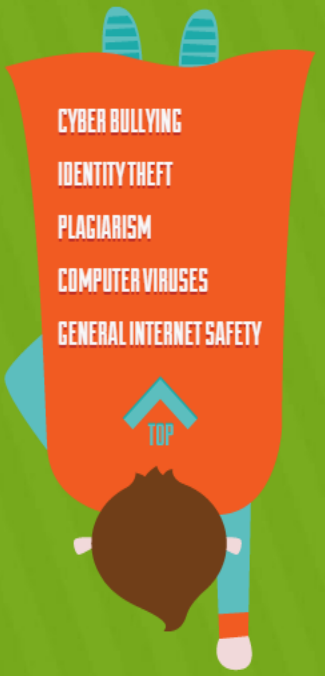

## FACTS


Common Cyberbully targets are kids in their pre-teen years.

Online conflicts will sometimes start in the real world, a.k.a. schools, and then transfer into the virtual world. Bullying is pushed to the virtual world because cyberbullies are mostly, if not completely, anonymous.

# LEGAL ISSUES

Cyberbullying is not to be handled lightly and can quickly become a serious problem. There have been many cases where cyberbullying has resulted in victims fearing for their lives and even committing suicide. There are specific actions that can actually cause a bully to break civil or criminal laws.




## CIVIL LAWS

In this case, a victim should try to resolve this problem by seeing a bully's parents or asking an attorney for advice on how to handle the situation.

Defamation

*Someone publishes a false statement about a person that damages his or her reputation*

Invasion of privacy/public disclosure of a private fact.

*Someone publicly discloses a private fact about a person under conditions that would be highly offensive to a reasonable person.*

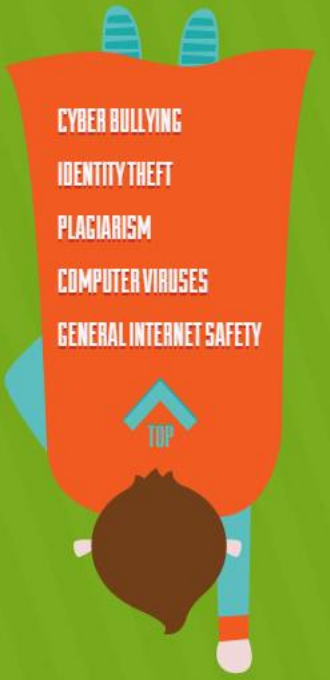
Invasion of personal privacy/false light.

$@#*%!

# CRIMINAL LAWS

When a bully is accused of breaking criminal laws, they can be subject to prosecution and even arrest.

- **Hate or bias crimes**
- **Making violent threats to people or their property.**
- **Engaging in coercion. Trying to force someone to do something they don't want to do.**
- **Making harassing telephone calls, sending obscene text messages, and stalking.**
- **Sexual exploitation and sending sexual images of children under 18.**
- **Taking a photo of someone in a place where privacy is expected (locker room, bathroom, etc.) and exploiting it on the internet.**




# PREVENTION

Luckily, there are practices you can put in place today to prevent cyber bullying from happening. Even though there's no "one size fits all" solution, here are some of the steps

## Tell someone.

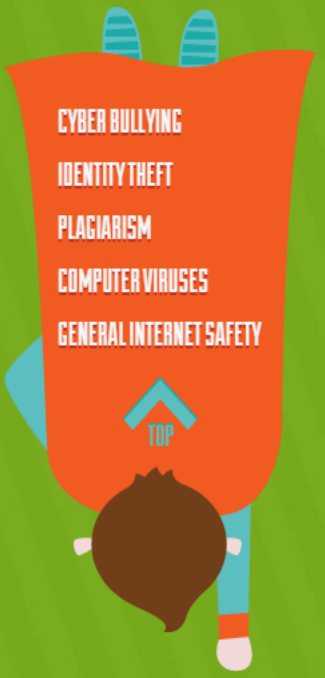
Just let a trusted adult know what's going on. The worst thing you can do is to keep it to yourself. Remember, it's not your fault!

## Don't instigate.

If someone is sending you hurtful messages or posting mean pictures, they're doing it to get an emotional response from you. Don't give them one! Don't respond OR retaliate. This will only encourage them to take it further.


## Block them.

If it's on Facebook or another website that allows you to block the person or leave the chat room, then do it!




## Be aware.

If you're a parent, encourage your kid(s) to talk about what they're doing online and whom they're doing it with.

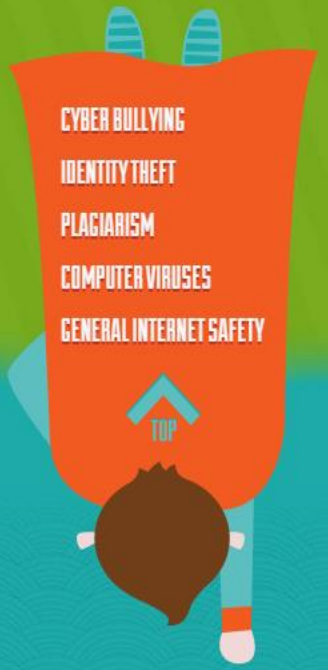
## Block them.

The majority of cyber bullying occurs by someone you already know. These are also the people that are closest to you and your passwords, so keep them safe.

Especially on public computers.


## Don't be a cyber bully yourself.

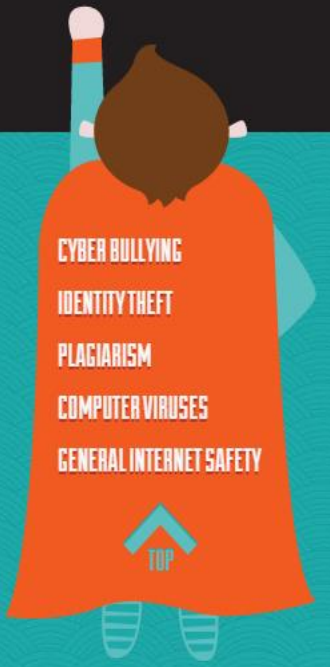
It's easy to be hurtful, so remember what it's like for the person on the other side.




# IDENTITY THEFT

*"Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity"* - **Wikipedia**

# IDENTITY THEFT



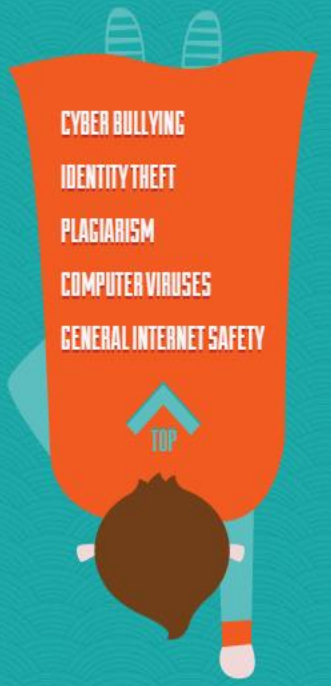

> *"Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity"* - **Wikipedia**

## BE CAREFUL

While there are many ways for your identity to get stolen, the easiest way to become a victim of identity theft is by sharing personal information over the internet. If you aren't careful, criminals could steal your identity by finding any of the following:


- Social Security Number
- Credit Card Information
- Bank Account Number
- Personal Identification
  *(driver's license, passport, etc.)*
- Stolen Passwords

# PROTECT YOURSELF




The best way to make sure that your identity never gets stolen is to act **right now** and follow these steps to protect yourself **before** an identity theft attacks.

## PASSWORDS

Your password's job is to protect almost everything on your computer; this includes your personal information, important files, and items with sentimental value.

Creating a strong password is an easy step that goes a long way. The lock on your front door is a complicated system of tumblers that isn't easily opened without a key. Like the lock, your password should seem complicated to others but simple to you.


Following these steps will help you easily create a strong password:

### Use more than one password.

*Using the same password for multiple accounts is an easy way to lose everything you have. Use different passwords so that if one account is broken into, the others will stay safe.*

### Be Relevant and Irrelevant.

*Make a password that you will recognize, but to others it seems random. Never use information that can be directly related to you in your password; like your name, social security number, address, etc.*

### Use (not-so) random characters.

*A password that looks random to the naked eye is more than perfect. For example: MFCIB93 seems like a bunch of gibberish but is easily translated into: My Favorite Color Is Blue and the numbers could refer to anything, like your birth year.*

### Length is important.

*The longer your password is, the harder to figure out what it is. This is the reason for a minimum character length on most websites that you have accounts on.*

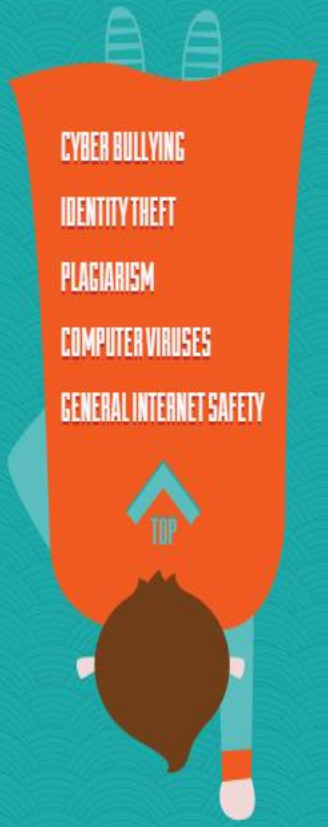
### Use the SUPR test.

**Strong** *Is the password strong? (make sure it's long and looks like random letters and numbers).*

**Unique** *Is the password unrelated to your other passwords?*

**Practical** *Can you remember it without having to write it down?*

**Recent** *Have you changed it recently?*



# PHISHING

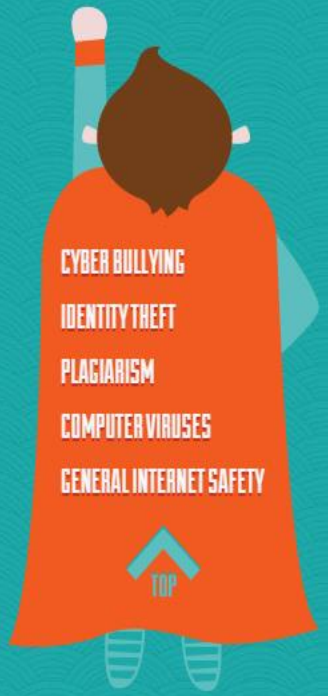

While there are many online scams on the internet, phishing is one that is geared specifically toward retrieving someone's personal information and using it to harm them. An identity thief, known as the phisher, will lure victims using emails and websites that seem harmless or secure.

Some common phishing messages would be:

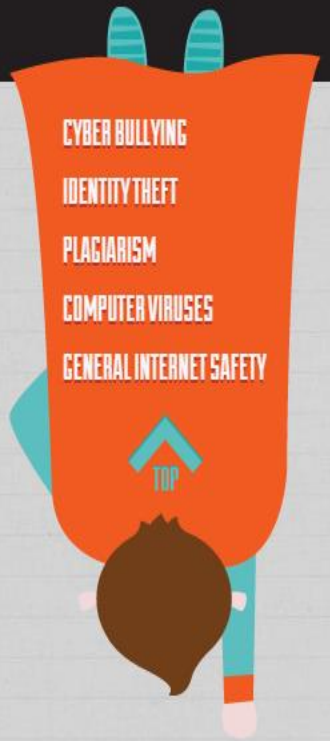
*"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."*

*We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*

*"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."*




# PLAGIARISM




> *"Plagiarism is the wrongful appropriation and purloining and publication of another author's language, thoughts, ideas, or expressions, and the representation of them as one's own original work."*
> **- Wikipedia**

Plagiarism is such a dirty word, you spend your entire life hearing about how bad it is and all of the awful things that happen if you do it. In reality, your entire educational career is founded on some form of plagiarism. All of your research papers and presentation involve information that you learned from somewhere else. While directly copying someone else's work can land you in some serious trouble, paraphrasing and citing your sources will end up saving your life someday.

## CONSEQUENCES OF PLAGIARIZING

Plagiarizing is a very serious situation so before we get into safely using copyrighted works, let's go through some things that might happen if you directly copy another's work.

### Expulsion

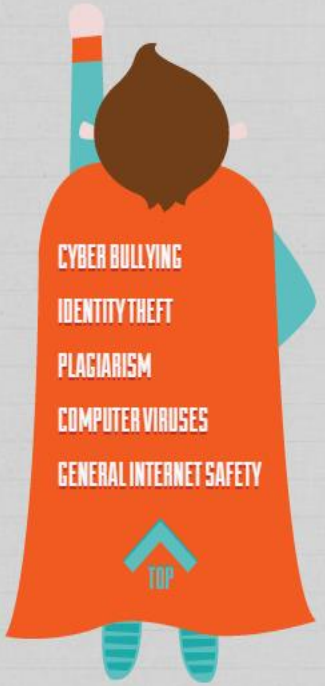
Almost every school from high school to college has zero tolerance for plagiarism.

### Court

Stealing someone else's work is called copyright infringement and depending on the circumstances you might end up in front of a judge and jury.


### Fines

Infringement penalties are very harsh, fines can be anywhere from $500 to $150,000 for each act of willful infringement.




## WHAT IS COPYRIGHTED?

# WHAT IS COPYRIGHTED?

The seven categories that copyright law covers are:

## Literary works

Both fiction and nonfiction, including books, periodicals, manuscripts, computer programs, manuals, phonorecords, film, audiotapes, and computer disks.

## Musical works

and accompanying words, songs, operas, and musical plays.

## Dramatic works

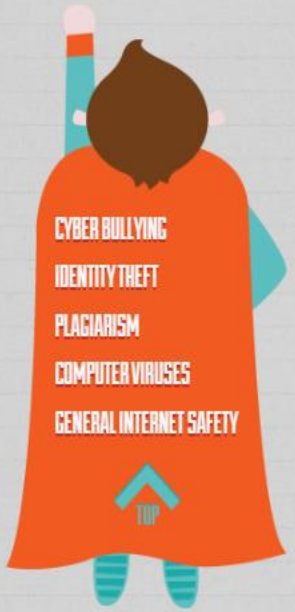
Including music, plays, and dramatic readings

## Pantomimed and choreographed works

Like dances or routines in shows.

## Pictorial, graphics, and sculptural works

Final and applied arts, photographs, prints and art reproductions, maps, globes, charts, technical drawings,

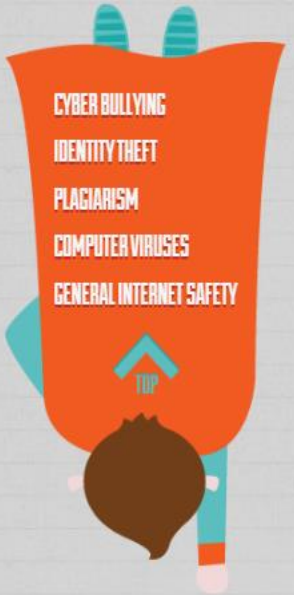


works

Slide/tape, multimedia presentations, filmstrips, films, and videos.

### Sound Recordings

Tapes, cassettes, and computer disks.




# FAIR USE

There are some sources that you can copy from without having to cite. This method of copyrighting is called fair use. There is a large gray area for which works fall under fair use, though.

Here are a couple examples of things that are free to use:

- Works that lack originality (phone books).
- Works in the **public domain**.

  • The **public domain** contains creative works that aren't protected bay any copyrights and may be freely used by anyone.

  • Works end up in the public domain because:
  - *The copyright for that work has expired.*
  - *The author failed to copyright their work.*
  - *The work is owned by the Government.*
  - *Any work published on or before December 31, 1922*
- **Freeware** - Software found online that the author has chosen to make available to anyone without any restrictions
- Commonly known facts
- Ideas, processes, methods, and systems described in copyrighted works

# SOURCE:

- https://www.opencolleges.edu.au/informed/cyber-safety/

# THANK YOU