

# Being Safe On The Internet

---



**YACHAD**



# Using the Internet

- The internet is a system that connects millions of computers worldwide!
- It is really exciting to use, since you have tons of information, videos, music, articles and much more at your fingertips!
- While the internet is a fantastic tool, you need to be **careful** and know how to use it **safely**!

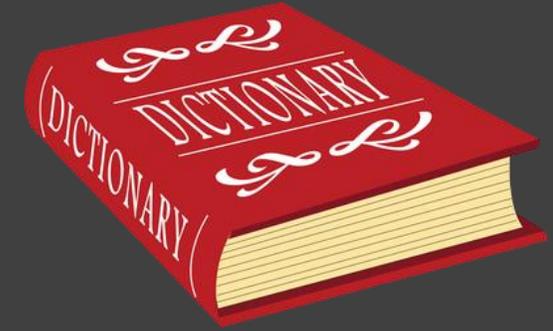


# Goal of This Training

- The goal of this training is to teach you how to be safe and aware while using the internet, so that you can enjoy what it has to offer
- You will learn **7 safety tips** that will help you every time you use the internet, whether you are using an Amazon tablet, an iPad, or a regular computer



# Definitions



Here are the meanings of some words that we will talk about in the training, that you may not be familiar with:

- **Attachments:** An electronic file sent with an email. This file could contain pictures, videos, documents or malware
- **E-Mail (Electronic Mail):** A way to send messages back and forth using the internet
- **Friend Request:** When someone asks permission to see what you are writing or posting on the internet
- **Internet:** A system that connects millions of computers worldwide
- **Link (short for Hyperlink):** A picture or text that brings you to other documents or websites by clicking or tapping on it
- **Malware:** Computer programs designed to damage or steal information from a computer or other electronic devices. A computer virus is a type of malware
- **Online:** Another word for using the internet
- **Posting:** Putting something on the internet, like a picture or something you wrote
- **Social Media:** Websites and applications (apps) that people use to:
  - Connect with others
  - Create and share content such videos, music, photos and opinions
- **Website or Site:** A connected group of pages on the internet that focus on a particular topic, and are run by one person or organization
  - For example, amazon.com or google.com

# What is Social Media?

- Social media is mentioned a lot when talking about the internet, but what is social media?
- Social Media refers to the websites and applications (apps) that people use to:
  - Connect with others
  - Create and share content such videos, music, photos and opinions



- Examples of social media are:
  - Facebook
  - YouTube
  - WhatsApp
  - Instagram
  - Tumblr
  - Tik Tok
  - Twitter
  - Skype
- Participating in social media is a very common way to use the internet. To join social media platforms, people must first sign up for an account

# Safety Tip #1: Check Your Privacy Settings

- If you create an account on social media sites (for example Facebook, Twitter, Instagram) they may automatically allow anyone, **even people you do not know**, to see what you are writing or posting
- You will want to change this, since you do not want strangers knowing your business
- To make this change, go to the Privacy section in the settings of these sites, and mark that you only want people you know (“friends”) to see what you are doing
- Make sure to check your privacy settings every few months, since the sites may change their privacy policy without you realizing
- If you need help doing this, someone at Yachad would be glad to show you how!



# Safety Tip #2: Beware of Friend Requests and E-mails from Strangers

- A “Friend Request” is when someone is asking permission to see what you are writing or posting on social media sites
- This can be a fun way to share your pictures or thoughts with the people you know and like
- But you **Do Not** want strangers to see your pictures or thoughts
- A good rule is to only accept “Friend Requests” or messages from people who you are friends with in the real world
- You also need to be careful of e-mails from strangers
- Never click on any links or attachments in an email from someone you do not know!
- These could contain malware, which are programs that could make your computer run very slowly or stop working well, or can allow strangers to see your personal information



# Safety Tip #3: Think Before You Post

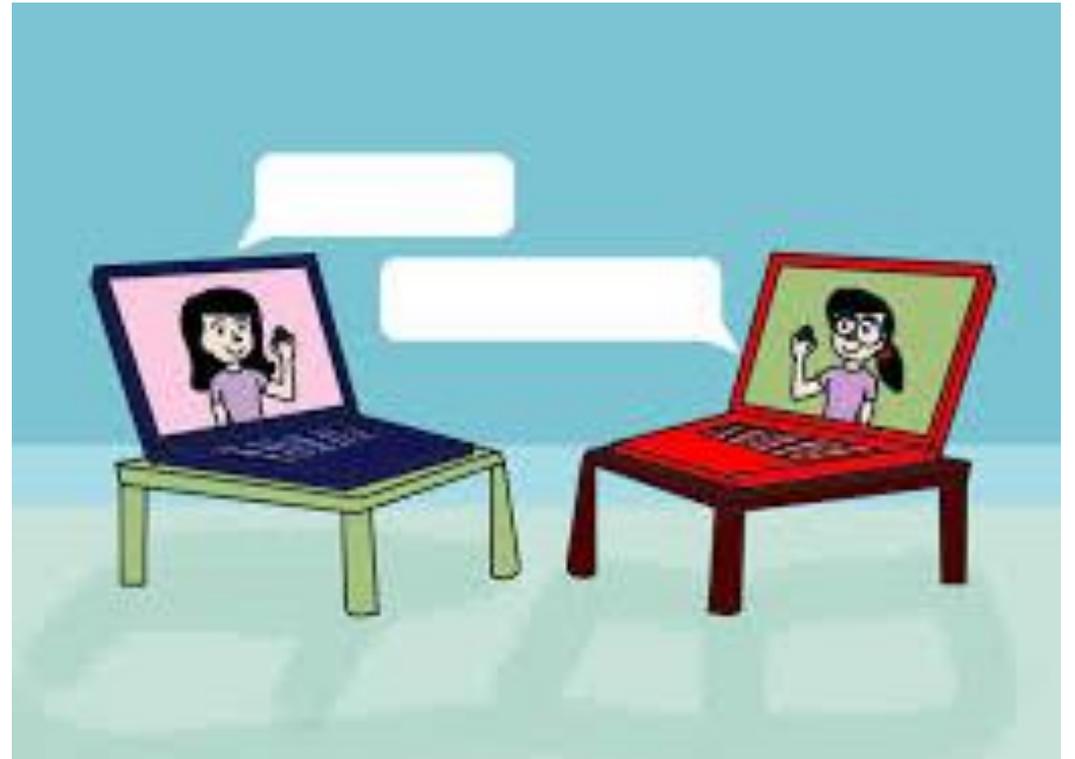


It is useful to know that once something has been put on the internet:

- It can never be permanently erased
- It can be seen by many, many people
- A good guide is to only post things that you would be happy with other people seeing and knowing if you were with them in person
- It is also very important not to post or share private information, such as your phone number, address, social security information, bank account number, or credit card number
- If you want to tell someone your phone number or address, do it over the phone, by a secure e-mail, or in person. **Do not** post it on the internet!

# Safety Tip #4: Never Meet Up With Someone Who You Have Only Become Friends With Online

- If you meet someone **new** on the internet, it is very important that you do not meet up with him or her in person
- You do not know this person well, and he or she could be dangerous
- However, friends who you **already know**, like those from work, a program, or school, can be fun to both chat with on the internet and to meet up with in person



# Safety Tip #5: Don't Believe Everything You See or Read

- Don't believe everything you read or see on the internet
- People could post that it is raining green eggs and jellybeans, but that does not make it true
- Make sure any information you are getting is from a person or organization that you trust and know to be truthful



# Safety Tip #6: Only Use Secure Websites



- Just like physical buildings have an address, websites have online addresses too
  - These addresses are called URLs
- The same way you make sure a building is safe before going into it, you also need to make sure a website is safe before sharing any of your personal information on it
- Before shopping, paying bills, or banking online, check that the website is “secure”
  - “Secure” means the information you are giving to the website is protected, and that no outside person can eavesdrop or steal your information
- You can tell if a website is secure by looking at its address
- A secure website’s URL will start with the letters “https”, and will have a picture of a lock beside it
- For instance, Yachad’s website address is: <https://www.yachad.org>
- The “S” at the end of “https” stands for “secure”. If there is no “S” at the end of “http”, then it’s not a safe site to go into and use!

# Safety Tip #7: Tell Someone You Trust

- If anything happens online that makes you uncomfortable or upset, please tell someone you trust
- For example, if you are being bullied or someone asks you to send an inappropriate picture of yourself, you should go to someone you know and trust for help



# Have Fun But Be Safe

- You can do a lot on the internet!

For example:

- You can connect with friends or family who live in a different state or even a different country
  - You can learn a new skill, like how to knit
  - You can Join a Yachad Virtual Program
  - You can find out the weather or the number to your local pizza place
- 
- But remember you still need to be careful and safe!
- 
- Follow the safety tips and rules that we just taught you and enjoy!



# Internet Safety Quiz

Let's see what you learned! I'm going to ask you some multiple-choice questions about internet safety.



# Question #1

You just bought a new cell phone and want to let your friends know your new number.

What should you **NOT** do?

- A) Post your new cell phone number onto your Facebook and Twitter accounts
- B) Send an email to your friends with your new number
- C) Call your friends on your new phone to say hi and tell them your new number



**The answer is A. You do NOT want to post private information like your phone number on the internet.**

## Question #2

Someone keeps posting messages to your Facebook page saying that you are a liar and a thief.



What **should** you do?

- A) Ignore the posts and hope the person will leave you alone
- B) Post your own nasty and mean messages to that person's Facebook page
- C) Tell someone you trust about the situation and ask for help

**The answer is C. Speak to someone you trust. They can help you to "block" that person from your Facebook page or to report their activities to Facebook.**

# Question #3

A friendly looking woman who you do not know has sent you a friend request.

What **should** you do?

- A) Accept her friend request and start chatting with her
- B) Do not accept her friend request
- C) Send her a message asking who she is



**The answer is B. You do not know this woman, and just like you wouldn't speak with strangers on the street, you don't want to speak with strangers online.**

## Question #4

You just signed up for an Instagram account, and are excited to use it, but to be safe before you start posting, you first need to:

- A) Get a professional picture taken for your profile page
- B) Figure out how to upload videos from your phone
- C) Check the privacy settings on your account



**The answer is C. You want to make sure that your account is private, so that people you do not know cannot see what you post.**

# Question #5

You have become friends with someone you play video games with online, and that person wants to meet up with you for coffee.

What **should** you do?

- A) Politely tell the person, "No thank you"
- B) Schedule a time to meet up with your friend at your favorite coffee shop
- C) Suggest you go out for dinner instead



**The answer is A. If you only know this person from the internet, it is not safe to meet up with him or her in person.**

# Question #6



You read on the internet that mayonnaise is better than sunblock at stopping sunburns.

What **should** you do?

- A) Buy a large supply of mayonnaise for the summer
- B) Look into whether mustard can protect your skin as well
- C) Find out where this information is coming from and if it is a trustworthy source

**The answer is C. Just because something is posted on the internet does not make it true! You need to find out where the information is coming from and if that source is honest and reliable.**

# Question #7

You want to buy a really nice shirt that you saw for sale on a store's website.



What **should** you do?

- A) Get your credit card out and start entering its number into the website
- B) Check the website's URL to see if the site is secure before entering in any payment information
- C) Look through the store's website some more to see if there are any other sales

**The answer is B. You want to make sure the store's website is secure, by checking that its address starts with "https", and that it has a picture of a lock besides it. Once you are sure the site is safe to use, then you can enter in your credit card number.**



Thank you!



- Thank you for taking the Internet Safety Training today!
- You did an excellent job learning how to keep yourself safe while using the internet!