

# Participate safely and responsibly online

26 minutes

In this learning path, you will be introduced to the safety risks you can face while using the internet. You will learn about online scams and how to avoid them. You will also learn about best practices for sharing information online. In addition, you will be introduced to cyberbullying.

## Online safety and privacy

17 minutes | 8 units

In this module, you will learn about some of the safety risks that can affect you when you are using the internet, and tips for staying safe and keeping your information private online.

### Protect yourself from phishing

3 minutes

#### Protect yourself from phishing

While there are many positive things we can do online, we should always be aware of the safety risks. There are many scams that online predators use to access people's information online.

You should be aware of these scams so that you can do your best to avoid them. **Phishing** is a common online scam that you should be aware of.

**Watch the following video to learn more about phishing and how to protect yourself from this online scam.**

#### [Video: Protect yourself from phishing](#)

The internet brings us many possibilities. We can talk to others, make purchases online, and do personal business from one place. But these online interactions aren't always safe. Let's talk about a popular online scam that you should be aware of.

A common way to catch a fish is to put food on a hook so the fish will want to eat it. Once they bite the food, they will be hooked. Phishing scams on the internet work the same way. People who want to steal your information are like fishermen. They send you an email or instant message through social media site or an online game. They often pretend to be someone they aren't and ask you for private information or they tell you to click a hyperlink, so you can complete an important task. If you give them the information or click the hyperlink, you will be hooked. But don't worry. These four practices can help protect you from phishing scams.

Practice number one, be careful of suspicious messages. Scammers try to make their messages look official and familiar, so you trust them. Think twice when you receive a suspicious message and avoid sharing personal information over message or email. This includes your home address, bank information, passwords, and more. Don't click on a link or download a file if you don't know or trust the sender.

Practice number two, look for signs that a webpage is safe and secure. Before you provide credit card info, enter a password or provide other personal info, verify that you are on a trusted secure website. Most secure websites have the prefix https at the beginning of the URL in the browser address bar. Additionally, make sure you are on the right webpage. Scammers often try to lead you to webpages that appear to be official and use misspellings of company names to trick you. www.microsoft.net is not the same as Microsoft's official website at [www.microsoft.com](https://www.microsoft.com).

Always check the URL to make sure you're on the right webpage.

Practice number three, keep your web browser and operating system up to date. You can turn on automatic updates to make sure the latest software releases are automatically installed on your computer. Keeping your device software up to date means you will receive the latest security updates that help to protect your computer.

Practice number four, install verified anti-malware software on your devices. This is special software designed to protect your computer from harmful software and hackers. Don't be the next fish to get hooked. When you use the internet, remember to think before you click, download, or share to protect yourself from phishing scams online.

## Communicate safely online

2 minutes

### Communicate safely online

The internet allows us to communicate with other people in new ways. However, it isn't always safe to communicate with other people online. You don't always know for sure who you're talking to when you're on the internet, so you have to be careful to stay safe.

**Watch the following video to learn how to communicate safely online.**

### [Video: Communicate safely online](#)

Using the internet, we can communicate with other people across the world in new ways. This has many benefits, but there are also some dangers. There are online predators using the internet every day. These predators often pretend to be people they aren't. So, it can be hard to know who you're talking to online. Here are three tips you can use to keep yourself safe from online predators when communicating online.

Tip number one, Use your instincts. If someone makes you feel nervous or uncomfortable, stop communicating with them and tell someone you trust immediately. Most websites and social media sites have tools that you can use to report suspicious activity.

Tip number two, Limit what you share. Online predators often try to get you to share your personal information through emails and messages. Avoid sharing personal information with an online stranger.

Tip number three, Keep your distance. Think twice about meeting someone in person that you have only talked to online. Online predators often use social media to pretend to be someone else by setting up fake profiles using other people's pictures. Even if someone seems friendly, it can be hard to know for sure who you're talking to online. Always tell a parent or someone you trust when an online stranger asks to meet you in person, so you don't end up in a dangerous situation. Many online predators use smart tactics to lure you into dangerous situations, but you can be smarter. Keep these risks and tips in mind, so you can stay safe when you talk to people online.

## Create strong passwords

2 minutes

### Create strong passwords

A big part of staying safe and keeping your information private online is protecting your information, your accounts and your computer using strong passwords.

**Watch the following video to learn how to create strong, effective passwords that can protect your information.**

#### [Video: Create strong passwords](#)

Passwords help protect your personal information and accounts from other people. A password is as important as the lock to a door. You want a strong lock that is hard to break and will keep dangerous people from coming inside. You also don't want anyone to find the keys to your lock. A strong password is like a strong lock for your account, you want it to be difficult for others to guess, you also want it to be safe and secure so others can't find it. Follow these tips to create strong passwords and keep them safe.

Tip number one, Use a combination of letters, numbers, and symbols in your password. Using a combination of uppercase and lowercase letters and characters and adding numbers can improve the strength of your password.

Tip number two, avoid using common words in your password. This includes common words and phrases like password or website, as well as personal keywords like your birthday, your

name, or your hometown. Hackers can easily guess these phrases in your password. A unique combination of characters and numbers creates a stronger password.

Tip number three, Use different passwords for different accounts. If someone guesses your email password, your safety and privacy may be in trouble if you use the same password for your bank account. Instead use different passwords for each online account you have.

Tip number four, your password is for you only. When you share it with others even friends and family, it is more likely that someone else will use it or won't keep it safe. Keep your passwords to yourself. When you log into accounts, make sure you log out when you're done, and don't save your login information on a public computer.

Additionally, avoid doing personal business on public computers and public networks, this makes it easier for hackers to access your information. Remember, using strong passwords and keeping them secure is important for your online safety and privacy. Keep these tips in mind when you create a new password. strong passwords

## Describe best practices for sharing information online

2 minutes

### Be smart when you share

When we go online, we can often do many things that threaten our safety without thinking a lot about it. It's important to think twice about what you share online and keep your safety in mind.

**Watch the following video to learn more about the risks of oversharing online.**

### [Video: Oversharing online](#)

The internet and the web make it possible for us to stay connected with friends and family across the world. We can use social media and other platforms to see what's happening in our friend's lives, share personal news, and stay in touch with others, but sharing things online, isn't always safe.

Consider this scenario, Harold gets a new car and wants his friends to see it. So, he posts a picture of it on social media. This might seem okay, but the picture includes a lot of personal information about Harold. Anyone can see his license plate number, what kind of car he's driving, and where he lives from one picture.

This might be okay for his friends to see it, but it can be dangerous if the wrong person finds this information and wants to use it in a bad way. It's important to keep safety and privacy in mind when you share things online.

When you set up profiles on social media websites, be sure to review the privacy settings of your account. If your account is set to public, anyone can see your information and what you share. Instead, use the private setting on accounts, so that only your personal connection can see what you share.

You should also be selective when you accept invitations to connect with someone via social media. Most social media platforms have a way for you to accept and deny requests, to have someone be your friend, or follower on the site. Once you accept someone, they have direct access to your profile and the things you share. Keep this in mind when you receive a request, and make sure you only interact with people you know and trust.

Even when you control who has access to your profiles and accounts, you can't control what other people do with your information. When you share something online, you can't erase it. Never share something online that you wouldn't want strangers and the public to see it. Always remember to think before you share. Keep your safety in mind and make smart choices when you share things online.

## Try it yourself

What did you learn from this video? Write down 1-3 things you will keep in mind when you share personal information online.

## Describe the importance of managing your digital footprint

3 minutes

### Your digital footprint

There's a lot we can do online, from browsing the web, to sharing updates on social media, to making online purchases. You should keep in mind that everything you do online becomes part of your online history, or your **digital footprint**.

You should think about your digital footprint when you share information or do things online because things that happen online are difficult to erase.

**Watch the following video to learn more about your digital footprint and how to manage it.**

### [Video: Manage your digital footprint](#)

If you use the internet, you should be aware of your digital footprint. Just like physical footprints that show someone steps on a dirt path, your digital footprint is a history of all the activity you do online. Any social media posts you make, any websites you visit, and any information you share online contributes to your digital footprint.

Once you post something online, it can't be erased. So, your digital footprint can last forever. This can be a good thing if your digital footprint includes things that give you a positive

reputation online. This can help you build your personal brand. Your online history can also help the apps you use know more about you. They can use this information to serve you better by adjusting to the things you like and your daily habits. But they can also use this information in the wrong way and share it with others. Keep the following tips in mind when you go online to manage your digital footprint.

Tip number one, know what your footprint says about you. Other people use your digital footprint to make judgements about you online. This can include employers when you apply for a job or recruiters when you apply for academic programs. It's important to know what your digital footprint says about you and how your information is being used. To see what your personal brand is online, you can search for yourself. Search for your name in the Bing search engine and see what results are displayed. If these results don't show what you want, think about what you share online and what information you allow other people to see.

Tip number two, Manage your privacy settings. You can modify the privacy settings of most of the social media sites and online applications that you use. This can help you control who sees what you share and what information shows up when someone searches for you online.

Tip number three, Manage your cookies. Cookies are notes given to your web browser as you browse the web. These cookies help apps track information that they need while you're using the app. This can help the app work better for you. But this data also contributes to your digital footprint. You can use the settings in your browser to limit or block the use of cookies on certain websites.

Tip number four, think before you share. Once you share something online, you can't take it back. Make sure you're okay with something being a part of your public digital footprint before you share it. Your digital footprint can live forever. Keep these tips in mind to make sure you're happy with your digital footprint and how it is used.

## Knowledge check

3 minutes

1. Which of the following components should you look for in the URL of a webpage, to make sure you're on a secure site?
  - http
  - secure
  - **https - Correct! "https" means the webpage is secure.**
  - ssh
2. Which of these passwords is the strongest?
  - **John@453 - Correct! This password contains uppercase, lowercase, special character and numbers.**

- john500
- JoHn300
- 125893

3. Your digital footprint is:

- The size of information in your online accounts.
- The number of people you're connected to online.
- **A record of everything you do and say online. - Correct! Your digital footprint makes it easy to track your actions online.**
- Your online username.

## Summary

1 minute

Congratulations!

You have completed the Online safety and privacy module and now can answer the following questions on your own:

1. What are some dangers of using the internet and the web?
2. What are some signs of safety risks and scams online?
3. What steps can you take to stay safe while using the internet?
4. How can you manage your digital footprint?

## Online civility

9 minutes | 5 units

In this module, you will learn more about rights and best practices for using information online. You will also learn about cyberbullying.

## Introduction

1 minute

We can use the internet to access lots of information and communicate with others, but we have to make sure we're behaving as responsible digital citizens.

In this lesson, you will learn how to responsibly use the internet and the web.

**By the end of this lesson you will be able to:**

1. Describe the rights that people have to information and content shared on the web.
2. Describe best practices for using information found on the web.

3. Describe the implications of treating others poorly on the web.

## Describe best practices for using information found on the web

2 minutes

### Use information responsibly

Although accessing information is easy in the digital world, there are some rules to keep in mind when you want to use information you find online.

**Watch the following video to learn some of the guidelines for using information that you find online.**

### [Video: Use information responsibly](#)

The internet gives us unlimited information and possibilities. We can find anything from funny videos, to our favorite songs, or information on how to solve a homework problem, but we must be responsible with the information we find online.

Consider a scenario. Harold wants to write a cookbook and sell it online. He is not good at taking photos, so he searches for images online. He downloads images of different foods and includes them in his book. This might seem okay because it is easy to do, but this is not a fair or responsible way to use information found online.

When someone puts their original work online including their words, images, videos, music, and more, they become the owner of the content. As the owner, they have certain rights, usually considered copyrights, to decide how that content can be used. If you use someone else's words or work as your own, it is considered plagiarism. This isn't fair to the original author and can get you into trouble. If you want to use someone else's content in your work, be sure to reference them to give them credit for their work.

When you are using someone's work in a product that you are selling, you should first obtain permission from the author. You might also have to pay for a license to use someone's work. Sometimes, the authors of content make their work available for free use.

You can use search engines like Bing to find images, media, and other types of content that are available for others to use. As you use the internet and find information online, make sure you use it fairly and responsibly.

## Describe the implications of treating others poorly on the web

3 minutes



## Cyberbullying

The internet allows us to connect with others online from all across the world. Unfortunately, people don't always treat each other nicely online.

**Cyberbullying** is a type of bullying that takes place over the internet. It can be easy to send mean messages or spread negative rumors about other people, but this can be dangerous for the person who is targeted.

**Watch the following video to learn tips for preventing cyberbullying and being a digital citizen.**

### [Video: Treat others respectfully online](#)

The internet and social media platforms connect us with our friends, family, and peers in new ways. Sometimes people take advantage of these platforms and use them to spread negative messages about others.

Cyberbullying, or bullying that takes place on the internet, can be just as bad as bullying in person. People can use the internet to send mean messages to someone, spread fake rumors, or share someone's private information without permission. When someone is cyberbullied, their feelings can be hurt, and their reputation can be damaged. You cannot always prevent cyberbullying, but you can play a part in making the internet a friendlier and safer place for everyone.

Here are some guidelines you can follow to promote digital civility online:

- Live by the Golden Rule. Treat others the way you want to be treated, whether you're in person or online.
- Avoid sending negative messages and participation in behavior that can hurt someone else.
- Respects differences. We're all different in many ways. When you interact with people online, respect their differences in opinion, experience, and culture. Even if you don't agree with something that another person shares online, you should still treat them with respect and make the internet a friendly space for communication.
- Pause before replying. Before you share anything online, always pause and think about the consequences. Will your message hurt someone else? Will it damage your reputation, or the safety or reputation of others?
- Think twice before sharing online. Stand up for yourself and others. If you feel unsafe online, you should feel comfortable to remove yourself from a situation and report it to someone you trust.

- When you see cruel or dangerous activity online, offer support to those involved, and report the incident to someone you trust. We can all play a part in making the internet a safe and friendly place for everyone.
- Do your part, and be a responsible digital citizen online.

## Knowledge check

2 minutes

1. Which one of these actions is not violating copyrights?
  - Using someone's images in a book you publish without their permission.
  - **Quoting a paragraph from someone's book and referencing them - Correct! You observe the copyrights when you cite the owner.**
  - Selling someone's video under your name.
  - Selling someone's book without a license.
2. Cyberbullying can take place:
  - Only on social media platforms.
  - Only through emails.
  - Only on SMS.
  - **On social media platforms and SMS, and through emails. - Correct! Cyberbullying can take place in any type of online communication.**

## Summary

1 minute

Congratulations!

You have completed the Online civility module and now can answer the following questions on your own:

1. What should you do when you want to use information that you find online?
2. What can you do to prevent or end cyberbullying?

## Print your certificate

2 minutes | 2 units

You must complete all of the modules in this course in order receive your certificate.

## Receive credit

1 minute

### Complete

Congratulations on completing Participate safely and responsibly online. Select **Receive credit** to complete the course and receive your certificate.

### Credit Received

Congratulations on completing Participate safely and responsibly online.

In the box below, please type your name as you would like it to appear on your certificate then select **View certificate**.