

## Introduction to Computers: Module 5



# Introduction to Computers

## Module 5



# Module 5: Online and Computer Safety

## Review

- Connecting to the internet.
- Internet Addressing.
- Using the Browser and Searching.
- Hyperlinks and Bookmarks.

## Topics

- Website security
- Pop-ups and Phishing
- Public WiFi access
- Virus removal and security software
- Dos and Don'ts using the internet
- Google Account setup

## Exercises

- Exercise 1: Secure website access.
- Exercise 2: Security software setup and scans at home.
- Exercise 3: Create a Google account.

---

# 1. Online and Computer Safety

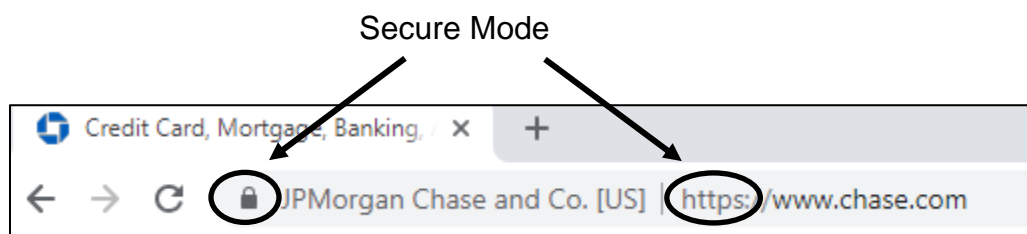
---

## Secure vs Open website access

When your browser connects to a website it starts a conversation between your computer and the website. The internet is shared by many people and the conversation between your browser and a website can be seen by other computers.

The industry has a special secure version of the browser language called **https**. Conversations between your browser and websites using the https language are scrambled and understood only by your browser and the website you're talking to.


You should always check to see if the website connection is secure before you share any personal or financial information. Check for the https reference in the website's URL shown in the address bar. The Google Chrome browser will also show a small lock symbol.




*Figure 1 - Secure website mode*

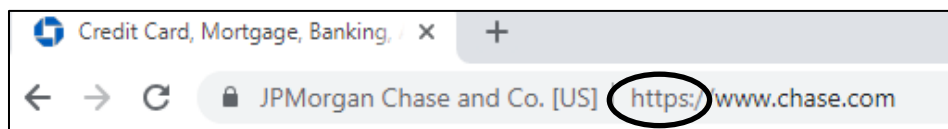
**Exercise 1: Secure website access**

In this exercise, you will open two websites and verify one is **Open** and one is secure.

1. **Open** the Google Chrome browser.
2. **Enter** peoplesrc.org in the browser address bar.
3. **Click**  and the website address will appear.



4. Note the browser says the site is "Not Secure".
5. **Click** on the "+" tab to open a new browser empty webpage.
6. **Enter** Chase.com in the address bar.
7. **Click**  key.



8. Note the browser reports the website communication is secure.
9. **Close** the Chrome browser.

---

## 2. Areas of potential risk

---

When using a computer, there are several areas that you need to give special attention to avoid problems. These include:

### 1. User Names and Passwords

**User names** and **passwords** are used to secure your personal information in your computer and websites.

#### User Names

A website user name can be a unique word or your e-mail address. It is how you are known to the website.

#### Passwords

You should make your website password difficult to guess. You should avoid using the same password to access important websites! You should never use your email password on websites with your personal information.

A good rule is to make a password:

- Eight or more characters long.
- Use at least two capital letters, two numbers, and one special character.

Some good examples are:

- My4@naE5
- L3#asTb6
- j0an44&T
- XX6jj2\*\*

You can also make a strong password by starting with a word or phrase. Then add numbers and symbols. For example, if your favorite song is “Another day in paradise” by Phil Collins then your base word might use the letters “anip”. When you add capitals, numbers and special characters your passwords would look like:

- adipXX23%
- adipA\$11



## Changing Passwords

You should change your passwords on sites with personal information on a regular schedule. This protects you if someone discovers your password. The recommended schedule is based on website importance:

- Banking websites: *every 2 months.*
- Shopping websites: *every 4 months*
- E-mail accounts: *every 6 months*
- All other personal sites: *every year.*

## Storing Passwords

As your list of active password grows, you will need a secure way to store them and refer to them. There are several options with different levels of risk:

- Write them down on a piece of paper in your wallet or purse – *the most risk.*
- Store them in a file in your computer – *less risk but could be found by a virus.*
- Hide them in secret location – *lower risk but difficult to find them when needed.*
- Store them in a smart phone app – *least risk but must be secure.*

## 2. Internet Pop-ups and Phishing

### Internet Pop-ups

A **pop-up** is a web page or window that unexpectedly appears while viewing a webpage. Most pop-up are helpful but some can be dangerous. Viruses can hide in very real looking pop-ups and make you believe that you must act immediately.

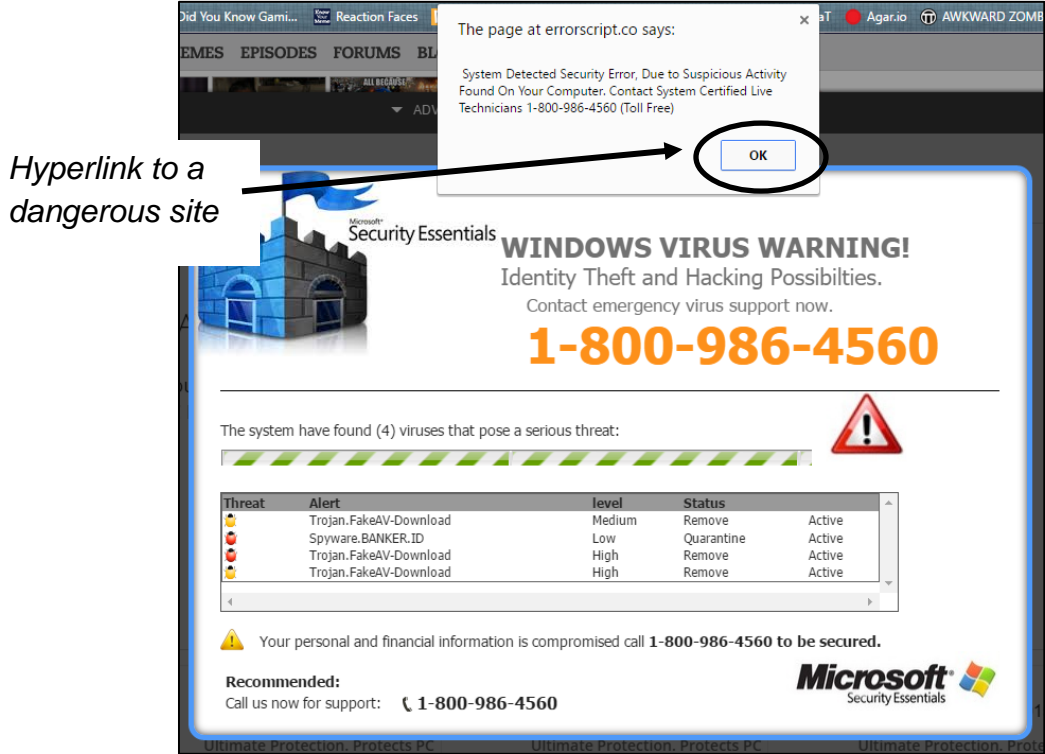


Figure 1 - Sample dangerous Pop-up window

In some cases, these pop-ups can disable your browser and force you to shut down your computer!

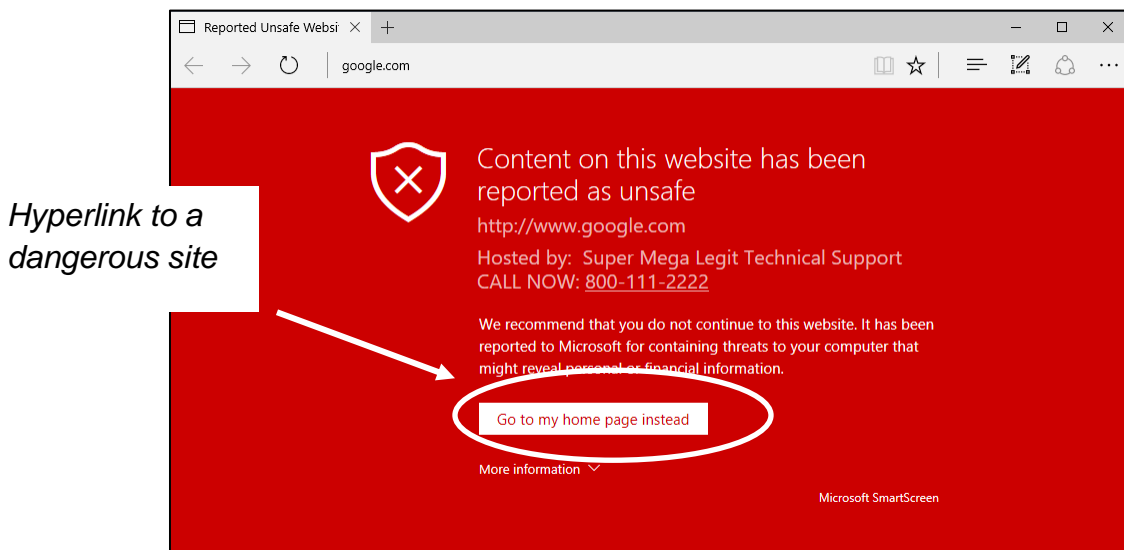


Figure 2 – Dangerous pop-up example

Never click on a Pop-up hyperlink! If the pop-up window will not close using the windows controls, you will have to close the browser window and or restart your computer.

## Phishing

**Phishing** is a special email or website page that looks real but is made to steal your passwords and other personal information.

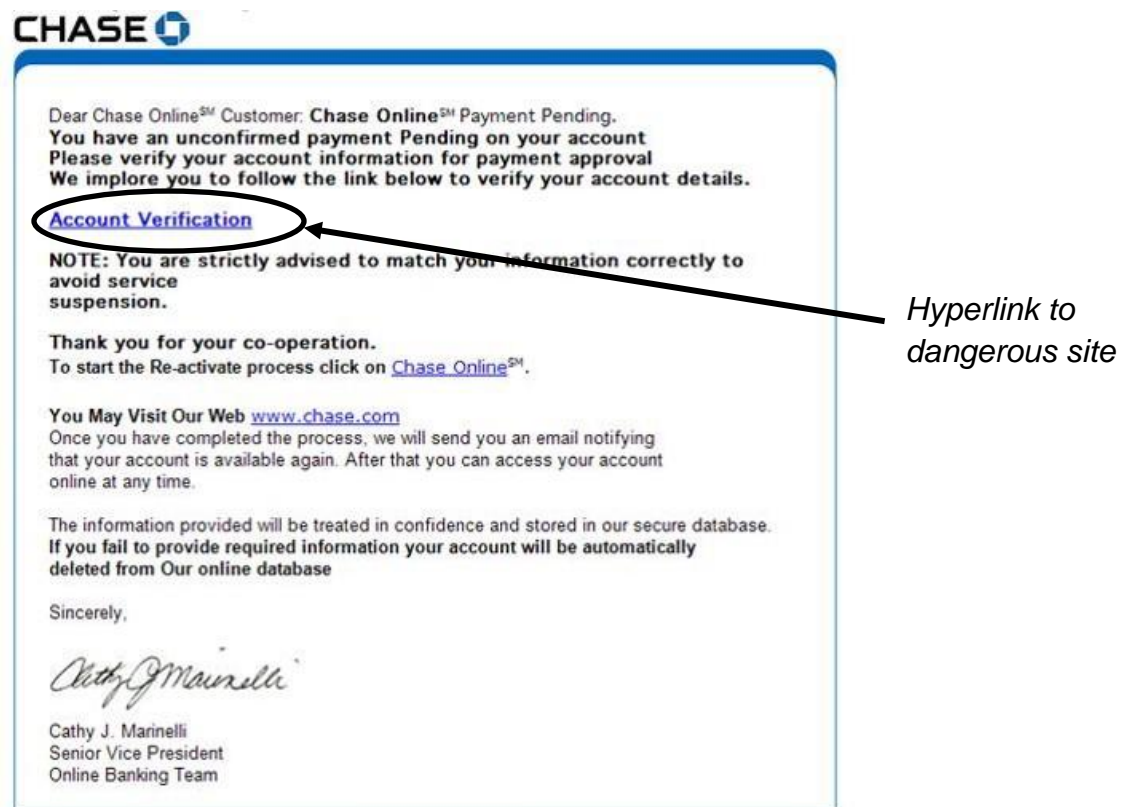


Figure 3 - Phishing example

No bank will ask you for your user id and password other than an account logon.





### 3. WiFi Access in Public Locations

Most public places have a WiFi service available for general use. Usually the WiFi service does not require a network password.

A good rule is never to share your personal information including passwords, banking, or personal information in a public location!

### 4. Virus Protection

#### Computer Virus

A **computer virus** is a computer program designed to infect and damage your computer. It can steal your personal information. A virus can spread from your computer to other computers.

Viruses do not start in your computer. *You help them to be received and installed.* Once your computer receives a virus it cannot be removed unless you use virus removal software.

#### Spyware Virus

Some viruses are called **Spyware** because they hide in your computer and act like a tape recorder. They listen to the keys you press and track the websites you visit. Later they share your information with criminals.

#### Sources of Viruses

Most of the viruses are found on the internet. Viruses from the internet are unexpectedly received by your computer when you click on a dangerous hyperlink or download an infected attachment from an email. Viruses can be received from a removable drive, DVD, or CD when the device is opened by your computer.

## Virus Removal

Viruses are removed from your computer by using special **virus removal** software. Virus removal software keeps an updated list of all the viruses that might be on your computer. The software scans your computer's file system looking for the virus infected files. If it finds one, it removes it from your computer.

Scanning for viruses can be automatic or manual. Most virus removal software has both options.

## Security Protection

Virus removal software also includes **security protection**. Security protection watches your internet connections and looks for viruses as they are received. The software can alert you when a virus is received or when you are connecting to a known unsafe website.

There are several security software and virus removal products available:

Product	Annual	Comment
<b>Norton</b>	\$55	Rated best in the industry.
<b>McAfee</b>	\$35	Some weakness but very good.
<b>Kaspersky</b>	\$50	A bit overpriced for the features.
<b>Webroot</b>	\$60	Good but overpriced for features.
<b>Windows Defender</b>	\$0	Adequate and Included in Windows 10; supported by Microsoft.

## Virus Safety

To protect from receiving a virus you should:

1. Check every webpage hyperlink before you click it!
2. Don't download an email attachment unless you know what it is.
3. Don't react quickly to unexpected messages; remember the Phishing examples.
4. Manage your passwords, and don't share your computer password.

## Windows Defender

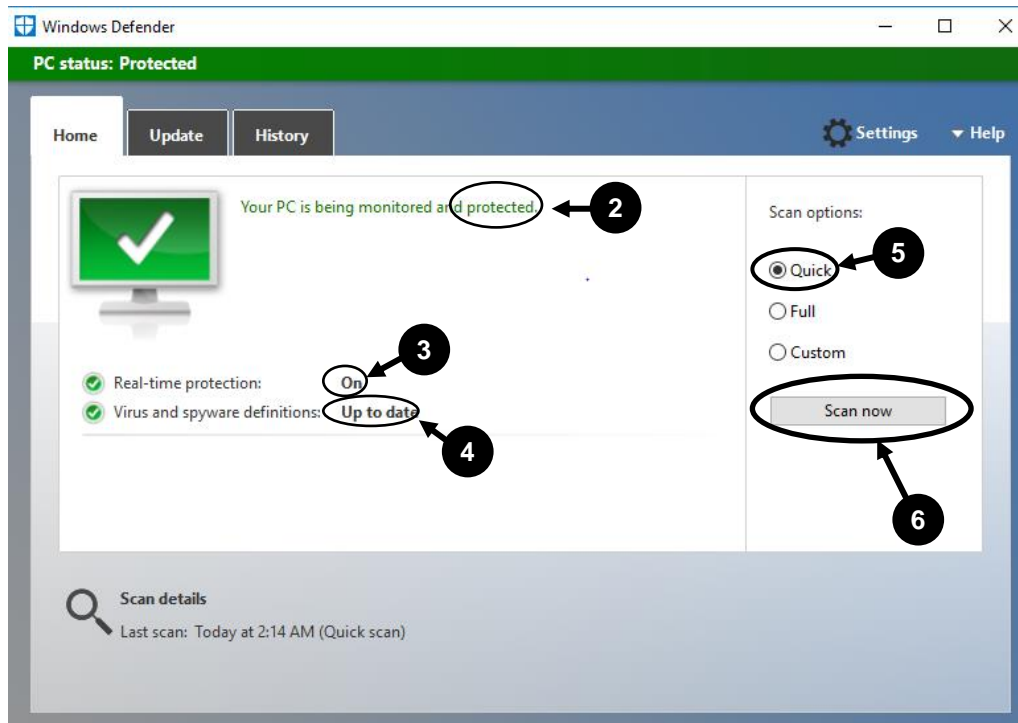
We will look at **Windows Defender** because it is part of Windows 10. There is no restriction on how many Security software products you can have on your computer. Many professional computer users have one or more vendor security products in addition to Windows Defender.

**Instructor Note:** Windows Defender is not active on the Training Server. Students should be advised to complete this exercise on their home computers. You can point out where the virus definition status and the scan options are referenced on the display.

### Exercise 2: Security software setup and scans

In this exercise, you will open the Windows 10 Windows Defender application and review the security features.

1. From the Desktop **click** the magnifying glass in the Task Bar and **enter** "Windows Defender". The Windows Defender application will appear.





2. Confirm that the computer Status is **protected**.
3. Confirm that the **Real-time time protection** is **on**.
4. Confirm that the Viruses and Spyware definitions are **Up to date**.
5. Confirm that the scan options are set to a **Quick**.
6. **Click** the **Scan now** button and confirm that the computer files are being scanned for Viruses and Spyware. Note the number of items (files) being scanned.
7. Click the **Update** Tab.
8. Confirm that the Virus and Spyware definitions are up to date.
9. Verify the data of the definition creations and update date are current.
10. Click the **History** Tab. (Note that you can view the list of quarantined files and all detected items.)
11. Close the Windows Defender application.

---

## 3. Dos and Don'ts using the Internet

---

Whether you are a new computer user or have years of experience, you will avoid problems if you follow this advice.

### ***General advice ...***

1. Everything you share on the internet is public.
2. You will catch a virus, so scan your computer frequently.

### ***You should ...***

1. *Use a different password with websites holding personal information.*
2. *Use virus protection software.*
3. *Think before you share information or click a hyperlink on a website.*
4. *Only shop online using secure sites.*
5. *Block and ignore Internet pop-ups.*
6. *Be wary of public WiFi.*
7. *Know that Apple computers are as vulnerable as Microsoft computers.*
8. *Use passwords to unlock your computer.*
9. *Be very careful using auction sites.*
10. *Keep your computer software current.*



## ***You should never ...***

- 1. Click on a hyperlink to an unknown website.*
- 2. Reuse your email password on other websites.*
- 3. Assume banks will pay you back.*
- 4. Store your credit card details on websites.*
- 5. Let someone use your computer with your password.*

---

## 4. Create a Google Account

---

Module 6 requires that you to have a **Google account**. If you already have a **Gmail account**, you can skip this exercise. If you do not have a Google account, you can create one by following the steps below. If you need more help, please attend one of the PRC's Open Training sessions before the next class.

Your Google account can be used after these lessons so don't forget your Username and Password.

**Instructor Note:** Each instructor will need a Google account to participate in the student exercises. Your Google account name should be of the form "[prcxxxxx@gmail.com](mailto:prcxxxxx@gmail.com)" where "xxxxx" is your volunteer number. Remember to remove all e-mails and files created during any previous class sessions before you start Module 6.

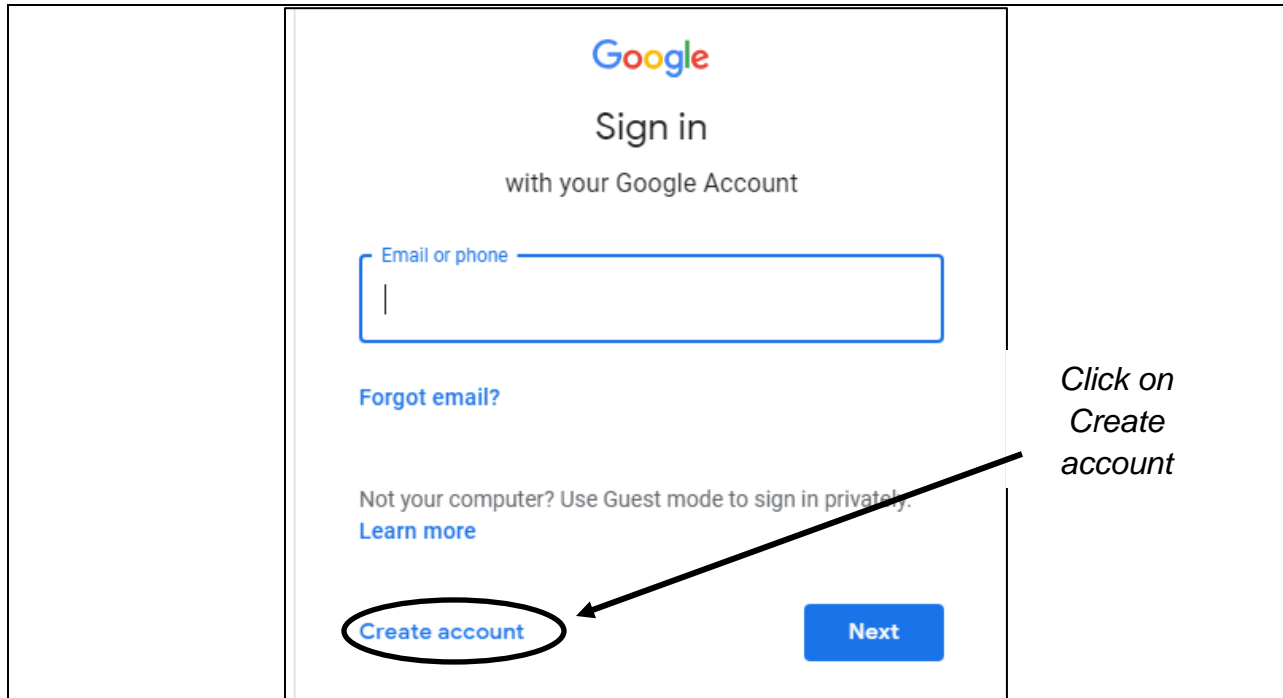
### Exercise 3: Create a Google account.

In this exercise, you will create a Google account to be used during the next session.

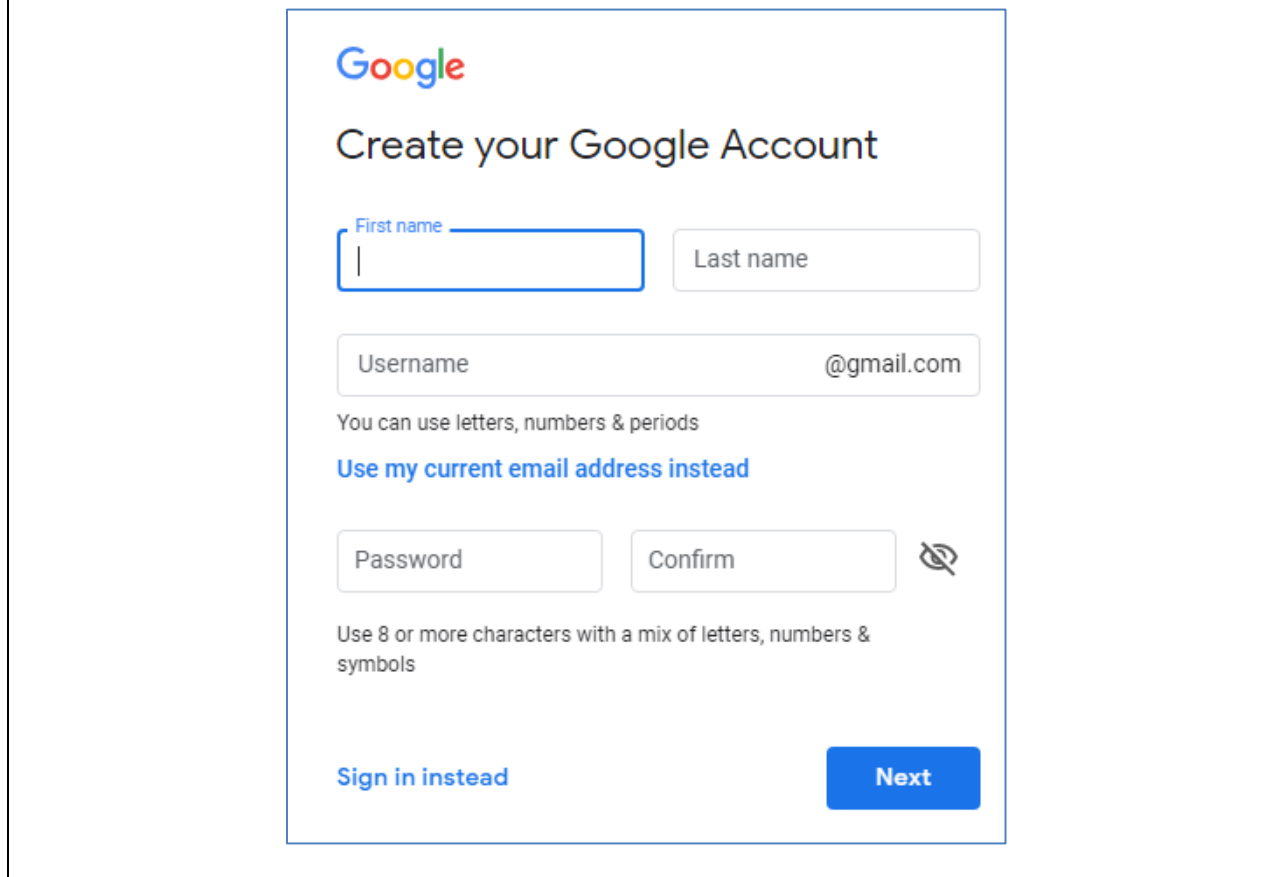
1. **Open** the Chrome browser.
2. **Click** the link Images in the upper right corner of the browser window. The Sign in button appears in place of the Images link.



3. **Click** the Sign in button and the Google Sign in page appears.

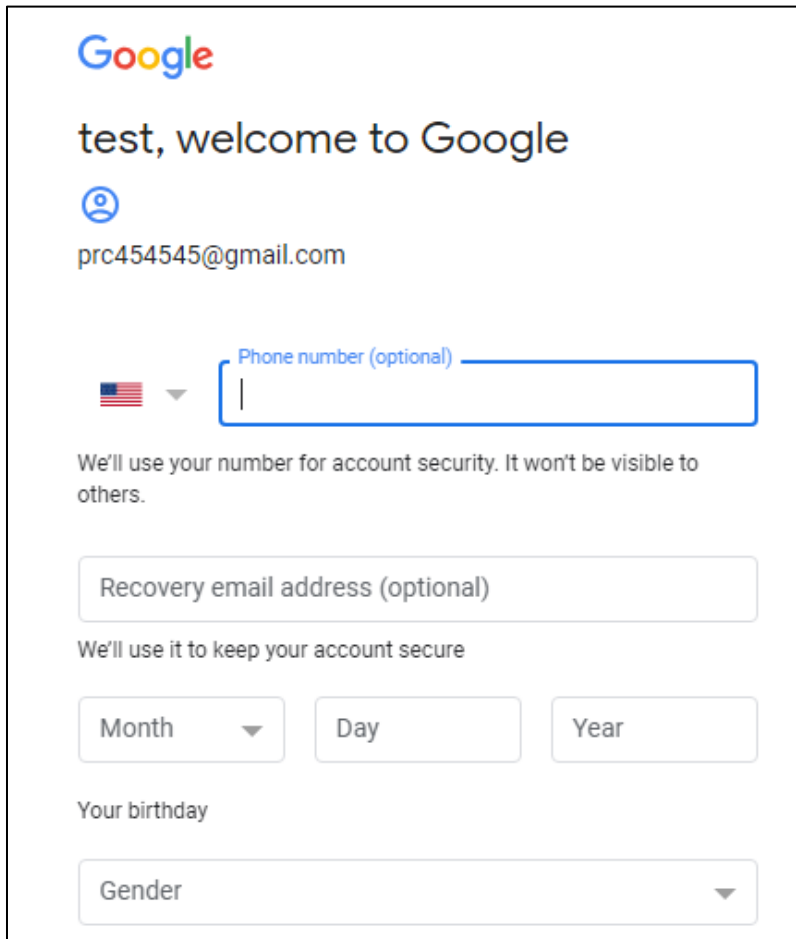


4. **Click** the Create account link. The “Create you Google Account” page appears.

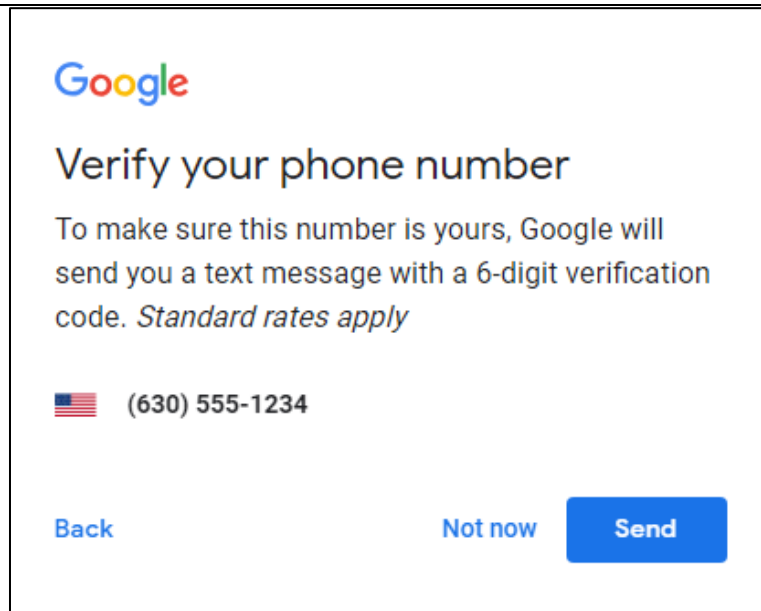




5. **Enter** your first and last name. For the username, use “prcXXXXX” where “xxxxx” is your Training Server login ID without the “S”.
6. Complete the remainder of the page including the password. **Do not forget the password!**
7. **Click** the Next button and the following page appears.

A screenshot of the Google account creation page. At the top is the Google logo. Below it, the text "test, welcome to Google" is displayed. A profile icon placeholder is shown above the email address "prc454545@gmail.com". There is a section for a phone number with a dropdown menu for country (currently showing the US flag) and a text input field labeled "Phone number (optional)". Below this is a note: "We'll use your number for account security. It won't be visible to others." There is a text input field for "Recovery email address (optional)" with a note below it: "We'll use it to keep your account secure". The birthday section includes three input fields for "Month", "Day", and "Year", with the label "Your birthday" above them. At the bottom is a dropdown menu for "Gender".

8. **Enter** your cell phone number and current email address. These are important if you forget your password!
9. **Click** the Next button when you are done entering the information. The following page appears.



10. **Click** the Send button to confirm your cell phone number. You will receive a text on your cell phone from Google. Respond with the verification code.
11. After your cell phone number is verified, you are asked to agree to the terms and conditions of using Google services. Accept the terms and conditions.
12. You now have a Google account. We will use the Google services in Module 6.
13. Remember to bring your Google account password to the next two classes.



---

## 5. Quiz / Review

---

1. Why is website security important?
2. What is the risk of responding to pop-ups and phishing screens?
3. What do you need to think about when you use a public WiFi connection?
4. Is it possible to completely avoid viruses and how do you remove them?
5. Which of the internet "Dos and Don'ts" are you most likely to do?