Internet Safety

Objectives

After completing this class you will be able to:

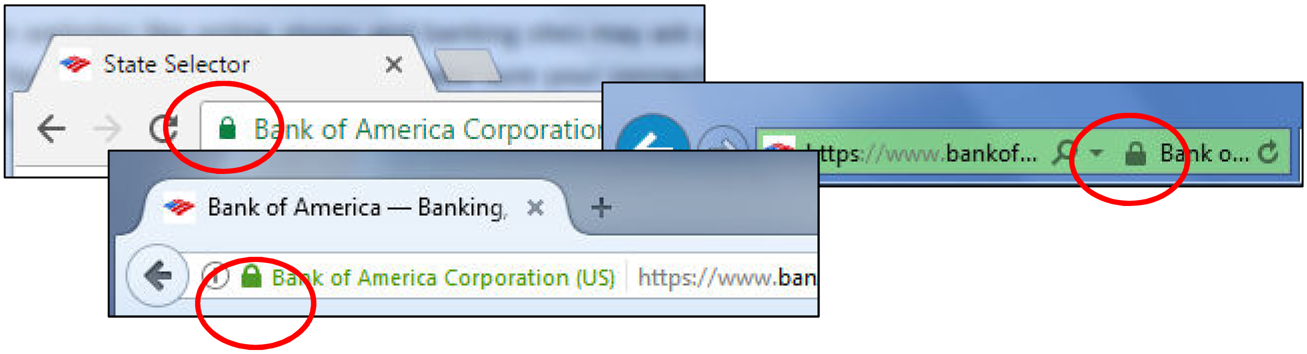
- Create strong passwords
- Identify spam and phishing schemes
- Define malware and other risks
- List basic tips to staying safe while online

Introduction

With the internet answers to just about any question can be found in seconds. While the internet offers many conveniences for modern life, it can also present certain risks that you should be aware of. While the internet is a great tool for things like keeping in touch with old friends and shopping online, it is also a popular tool for cybercriminals and identity thieves. In this class, we'll review the common risks presented by the internet and show you some techniques you can employ to avoid the danger.

Secure Connections

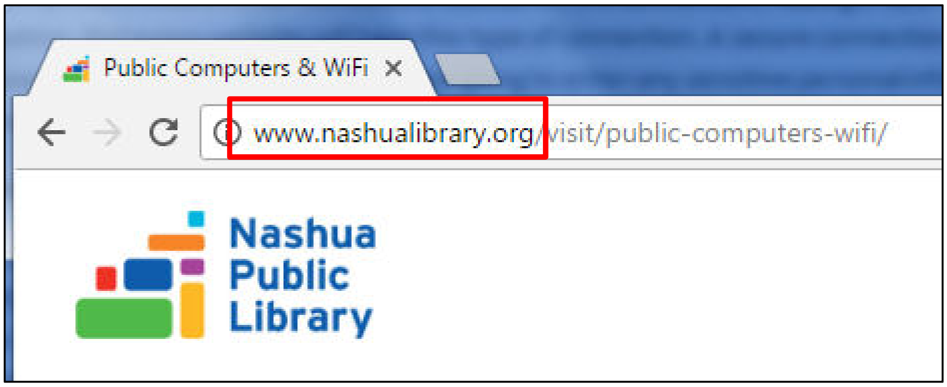
Certain websites like online stores and banking sites may ask you to enter sensitive information. On these types of sites, it is important to make sure your connection is secure. To see if a connection is secure, look for a **lock symbol** in the address bar before the web address.


State Selector
Bank of America Corporation
https://www.bankof...
Bank o...
Bank of America — Banking,
Bank of America Corporation (US)
https://www.ban

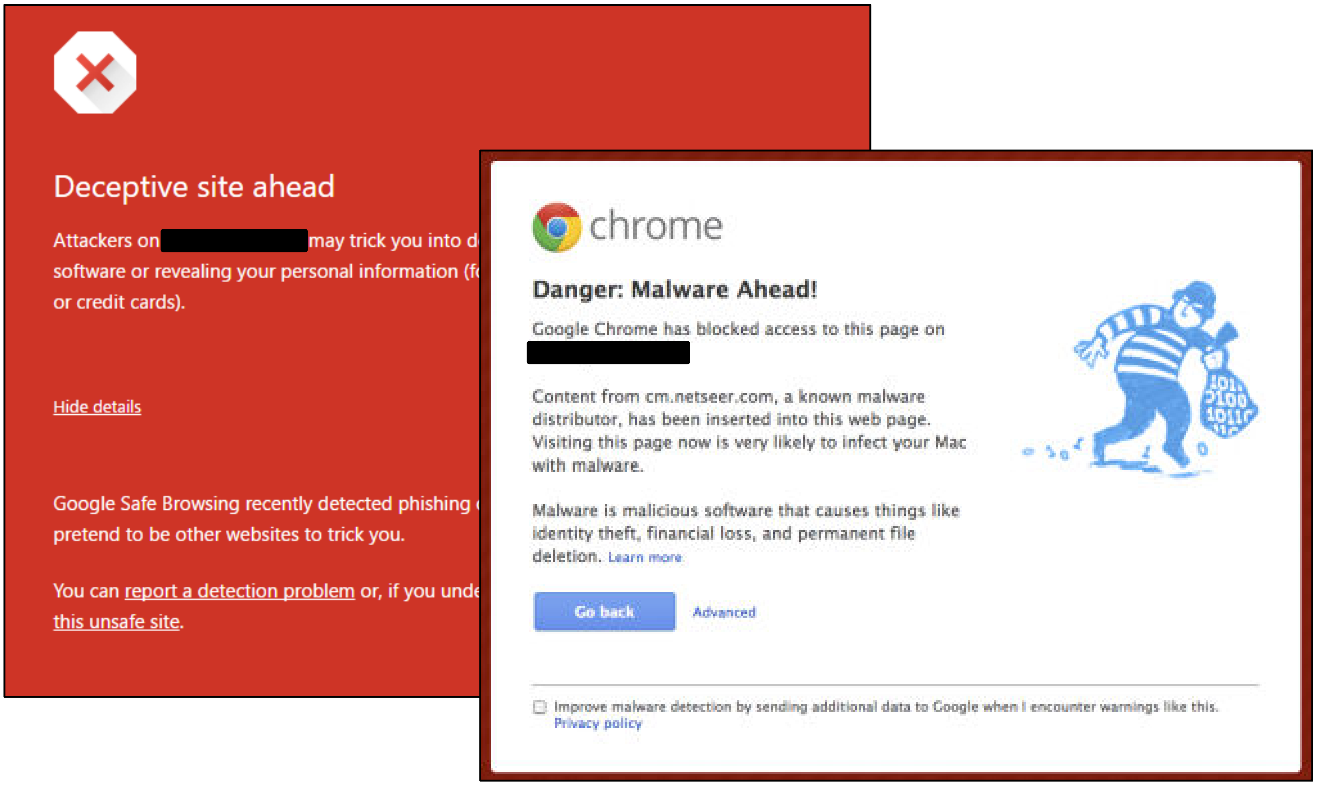
The lock symbol indicates that the website uses an HTTPS connection, making it safe to enter personal information. Not every website will have this type of connection. A secure connection is not required for every website. But make sure that if you are going to enter any sensitive personal information, that the website has an HTTPS connection.

Domain Names

When browsing for websites online, double-check the domain name to make sure a site is legitimate. Like phishing email links, a malicious site may have a similar name to trick visitors into thinking they are on the right page. To protect yourself, stop and look at the domain name in the address bar. Most browsers like Chrome, Firefox, and Internet Explorer will make the website domain more visible by making it black, while the rest of the website address is in gray. This is just one feature that helps you stay safe.


Public Computers & WiFi ×
www.nashualibrary.org/visit/public-computers-wifi/
Nashua
Public
Library

Also if you try to access a website that the browser thinks contains malware or malicious content, you will likely get a message one shown below. It will vary depending on the type of threat and the browser you are using.



Deceptive site ahead

Attackers on [redacted] may trick you into d
software or revealing your personal information (f
or credit cards).

Google Safe Browsing recently detected phishing
pretend to be other websites to trick you.

You can report a detection problem or, if you unde
this unsafe site.

chrome

Danger: Malware Ahead!

Google Chrome has blocked access to this page on [redacted]

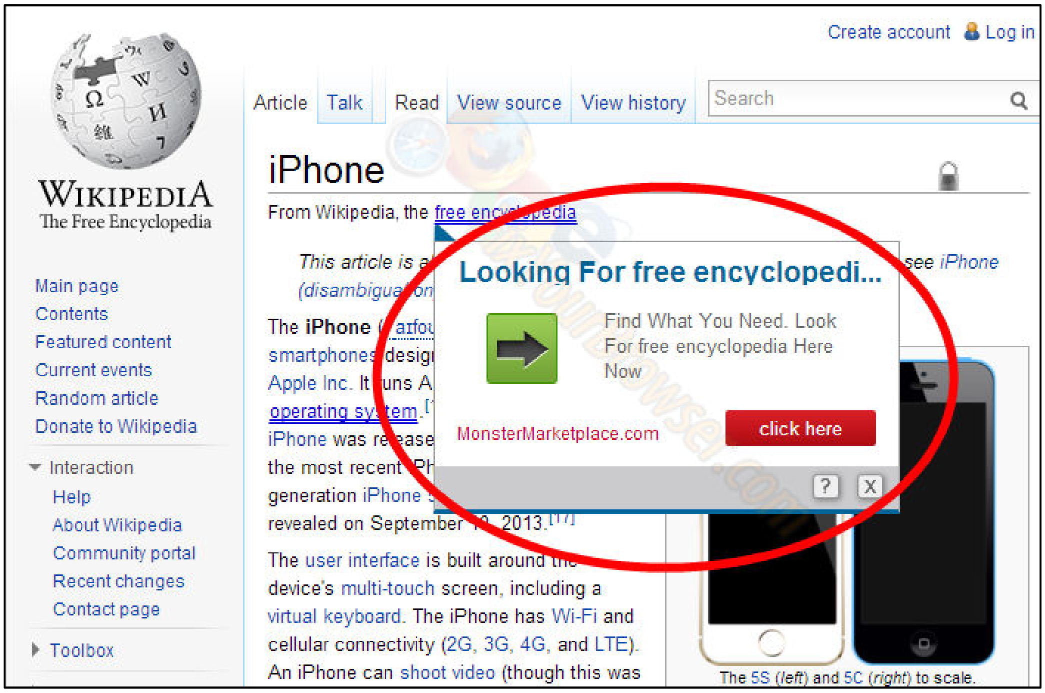
Content from cm.netseer.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

□ Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

Malware

Malware includes any malicious software that could infect a computer. You have likely heard of computer **viruses**, but malware can also include **spyware**, **adware**, **Trojans**, and **worms**. Clicking on the wrong link in a suspicious email could download a virus or malware to your computer. For example, the image below shows an adware popup that appeared when the visitor was looking something up on Wikipedia.



iPhone

From Wikipedia, the free encyclopedia

This article is a … (disambiguation) … see iPhone

The **iPhone** (aɪfoʊ … smartphones desig… Apple Inc. It runs A… operating system.[… iPhone was release… the most recent iPh… generation iPhone … revealed on September 10, 2013.[17]

The user interface is built around the device's multi-touch screen, including a virtual keyboard. The iPhone has Wi-Fi and cellular connectivity (2G, 3G, 4G, and LTE). An iPhone can shoot video (though this was

Looking For free encyclopedi...

Find What You Need. Look For free encyclopedia Here Now

MonsterMarketplace.com

The 5S (*left*) and 5C (*right*) to scale.

You can help prevent malware attacks on your computer by learning safe browsing habits and taking steps to secure your computer. We have already reviewed how to identify a suspicious or spam email, but there are other steps you can take, like such as installing an anti-malware software or antivirus program on your computer. A few reputable programs include:

Malwarebytes: https://www.malwarebytes.com/

Bitdefender: https://www.bitdefender.com/

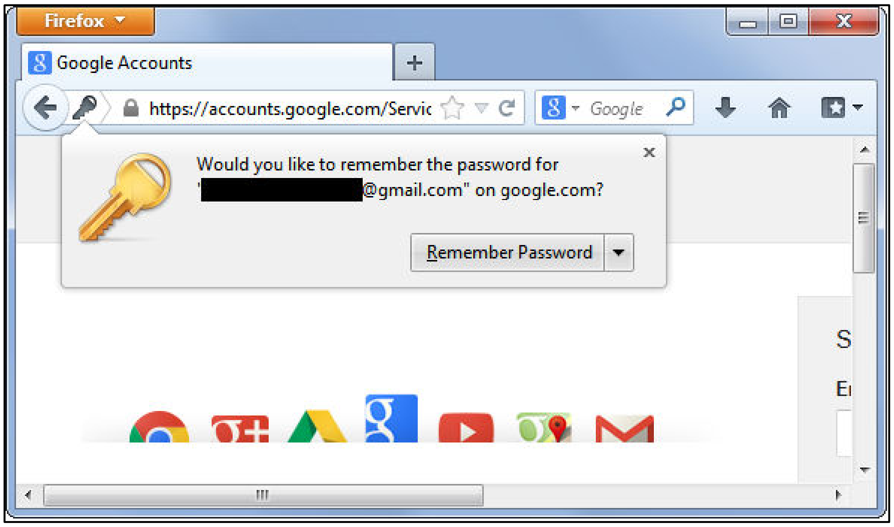
Norton: https://www.norton.com

Internet Browser Security

While browsing the internet you may accidentally download malware or run across fraudulent websites without really knowing it. Fortunately, your browser has some built in features to protect you from these threats. Knowing how to use them to your advantage is important.

Stored Passwords

The average person has several passwords. It can be difficult to remember them all, so internet browsers have a feature that offers to remember your password for you.



Would you like to remember the password for "[redacted]@gmail.com" on google.com?

Once remembered, the password field will automatically populate when you visit the sign in page for that particular site. This may be convenient on your home computer, but do not allow the browser to remember your password when you are using a public computer or one that is not your own. Also, when using a public computer, remember to **sign out** of the website you are using.

Of course, keeping your browser software up to date is a good way to stay protected. Most browsers will notify you when an update is available, but you can also check for updates in the browser's settings menu.

In Chrome:

1. Click the Menu button
2. Select "Settings"
3. Click "About"

In Firefox:

1. Click the Menu button
2. Click "Options"
3. Click "Advanced"
4. Click "Update"

Internet Explorer:

1. Click the gear-wheel icon
2. Click "About Internet Explorer"
3. Click "Install new versions automatically"

Passwords

Creating a safe password is really about finding a balance between something that you can remember and something that would be very difficult for others to guess. For even more security, avoid using the same password for all your online accounts.

Tips for creating a strong password:

- The longer, the better. It should be at least 6 characters
- Include a mix of uppercase and lowercase letters
- Include numbers and symbols (ex: !@#$)
- Try a password generator like https://strongpasswordgenerator.com/

Examples of poor passwords to avoid:

- Your name
- Your birthday

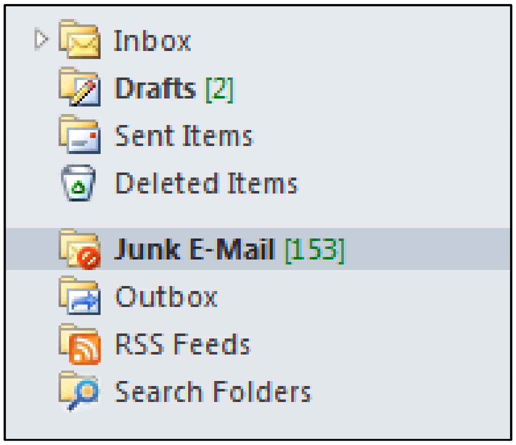
- Your email address
- Password123
- Your child or pet’s name

Keeping track of all your passwords can be a daunting task. One option for keeping track of them is a type of software called a **password vault or manager**. This program stores all of your passwords in one place where you can easily retrieve them. Programs are available for computers and mobile devices.

Spam & Phishing

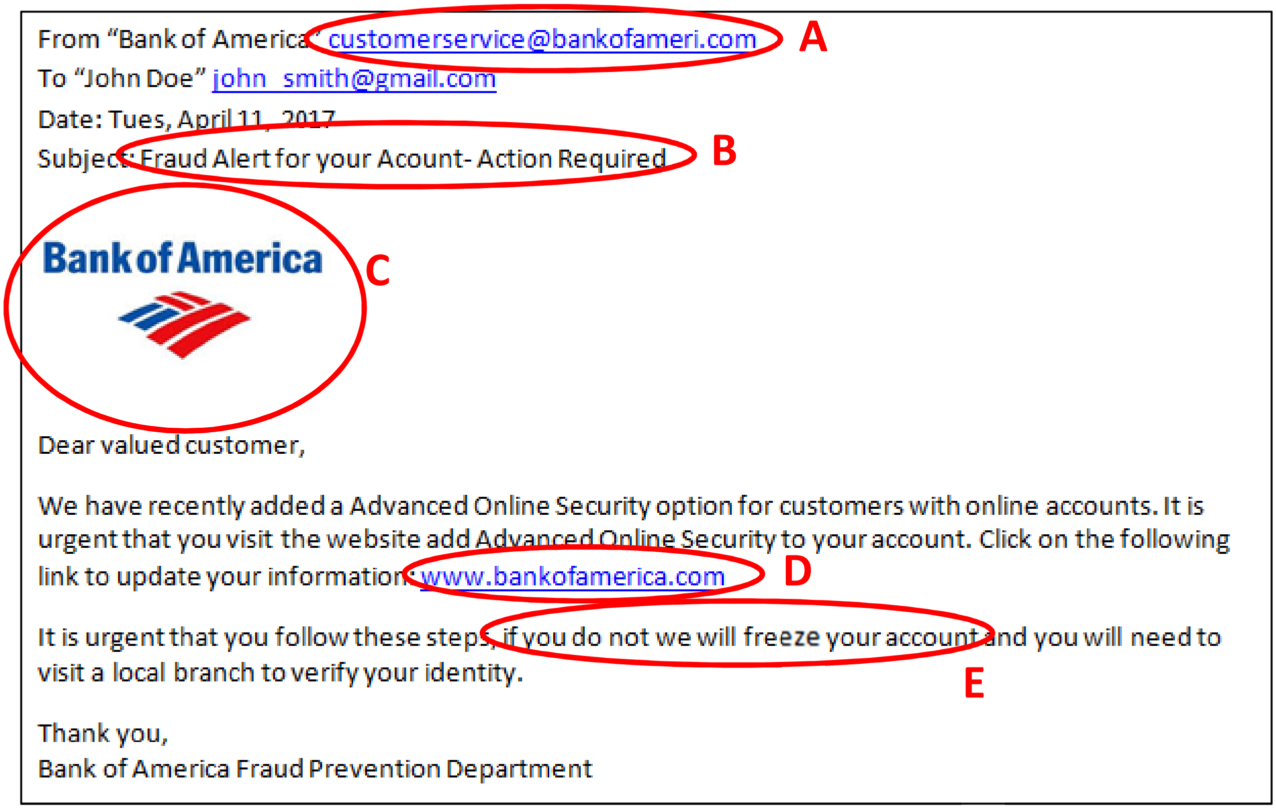
If you have an email address, you’ve probably dealt with **spam** or **junk mail**. While spam can simply be an inconvenience by filling up your inbox, it can also be a gateway for **phishing scams** and **viruses**. For this reason, you need to be careful of what you open and click on in your email account.

Spam or **Junk Mail** is just like the junk mail you receive in a physical postal mailbox, consisting of unsolicited advertisements, mass mailings, and the like. Most email providers will place suspected spam in a specific folder in your Inbox.



Phishing scams are designed to trick you into giving out sensitive or confidential information. Emails from phishing scams might appear to be from trusted source, such as a bank, and will typically ask you to enter personal information such as a birthdate, password, or credit card number. While phishing message can appear convincing at a first glance, there are a number of details you can look for to spot a phishing scam.

While this email may look official on the surface, taking a closer look will reveal that it is a phishing email.



From “Bank of America” customerservice@bankofameri.com
To “John Doe” john_smith@gmail.com
Date: Tues, April 11, 2017
Subject: Fraud Alert for your Acount- Action Required

Bank of America

Dear valued customer,

We have recently added a Advanced Online Security option for customers with online accounts. It is urgent that you visit the website add Advanced Online Security to your account. Click on the following link to update your information: www.bankofamerica.com

It is urgent that you follow these steps, if you do not we will freeze your account and you will need to visit a local branch to verify your identity.

Thank you,
Bank of America Fraud Prevention Department

A: Check the **sender’s email address.** Scammers may use an email address that appears close to the real company’s one. Rather than being from bankofamerica.com this email address comes from bankfoameric.com.

B: Look for a subject line that appears **urgent**. This is one way the scammers try to draw people in.

C: Don’t be fooled by **official looking logos**. Scammers can use a copy of any logo.

D: Don’t click on any **links.** While this appears to be a link to the official site, it may actually link to another website.

E: Look for **threats** within the email that create a sense of urgency. Scammers will often suggest that failure to respond immediately will result in consequences such as having your account frozen.

Other email scams exist as well. In some instances, a scammer might present themselves as a person you know in real-life and ask for money. Or a scam may promise to send you money if you provide a small amount upfront. Never send someone money in response to an email request. Also, you should not download attachments from suspicious emails. An attachment could contain a virus or malware that could infect your computer and steal confidential information.

Social Media

There are several important safety issues to keep in mind when you are using social media sites such as Facebook or Snap Chat.

1. The internet is forever

Once you put something on the internet, whether it is text, picture, or video, you can never be sure what will happen to it. While you may be able to delete a post off of your Facebook page, you can never be certain that someone else hasn't copied it, reposted it somewhere else, or saved it.

While you may want to show your friends a picture of yourself being silly at a party, think about the effect that picture might have if you are applying for a job, and the person interviewing you saw it. Once you put something on the internet it can be very difficult to get rid of all trace of it.

2. The internet is not private

There are certain websites and blogs, such as Facebook, that allow you to adjust privacy settings (you can learn more about Facebook privacy settings in our Facebook class) but services like Facebook can change their privacy features at any time. Before you post anything personal on the internet, like your name, address, phone number, or even pictures of children, think about who might be able to see them. If you can share that information through a phone call, an email, or a private message, that is a better idea.

Don't forget, NEVER post information such as your social security number, credit card, or bank account information on social media.

3. People on the internet may not be who you think.

It can be easy to feel like you have gotten to know someone well over the internet. It can be a very easy and comfortable way to talk to people, and you can feel like you have gotten to know them well. Some people even fall in love with people they have met over the internet.

It is important to keep in mind though that the internet is anonymous. If you are becoming friends with someone you've never met it can be tempting to tell them small lies, about things like your age or your appearance. Some people use the anonymity of the internet to tell bigger lies, or even to take advantage of people.

How to stay safe?

Here are some basic things you can do to ensure your safety when interacting with people over the internet:

1. Do not ever give your credit card number, bank information, or social security number to someone through email or social media.
    - Any legitimate retailer will use a service such as PayPal, or a recognized commerce website such Amazon.com, or eBay.com.
    - If your friends or family are contacting you about money over the internet, call them on the phone to make sure their email and social media has not been compromised!
    - If a friend is asking you for money, but you don't have their phone number, and have never met them in person, they may not be a real friend! Ask if there is something else you can do to help, like contacting their local police or another social service in their area.

2. If you meet someone new through the internet, whether it's a friend, a potential date, or even a person you are going to buy something from, do not give them your home or work address, even if you are sure they are trustworthy.
    - Offer to meet them in a public place where you are comfortable, such as a restaurant, a coffee shop, or a crowded park.
    - If you are going to meet someone you have met on the internet, make sure a friend, family member, or coworker knows where you are going, and when you plan to be back. If you change your plans, let them know.

3. Do not post anything on the internet that you would not post in your local newspaper.
    - Before you post anything on the internet think about how you feel if your mother, your boss, or your grandchildren saw it. Because they might!