NATIONAL 4-H COUNCIL

Teens **Teaching** Tech:

A guidebook for bridging the generation gap with technology

MENTOR UP
WHAT YOU KNOW IS WHAT THEY NEED™

AARP® FOUNDATION

UGA extension

TABLE OF CONTENTS

TECH 101

A Comparison of Different types of Devices

Apple vs. Windows/Android

Main differences are:

- Operating system: how the device executes commands and operates software
- User interface: design and functionality
- There are also design and function differences across the various devices
- Types of devices covered today:
- Computers-laptops
- Tablets
- Phones

		Windows
Security	Apple computers are less vulnerable to viruses and other malware. Viruses are beginning to target Apple computers due to the lack of experience when it comes to fighting viruses on Macs.	Windows computers are very susceptible to viruses and malware, especially if not protected by an antivirus program.
Price	When compared to a PC, an Apple computer, its peripherals, upgrades, and repairs are often more expensive than a PC. Average price: $1,500.	The vast majority of PC's and their peripherals are cheaper and more affordable when compared to a new Apple Macintosh computer. Average price: $700.
Operating System	The Apple Macintosh operating system is often a much cleaner, faster performing, and more stable operating system.	Many PC manufacturers bundle bloat ware with their computers. With this extra software and drivers from dozens of manufacturers, the Windows operating system can be slower in performance and less stable.

Software	The available software options for an Apple computer are greatly increasing, with many software titles that are exclusive to Apple.	More people are using and developing software for PC's running Windows, which means there is a larger selection of software available for Windows. There is also an almost endless supply of free programs.
Quality	The Apple Macintosh computer is often built with a lot better materials when compared to most PC's.	To help keep the overall costs low, some PC manufacturers build their computers from plastics and other cheaper materials when compared to a Mac. However, there are also PC manufacturers who meet and sometimes exceed the quality of Apple computers.
Upgrades	Apple computers are being built with more interchangeable parts, making them easier to upgrade than they used to be. Upgradeable parts for Apple computers can be expensive.	Just about every part of a PC can be upgraded. Also, because of openness and competition between hardware vendors, parts are usually cheaper and more readily available for the PC.
Boot time	Apple computers can often boot faster than a PC, due to excellent operating system coding and the efficient hardware for fast boot times.	PC's running Windows and built with hardware designed by dozens of different companies usually have slower boot times.
Repair	Many of the new MacBooks and other Apple products are starting to use glue to hold components inside the computer in place. Glue can make repair difficult and expensive.	Although PC laptops can be more difficult to repair than desktop computers, their components are often easier and cheaper to repair or replace than those in a MacBook or Apple computer.

Tablets

Similarities and overlap with computer differences

iPad

Strengths:

- In the Apple's app store, there are more than 800,000 apps, among which 300,000 apps have been specifically designed for iPads.
- Is more stable because each app is approved individually after thorough testing to ensure that it delivers as it claims.
- Ease of use.
- It is easy to eradicate bugs in the device and thereby operating the device is simple and less of a hassle

Weaknesses:

- The iPad offers less customization options to the users.
- The device also lacks the option to expand its storage.
- The price of iPad is much higher than an Android tablet. Average price: $399.

Android

Strengths:

- One of the biggest strengths of an Android tablet is its customization. You will get thousands of options to customize the device according to your requirements.
- The app store of an Android device has also been improved, featuring 800,000 aps. Lack of direct supervision means more apps will be released in the app store than in Apple's app store.
- Wide variety of devices, such as Google Nexus, Samsung Galaxy, and Kindle Fire just to name a few.

Weaknesses:

- The lack of direct supervision of Google app store is the major drawback of the Android devices.
- Top tier services such as games that take much time and resources to load.
- Piracy and malware is another issue that has done damage to the Android platform.

Phones

Similarities and overlap with computer and tablet differences

iPhones

Strengths:

- Great quality product with simple usability and clear communication.
- Dual-contact touch screen with twice the resolution of average computer screen.
- Integrated email, phone, and web features.
- Easily connected across multiple Apple products. Can sync with Macbook, iPad, and iPod.

Weaknesses:

- Sealed-in battery. Must send it back to Apple for a replacement.
- No memory card slot.
- High price point. Average price: $499.

Android

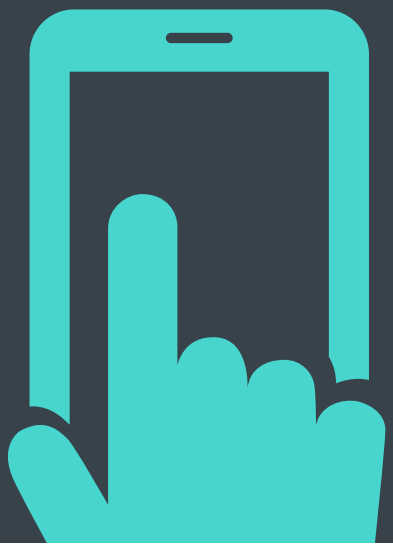
Strengths:

- A variety of manufacturers to choose from. With Android, there is pretty much a phone for every type of person.
- Widgets on your home screen are totally customizable. A widget is a kind of gadget that sits on your home screen and performs a specific function.
- Integration with Google Services, such as Gmail, Google Reader, Google Calendar and every other Google service.

Weaknesses:

- The Google Play Store still lags behind the iTunes Store in the quality of its apps. The openness of the Google Play Store has also made Android users more susceptible to downloading malware through scuzzy apps.
- Android is seen as too difficult to use for first-time smartphone buyers. The setup is more complicated than iPhones.
- Because of how many different Android devices there are, tech support for your specific Android smartphone may be harder to come by than if you go Apple.

HOW TO SETUP A SMARTPHONE



Introduce someone to a smartphone (or tablet, for that matter) for the first time, and you'll quickly realize how much you've taken for granted. From swiping to unlock and tapping to answer calls, here are the basics you'll have to show your smartphone newbie.

Set Up the Phone

Some things you can set up in advance and then show them later if necessary, while other things like navigating around the phone and downloading apps are probably best demonstrated in person (see the next section for that).

For example, you can insert the SIM card (if needed), set up a new Gmail or iTunes account, turn on screen lock, and install basic apps without the person looking over your shoulder. The Android and iOS startup screens conveniently walk you through setting up the new device (if you're giving someone your old phone, set it back to its factory settings first), but here are some tips to keep in mind:

- Save their login information. After setting up their new user account for iTunes or Google, add their login information to your password manager, because at some point in the future, you'll need to retrieve it for them. Password managers like LastPass and 1Password can help you generate a long password that's pronounceable and thus easy for them to remember.
- Enable Find My Phone. During the setup process in iOS, make sure you choose yes to activating Find My iPhone. Android users can go into the Google Settings app and Android Device Manager to enable remote wipes. Both of these will help locate the phone if it gets stolen or, perhaps more likely, lost under a seat cushion.
- Set up the lock screen. Add a passcode lock to secure the device (in iOS, this is under Settings > General > Passcode Lock. In Android, it's Settings > Security > Screen lock). Alternately, if the phone has a fingerprint scanner (like the iPhone 5 or the Samsung Galaxy S5), you can set that up with the person (fun!). You can also add owner information in the same Security screen in Android and/or set the wallpaper up to add emergency contact information to the lock screen.

Set Up the Most Important Shortcuts

You probably know which apps the person will most likely use regularly, so put them front and center on the home screen and favorites tray, if they're not already arranged there. The obvious ones are the web browser, contacts, photos, camera, calendar, maps, and messaging apps. I set up shortcuts to important contacts on my mother-in-law's Android home screen, because she's going to use her smartphone mostly as a phone, and that one-touch dialing is a big deal for her.

Show Them What All the Buttons Do

There are two kinds of people in this world:
The kind who instantly push all of the buttons to see what they do, and the kind who want you to tell them which buttons to press. I'm going to be ageist here, but babies and toddlers seem to fall into the former category (they'll not only push the buttons, they'll smash them and gnaw at them, perhaps learning something along the way), while folks more careful around expensive technology (i.e., your parents and grandparents) are more wary of doing something wrong by pushing random buttons.

The first thing to teach is what the main buttons do: How to turn the device on and off, raise or lower the volume, and get back the home screen. These are the three buttons common to both Android and iPhone devices. You'll also want to show them the ports: Where to plug in the charger, headphones, and any removable media.

Android devices also add a standard set of buttons on the bottom: Home, back, menu, and (sometimes) search. You'll have to demonstrate what those are for too. For example, "This back arrow takes you to the last level in an app or back a page when browsing this web" or "This double box button shows you all of the apps you have open."

Teach Them How to Get Around and Use Apps

Swiping, tapping, tapping and holding are new skills for people who've never had a touch device. You'll need to demonstrate how to move between screens, switch between apps, swipe down for the notifications bar (and search on iOS), and how to move things around by touching and dragging.

The built-in apps you should help them play around with include:

- Phone and contacts: how to add contacts, answer an incoming call, and even how to hang up the phone (Seriously, don't take anything for granted.)
- Camera: how to focus, take a photo, share photos via email or text message, and where the photos end up

Email: how to send an email, move emails around, create attachments

- **App Store:** how to search it, download apps, where they end up
- **Notification Center:** what it shows you
- **Settings:** how to quickly access main settings in iOS Control Center or from Android's top bar
- **Messages:** how to send and read text messages

SAFETY TIPS FOR MOBILE DEVICES

Keep a Clean Machine.

Mobile devices are computers with software that needs to be kept upÐtoÐdate (just like your PC, laptop or tablet). Security protections are built in and updated on a regular basis. Take time to make sure all the mobile devices in your house have the latest protections. This may require synching your device with a computer.

- Keep security software current: Having the latest mobile security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- Protect all devices that connect to the Internet: Computers, smart phones, gaming systems, and other web enabled devices all need protection from viruses and malware.

Protect Your Personal Information.

Phones can contain tremendous amounts of personal information. Lost or stolen devices can be used to gather information about you and, potentially, others. Protect your phone like you would your computer.

- Secure your phone: Use a strong passcode to lock your phone.
- Think before you app: Review the privacy policy and understanding what data (location, access to your social networks) on your device an app can access before you download it.
- Only give your mobile number out to people you know and trust and never give anyone else's number out without their permission.

Connect with Care.

- Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.
- Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.
- Protect your $$: When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.
- When in doubt, don't respond. Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or to immediate action are almost always a scam.

Be Web Wise.

Stay informed of the latest updates on your device. Know what to do if something goes wrong.

- Stay current. Keep pace with new ways to stay safe online. Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- Know how to cell block others. Using caller ID, you can block all incoming calls or block individual names and numbers.
- Use caution when meeting face to face with someone who you only "know" through text messaging.
- Even though texting is often the next step after online chatting, that does not mean that it is safer.

Be a Good Online Citizen.

It is easy to say things from via phone or text that you would never say face to face. Remind your kids to maintain the same level of courtesy on the phone as they would in the real world.

- Safer for me more secure for all: What you do online has the potential to affect everyone—at home, at work and around the world. Practicing good online habits benefits the global digital community.
- Text to others only as you would have them text to you.
- Only give your mobile number out to people you know and trust and never give anyone else's number out without their permission.
- Get permission before taking pictures or videos of others with your phone. Likewise, let others know they need your permission before taking pictures or videos of you.

STOP

Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK

Take a moment to be certain the path is clear ahead. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Visit **http://www.stopthinkconnect.org**
for more information.

ONLINE COUPONING

One of the major components of the Tech Wizards Mentor Up program is food insecurity. This lesson is developed to teach seniors about how to use store reward cards to save money on their weekly grocery bills.

Each of us is in a unique location with different stores in the area. We focus heavily on Kroger and Publix as they are two of our biggest grocery store chains. We also teach about the Wal-Mart Savings Catcher as well.

What is Online Couponing and Why Should I do it?

Online Couponing is a new type of couponing that prevents you from having to buy a newspaper and cut out the coupons. This is good for those who want to save money but not spend a ton of time organizing tiny print coupons.

What if I don't have a printer?

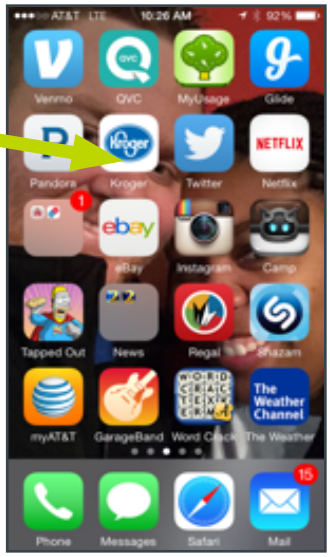
If you do not have a printer then don't fret, today we are actually focusing on couponing with your smart phone through various apps.

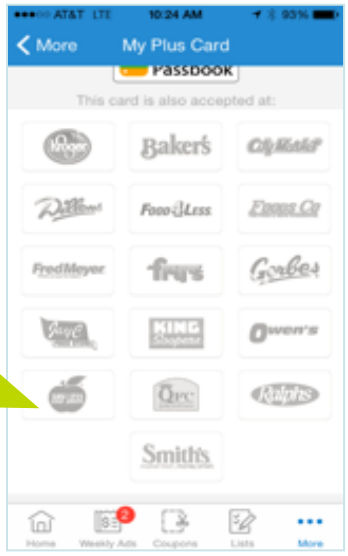
Can I combine paper and online coupons?

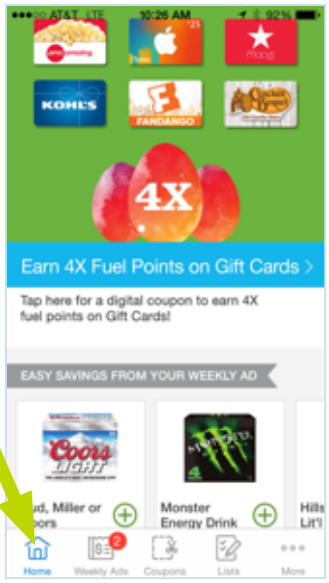
Yes, most stores will allow you to combine a store coupon (Online Coupon) and a manufactures coupon.

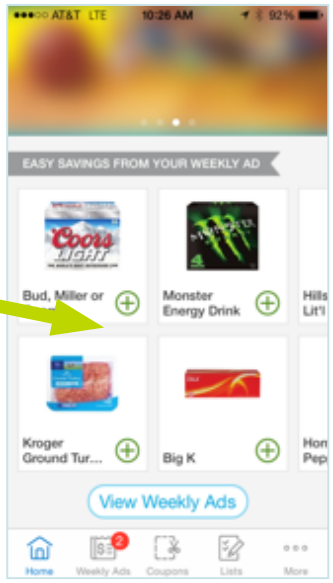
Kroger App

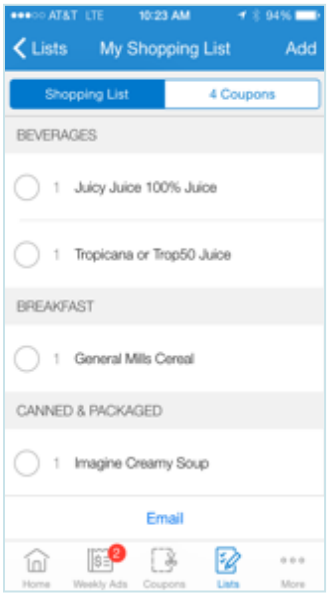
Grocery Store Apps are one of the easiest ways to save money. By downloading the app and registering your savings card you can automatically load coupons while you are in the store.

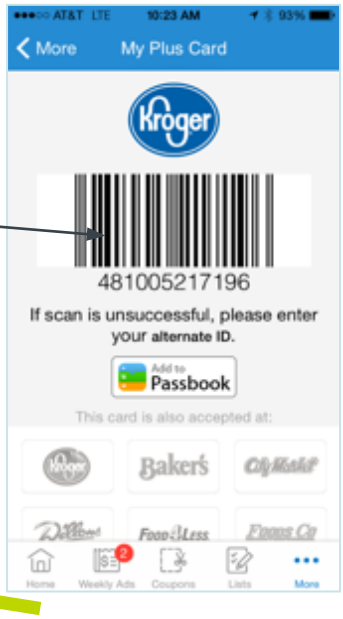




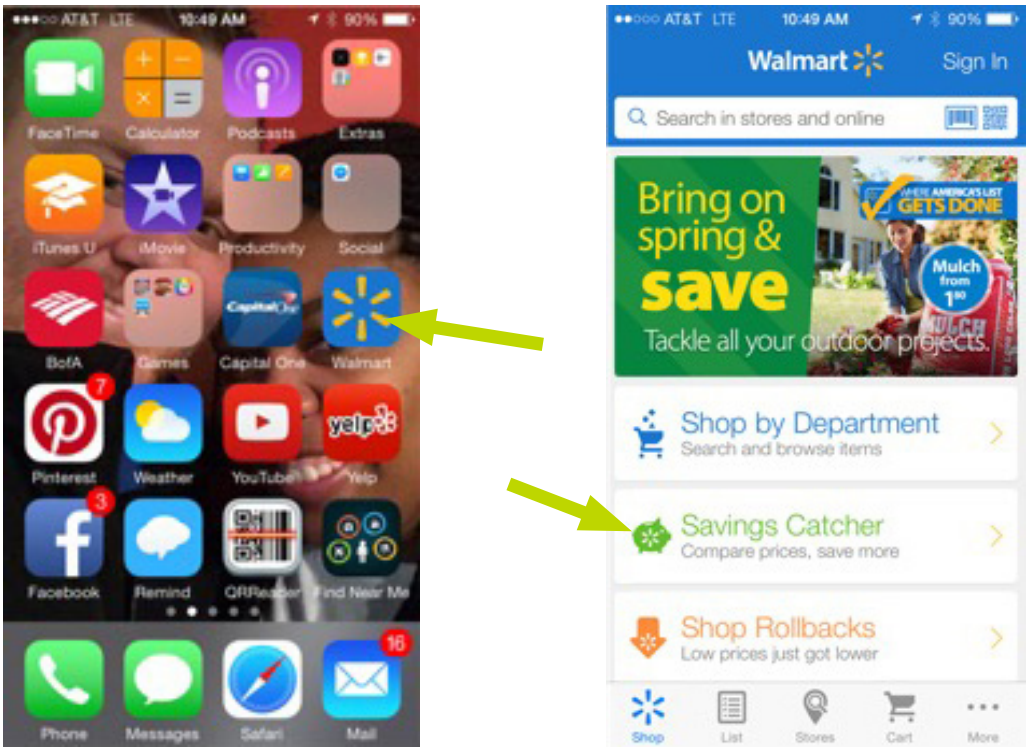


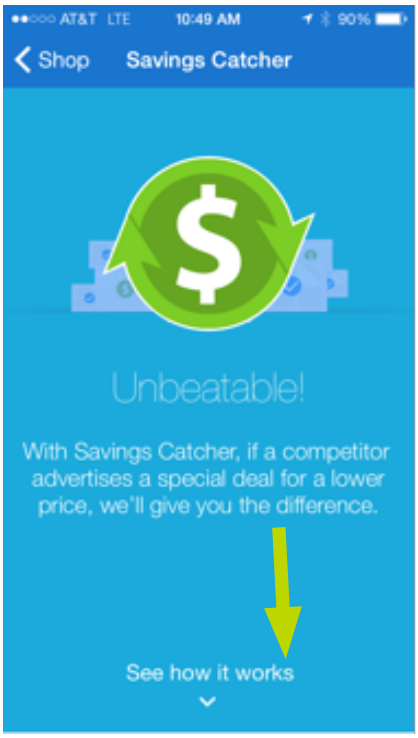


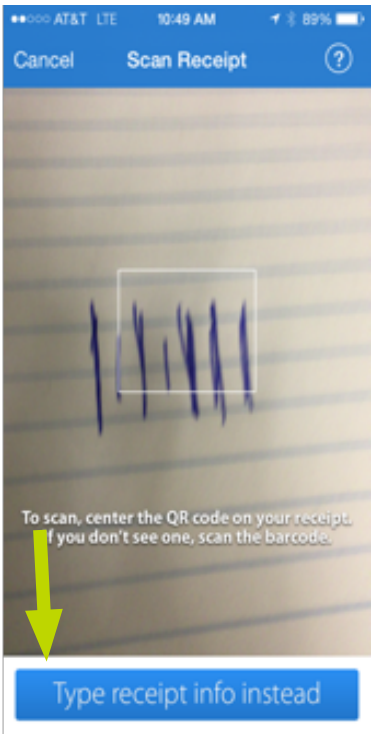




Walmart Savings Catcher







SOCIAL MEDIA 101

Learning the basic of what social media is and the best practices to use it

What is Social Media?

- According to Merriam-Webster dictionary social media is: forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content
- Social media technologies take on many different forms including blogs, business networks, enterprise social networks, forums, photo sharing, products/services review, social bookmarking, social gaming, social networks, video sharing and virtual worlds.
- Social media can be both websites and applications, with many social media sites having both websites and applications.

Examples of Social Media

Social Media Best & Safe Practices

Protect your identity

- Be honest about yourself, while also taking steps to protect yourself.
- Never give our personal information through social media. Don't provide personal information that others could use against you, or allow identity thieves and other criminals to take advantage of you.
- It is recommended that you do not list your home address or personal telephone number or work telephone number, but it is your choice if you want to.
- Be respectful of others
- When posting comments, refrain from posting material that is vulgar, obscene, threatening, intimidating, harassing, or an act of discrimination, harassment, or hostility towards another.
- The tone of your comments should be respectful and informative. Personal attacks, online fights, and hostile communications are not a best practice.
- Remember this simple rule: Communications, comments, or content that would not be acceptable in front of others should not be made merely because you are doing so on social media.
- Your profile is public and can be seen by others, including employers or potential employers. Keep this in mind when posting or commenting on social media.

Social Media Tips

- Assume that everything you put on a social networking site is permanent.
- Be selective about who you accept as a friend on a social network. Identity thieves might create fake profiles in order to get information from you.
- Change Your Passwords: often and do not use the same password for social networking sites that you use for your email accounts and online banking.
- Know what action to take if someone is harassing or threatening you. Remove them from your friends list, block them, and report them to the site administrator.

FACEBOOK BASICS

Getting Started

- Press the Facebook app icon.
- If you already have an account, log in.
- If not, press sign up at the bottom of the screen.
- Complete the sign up by filling out your name, birthday, gender and email address.
- After agreeing to the terms of use and confirming your email, your account should be made.

Your News Feed

- This is the first screen that should pop up once you've opened the app and logged in.
- This is where you can see anything that your friends post
- Posts come up by showing the person's profile picture, name, and what they decided to post.
- In order to see everything that is on your News Feed, you navigate that page by scrolling down.

Updating Your Status

- Tap "Status" from the Newsfeed or the Timeline.
- While you are making your status you can also:
  - ❍ Add Photos
  - ❍ Tag Friends
  - ❍ Add How You're Feeling
  - ❍ Add Your Current Location

Requests

- This is where anyone who sends you a friend request pops up. You have the ability to accept or deny these.
- The list, "People You May Know" consists of mostly mutual friends that you share with various people in your friends list.
- These are not people who have sent you requests, but suggested users that you may want to follow.

Adding Friends

- Type your friend's name or email in the search bar at the top of any Facebook page.
- Select their name to go to their profile.
- Click the Add Friend button. You might not see this button on some people's profiles, depending on their privacy settings.
- If they approve you to be their friend, you'll receive a notification in your notification tab, at the bottom of the screen.

Notifications

- You can access your notifications through the "Notifications" tab located at the top of the screen to the right of the "Messages" button.
- This is where everything that you have been tagged in, things of yours people have liked or commented on, birthdays, requests, and more are displayed.

Privacy

- Tap  and scroll down to privacy.
- Here you are able to choose who is able to see the things you post and share.
- You can also choose who is able to contact you through Facebook.
- You can also block users through the privacy setting.

Your Profile

- Your profile page is accessed by clicking  in the top left hand corner and clicking your name at the very top of the side bar list.
- This is your own personal page that your friends, or anyone can access based upon of your privacy settings.
- This is where you can put a profile picture, cover picture, as well as where you can access all of your pictures and statuses.
- This is also the page that people on your friend's list can post messages to you as well as pictures, links, etc.
- These things are not private, but on display for everyone on your friends list to see

Responding to Posts

- You can comment on posts that your friends have made, and even respond to comments from others on your own post.
- The process for commenting and replying is the same.
- To respond to a post, look below the post and you will see three options: like, comment, and share.
- Clicking the like button will make your name appear on a list of people who have liked the post.
- Clicking the comment button will allow you to post a comment to the post. Click the comment button, type your comment, and then like post to post your comment.
- Clicking the share button allows you to share a post to your timeline or with other people. Click share, decide where you want to share post to, and then click share link.

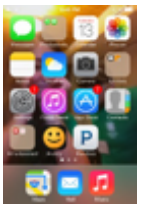
Logging Out of Facebook

- To log out of your Facebook account you must first click on 
- Scroll down to the very bottom of the side bar list.
- Click on log out. A text box will appear asking you if you want to log out, click log out again.
- If you have successfully logged out you should be taken back to the log in page for Facebook.

HOW TO TAKE PHOTOS ON THE IPAD 2

Features

- The iPad 2 comes with two cameras that allow you to capture video and photos. And because one camera is front-facing and the other is rear-facing, you can switch between them to capture images of yourself holding the iPad or images of what you're looking at. The front-facing camera captures VGA video and 3-megapixel photos; the rear-facing camera captures high-definition video and 5-megapixel photos.
- When you capture photos, they appear in the Photos app's Camera Roll, where you can view them, e-mail them, and so on.
- When you use an iPad camera, you can switch it between a standard camera and a video camera, and choose whether to use the front or back camera. To work with the standard camera to take pictures, follow these steps:



1. Tap the Camera app icon on the Home screen to open the app.
    a. If the Camera/Video slider setting at the bottom-right corner of the screen is shifted to the right, slide it to the left to choose the still camera rather than video.

2. Move the camera around until you find a pleasing image, and then tap the Capture button at the bottom center of the screen.
    a. You've just taken a picture and it has been stored in the Photos app automatically.
    b. Tap the screen in a particular area of an image before taking your photo to have the camera adjust focus on that area using the autofocus feature.

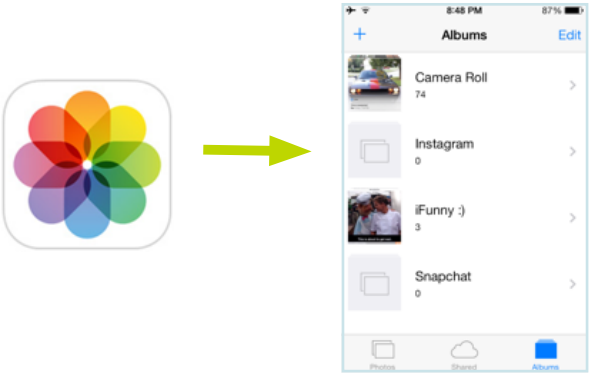
3. Click the Capture button and release it to take another picture.
    a. Remember to smile!

4. To view the last photo taken, tap the thumbnail of it in the bottom-left corner of the screen.
    a. The Photos app opens and displays the photo. Flick right to display other photos you've taken.

5. Tap the Menu Button
    a. A menu that allows you to e-mail the photo, assign it to a contact, use it as iPad wallpaper, print it, or copy it appears.

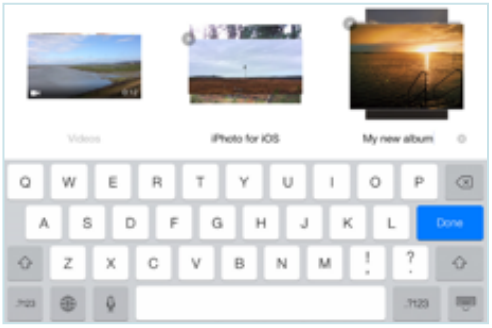
How to create a new album in the photos app on iPhone and iPad

- Open the Photos app on your iOS device and you'll see a blue button at bottom of the screen called Albums. Tap it and you'll see separate albums for the Camera Roll, your Photo Stream, Panoramas, Videos and third-party apps (if installed). Albums are a helpful way of organizing photos and separating content, so it's a good idea to add your own if you have a lot of images and want to categorize or present them within groups.



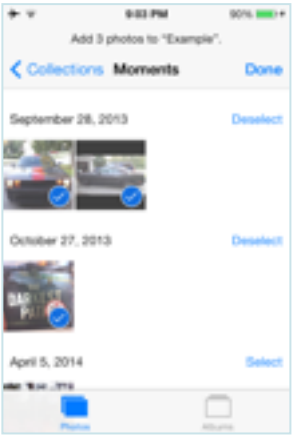
New Ablums

- To add an additional album, just tap the blue plus icon at the top of the screen. A pop-up window will appear asking for an album title. Enter one using the on-screen keyboard, then tap the Save button.



Adding Images

- Next we need to add some images to the new album. You'll see a window automatically appear that contains all the available images on your device. Tap on as many images as you'd like, then tap the Done button at the top of the screen. These images will now be added to your new album.

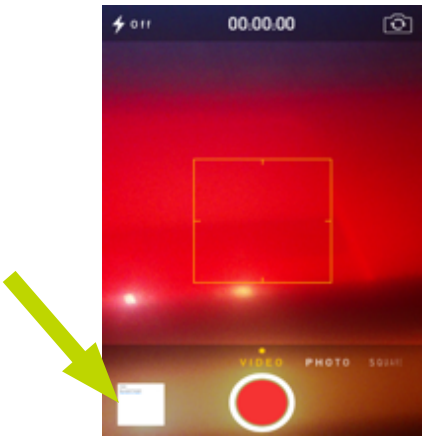


HOW TO CAPTURE VIDEO ON THE IPAD 2

In iPad 2, two video cameras that can capture video from either the front or back of the device make it possible for you to take videos that you can then edit and share with others.

1. **Tap the Camera app on the Home screen.**
   Use the Camera/Video slider in the bottom-right corner to switch from the still camera to the video camera.
   a. If you want to switch between the front and back cameras, tap the icon in the top-right corner of the screen.

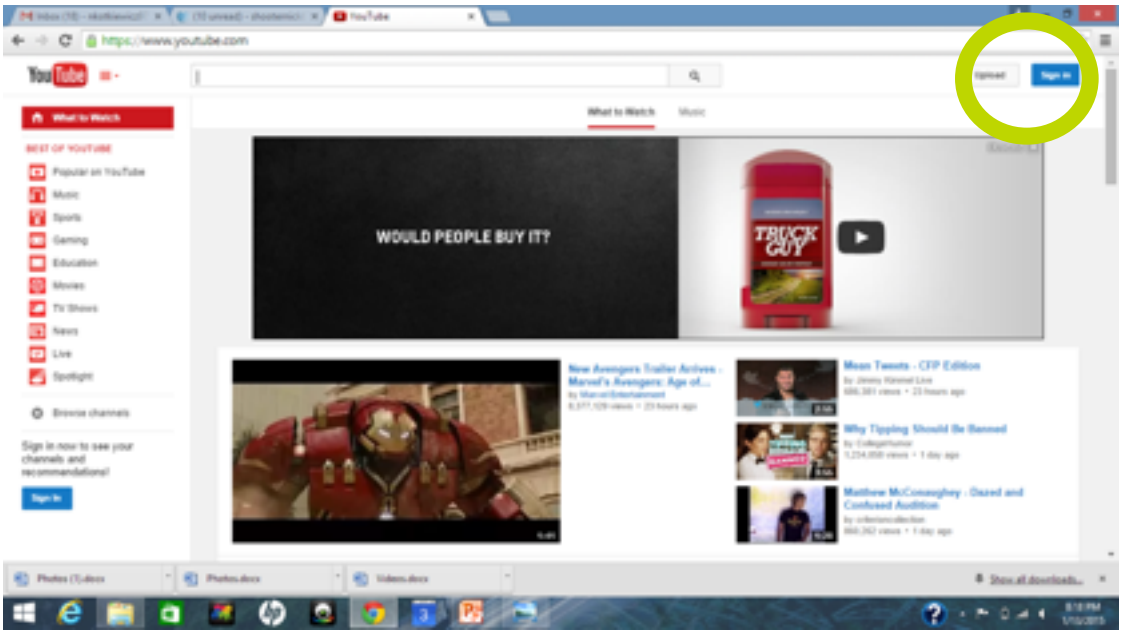
2. **Tap the Record button to begin recording the video.**
   a. Before you start recording, make sure you know where the camera lens is (in the top-center portion of the device on the front and top-right side of the back). While holding the iPad and panning, you can easily put your fingers directly over the lens! The Record button flashes when the camera is recording.



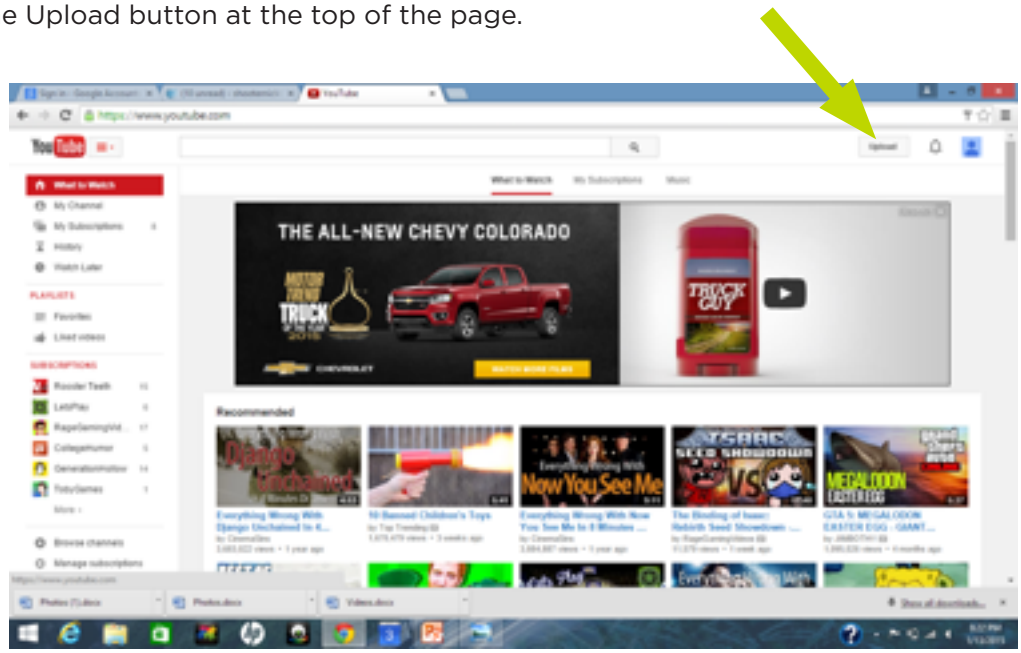
3. **To stop recording, tap the Record button again.**
   a. A thumbnail link to your new video is now displayed in the bottom-left corner of the screen

Uploading Video to YouTube

1. Signing into YouTube



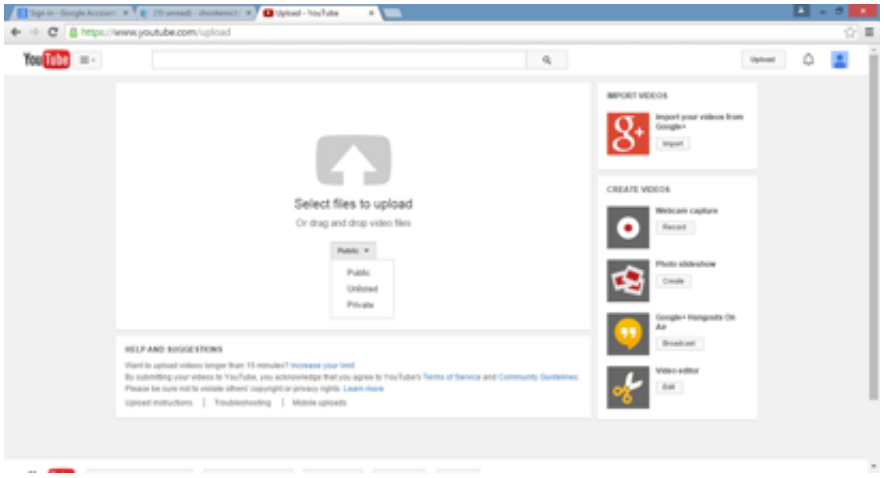
2. Click the Upload button at the top of the page.



3. Select the video you'd like to upload from your computer

   a. Before you start uploading the video you can chose the video privacy settings. As the video is uploading, you can add information (e.g. title, description, tags), change your privacy settings, add the video on a playlist, choose a custom thumbnail or decide if you'd like to post it to Google+, Facebook, or Twitter.

   b. You can edit both the basic information and the advanced settings of the video, and decide if you want to notify subscribers (if you untick this option no communication will be shared with your subscribers). Partners will also be able to adjust their Monetization settings.



4. Editing

   a. Make any changes you want to the video settings and information, then click Publish to finish uploading it on YouTube. You can always publish your video at a later time in your Video Manager. If you set the video privacy setting to Private or Unlisted, just click Done to finish the upload or click Share to privately share your video.

   b. If you haven't clicked Publish, your video won't be viewable by other people.

   c. Once the upload is completed you will receive an email to notify you that your video is done uploading and processing. You can then forward that email to friends or family for easy sharing. If you prefer not to receive notification, you can opt out by visiting your email settings.

5. Keep Videos Private

   a. It's tempting to showcase your videos to the world, especially if you have something unique, odd, or funny that you think will attract peoples' attention. After all, YouTube is responsible for making random videos worldwide hits. As intriguing as this sounds, it's best to keep a lot of your videos set to private so only a select group of people (up to 50) can view them. This is especially important if you're a professional and need to uphold a reputation.

   b. If you want to set your videos to private, follow these easy steps:
      i. Visit your Video Manager
      ii. Find the video you'd like to set to private and click the Edit button
      iii. In the "Privacy Settings" drop-down menu, select Private
      iv. Click Save Changes

6. Set Videos to “Unlisted”

   a. If you want to showcase your video to more than just a select 50 people, but don’t want the video listed to everyone in public, then you’ll want to set your videos to “unlisted.” What this means is that anyone with the direct web address can watch the video, but without this address the videos are impossible to find. They don’t show up on your YouTube channel, in search results, or anywhere else on the site.

   b. If you want to set your videos to unlisted, follow these easy steps:
      i. Visit your Video Manager
      ii. Find the video you’d like to set to private and click the Edit button
      iii. In the “Privacy Settings” drop-down menu, select Unlisted
      iv. Click Save Changes

7. Adjust Account Privacy Settings

   a. YouTube is an interactive website, and your videos aren’t the only thing you need to protect from the prying eyes of the public. Whether it’s liking videos, subscribing to them, or your contacts sending you messages and sharing your videos, it’s important to stay proactive in making sure you know who can track what you like and watch.

   b. If you want to set your account privacy settings, follow these easy steps:
      i. Click on your avatar and select YouTube Settings
      ii.On the next screen, click on Privacy at the top left
      iii. On this screen you’re able to set up and check your account privacy settings. Under “Likes and Subscriptions,” you can check the box to make sure any videos you like and any channels you subscribe to stay private and confidential. Under “Search and Contacts,” you can control who can contact you, share your videos, and find you by email address.

8. Control Channel Activity

   a. If you choose to keep your videos and content public, then you may attract people who don’t agree with what you’re posting and may spew insults and span your YouTube channel. It’s important to stay proactive in previewing and approving comments, video responses, and ratings if you want your channel clean and free from negativity. This prevents unsuitable comments from being published and deters posters from accessing your channel and doing it again.

   b. If you want to disable or preview and approve comments, follow these easy steps:
      i. Visit your Video Manager
      ii. Find the video you’d like to edit and click the Edit button
      iii. Click Advanced Settings
      iv. Adjust your preferences under the “Comments and Responses” tab
      v. Click Save Changes
      vi. If you selected to preview and approve comments, continue:vii. Under “Allow Comments and “Allow Video Responses” select Approved
      viii. Click your Username in the top right corner
      ix. Click Inbox
      x. Click Comments on the left side of the page

9. Check Your Account and Report Abuse

   a. Last but not least, you want to check your account often and make sure you update your settings according to your preferences. Log out of your account and check your page as a public user to see what’s being accessed and what’s not. Also, if you notice bad behavior and abuse, make sure you report it. YouTube is a community, and if there’s harassment, inappropriate remarks being made, or if someone is violating your privacy, site administrators need to know about it. Use this tool to do so.

HOW TO USE PHOTO STREAM ON THE IPAD 2

How does it work?

- It works by automatically uploading every photo you take on iPad to iCloud, then pushes them down to your other iOS devices, Mac, iPhone, PC. That means you can snap a photo while on a walk, then arrive back home and find it waiting for you on your Mac or other apple product.

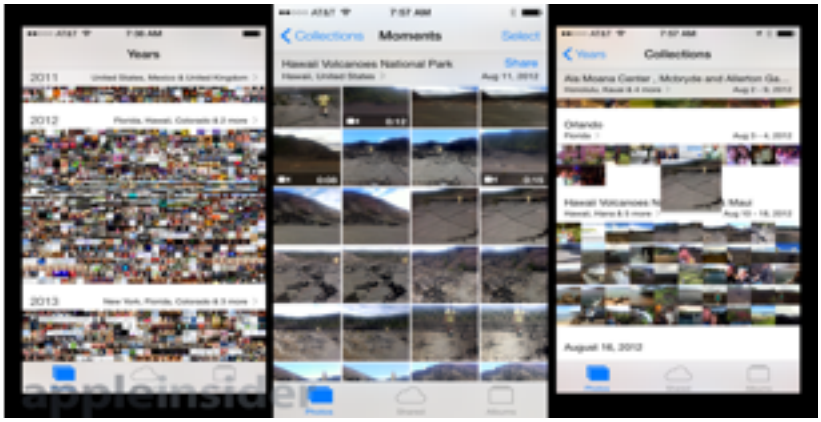
Features

- You can save up to 1,000 images in iCloud, and they stay there for a month.
- This gives you plenty of time to save them permanently to your desktop computer, or edit them on your iOS device using iPhoto.
- It's also possible to create a shared Photo Stream with friend and family, enabling them to see and comment on your photos.

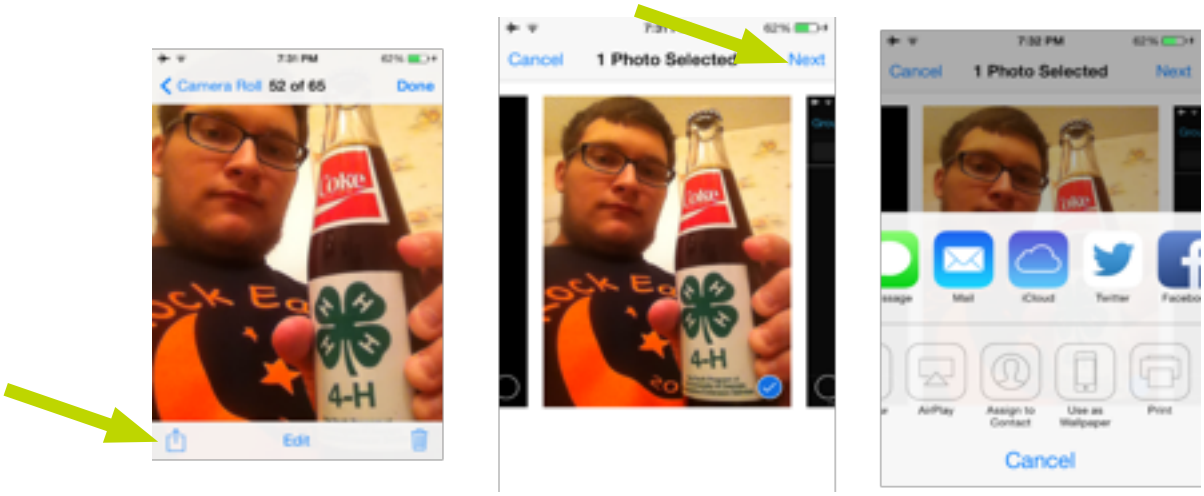
1. Enable Photo Stream
   - Photo Stream is usually enabled when you activate your iPad. But if you chose not to enable it at the time, open the Settings app, tap iCloud, choose Photo Stream then toggle to Off/On switch.

2. View Your Photo Stream

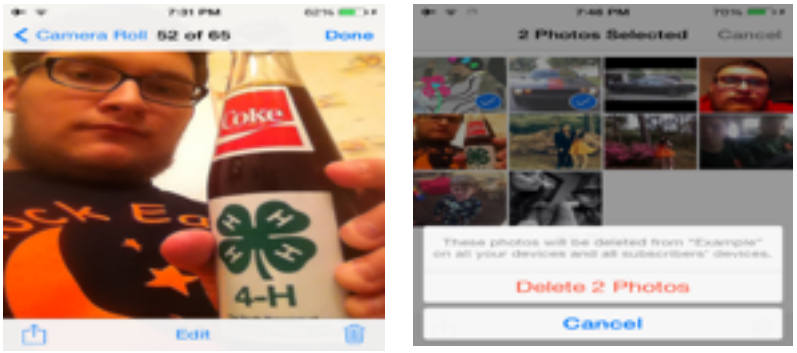
- You can access your Photo Stream by opening the Photos app, then tapping the Photo Stream button at the top of the screen. All the photos you've taken using your iOS devices will appear here in chronological order.



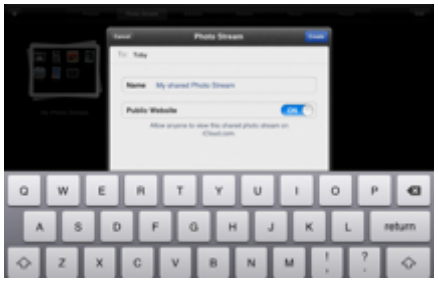
3. Share Your Photo Stream
   - While viewing an image, tap the Share icon in the bottom left corner of the screen. You'll see various options for sharing the image, including by E-Mail, Twitter, Facebook, Message, a printer plus the ability to save it to the Camera Roll or use it as a background wallpaper.



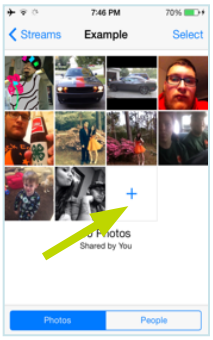
4. Deleting an image
   - While viewing an image, tap the Trash icon to delete it from Photo Stream. You can delete multiple images by tapping the Select button in the main Photo Stream window, tapping the images you wish to remove, then the red Delete button.



5. Created a shared Photo Stream
   - It's easy to share images with friends and family using Photo Stream. To get started, open the Photos app, tap Photo Stream, then tap the plus icon in the top corner of the screen.

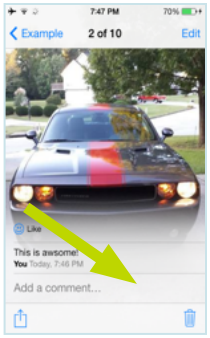


6. Add Friends
   - Next, type the names of the friends and family you wish to share your images with (or tap the blue plus arrow to select them from your Contacts list), then give the Photo Stream a name. You can also add a link to this new Photo Stream to your public iCloud account by toggling the On/Off switch. Tap the Create button once you're ready.



7. Insert Photos
   - You'll now see your new shared Photo Stream appear. Tap on it, then tap the Edit button at the top of the screen. Next, tap the plus button to insert new photos. These can be from your Photo Stream, Camera Roll or Photo Library.

8. Add a comment
   - Once you've added photos to your shared Photo Stream, tap on one and you'll see a comment icon with a plus inside it at the bottom of the screen. Tap this icon to add a comment or Like it. You can also leave comments and Like photos in your friends and families shared Photo Streams.



9.Delete and Edit
   - While viewing your Photo Stream albums, tap the Edit button in the top right corner of the screen. You'll see options for deleting a shared Photo Stream, editing the name, adding other people who can see the Stream and also a toggle switch for setting its public status.

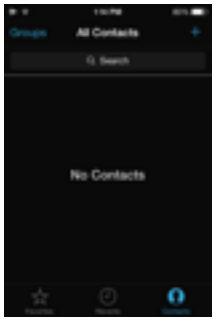
HOW TO USE FACETIME

How to get on Facetime

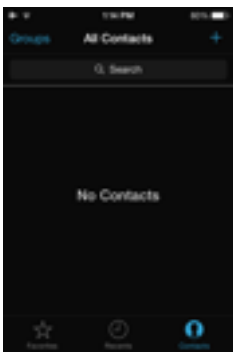
1. Click on the app that says “facetime” (green button)

2. If you have an Apple ID sign in, if you do not, create one.

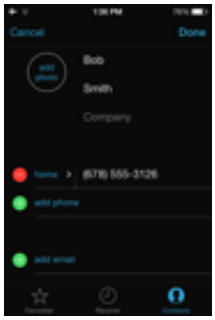
3. Then you will see “contacts”. It will be empty until you put names or numbers of contacts in it.



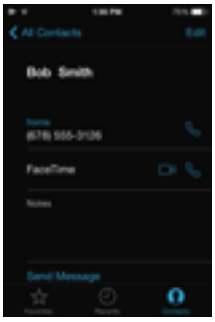
4. Press the “+” next to “all contacts” in the top right corner



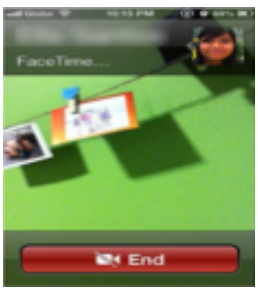
5. Put in contact name, number, or email on their name.



6. When you find someone click on their name next to Facetime , for video camera for video call



7. Video screen will come up, wait for next person to connect to call

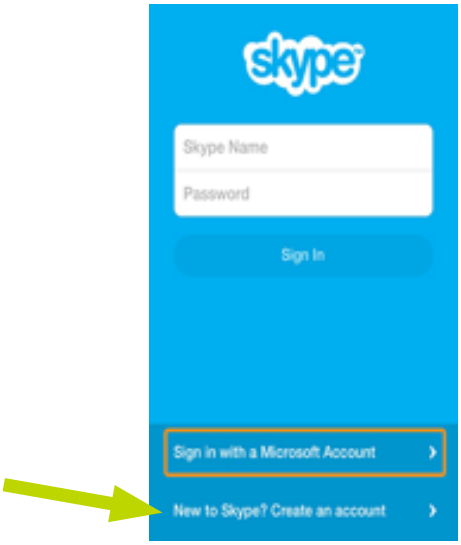


SKYPE BASICS

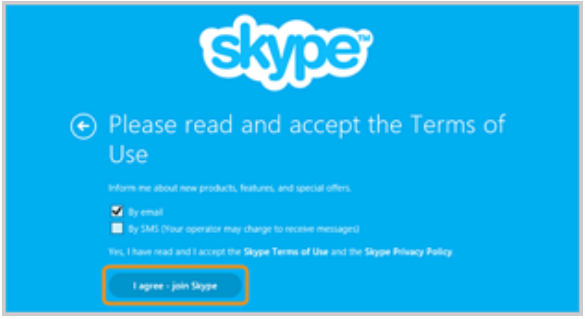
Joining Skype

1. Start Skype by taping on the Skype app icon 

2. Tap create account



3. Tap I agree to the Skype terms of use



4. Enter the required details, choose your Skype name and tap create account.

Signing into Skype

1. Start Skype

2. Sign in with your Skype name and password

3. Tap sign in

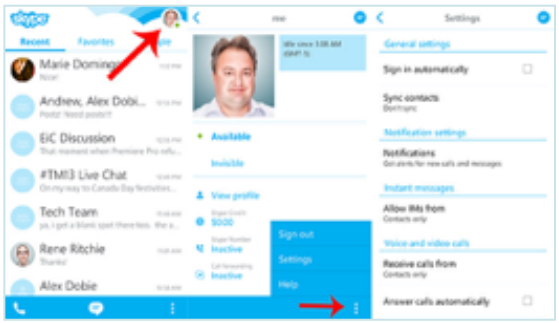
4. Read through the introduction, or tap done to skip it

Edit Your Profile

- Just tap your profile picture or name in the top left corner of the screen

How to sign out of Skype

- To sign out of Skype, simply return to the home screen, tap your profile picture on the right side of the screen and select sign out



SCAMS

Current Scams towards seniors

In a new report, the Internet Crime Complaint Center (pdf) says it received nearly 315,000 fraud complaints in 2011, with the bad guys making off with $485 million. (Known as IC3, the center is jointly run by the FBI and the nonprofit National White Collar Crime Center.) Analysis of victims' ages suggests that older people are particularly likely to fall for schemes in which the crooks claim to be government officials. Romance cons, too, were hard for older people to resist.

Here's the lowdown on the top five flimflams.

1. Work from home

   Generating 17,352 complaints, the number one spot goes to an especially dangerous version of the work "opportunity." Through advertisements in newspapers, online job sites, emails and social networking sites, scammers recruit innocent job seekers as "mules" to unknowingly steal or launder money. They work at their computers, thinking they're a "money transfer agent" or a "payment processing agent" for a legitimate business, but in fact they're moving stolen money abroad and unwittingly disguising its true origins. The scammers may also compromise the victims' own accounts or identities.

   Overall, victims lost $20 million total through identity theft and account tampering, averaging $1,160 per victim. "Regrettably, due to their participation, these individuals may face criminal charges" for check fraud and receiving and moving stolen goods, notes the report.
   Losses to the 50-plus: $8.4 million

   Men
   50-59: 1st in complaints, losses of $2.8 million
   60-plus: 5th in complaints, losses of $2 million

   Women
   50-59: 4th in complaints, losses of $2 million
   60-plus: 5th in complaints, losses of $1.5 million
   The most complaints were filed by those in their 20s, but people in their 50s lost the most money.

2. Government official impersonation

There were 14,350 complaints about emails that falsely claim to come from a government agency. Fast-growing are FBI fakers demanding money to prevent arrest, but the category also includes emails that seek money and personal information and purport to be from the IRS, Social Security Administration, Medicare or other agencies. In truth, government agencies do not send unsolicited emails. The total losses were $3.5 million, with a per-victim loss of $245.
Losses to the 50-plus: $2.2 million

Men
50-59: 1st in complaints, losses of $328,000
60-plus: 2nd in complaints, losses of $1.1 million

Women
50-59: 1st in complaints, losses of $501,000
60-plus: 4th in complaints, losses of $250,000
Over-60s lost the most money, $1.35 million,
with those in their 50s in 2nd place at $829,000.

3. Loan intimidation

The subject of 9,968 complaints, loan intimidation scams usually come by phone, but sometimes email. Fraudsters claiming to be with law enforcement, a law firm or a government agency threaten arrest or legal action for a supposed delinquent loan. To make their ruse convincing, they often already have targets' personal information such as Social Security numbers and birth dates. The IC3 reports that many victims say they completed online applications for loans and credit cards before the calls began. Overall, these scams netted more than $8 million in 2011.
Losses to the 50-plus: $3.5 million

Men
50-59: 4th in complaints, losses of $570,000
60-plus: 5th in complaints, losses of $1 million

Women
50-59: 4th in complaints, losses of $970,000
60-plus: 5th in complaints, losses of $927,000
Among both genders, 30-somethings filed the most complaints and those
40 to 49 lost the most money, nearly $2 million.

4. Romance

Fueling 5,663 complaints, cyber-romance scams snagged not only hearts but $50.4 million from their victims. You know their MO: Once they woo targets met on dating websites and in chat rooms, they request wire transfers supposedly to help with a personal hardship, pay for an airline ticket for a meeting or meet some other heart-rending expense. The IC3 averaged 15 complaints a day, with per-victim losses of $8,900. Losses to the 50-plus: $34.3 million

Men
50-59: 2nd in complaints, losses of $3.6 million
60-plus: 5th in complaints, losses of $2.6 million

Women
50-59: 1st in complaints, losses of $18.8 million
60-plus: 3rd in complaints, losses of $9.3 million
Women age 40 and older are the most targeted — and victimized.

5. Auto auctions

Generating 4,066 complaints, auto auction scams cost victims nearly $8.3 million. Crooks advertise a vehicle at a great price, claiming they must sell it quickly because they are moving, being deployed by the military or experiencing hard times. They request immediate full or partial payment through a third party, usually part of the scam ring. Of course, it turns out the vehicle doesn't exist or isn't theirs to sell. Sometimes scammers add credibility by posting photos stolen from legitimate auto auction websites. The per-victim loss averages about $2,000. How the 50-plus fared: Losses of $2.6 million

Men
50-59: 3rd place in complaints, losses of $1 million
60-plus: 5th in complaints, losses of $884,000

Women
50-59: 4th in complaints, losses of $448,000
60-plus: 5th place tie with those under 20 in complaints, losses of $257,000
Those 40 to 49 of both genders lost the most, nearly $2.1 million.
Women in their 20s and men in their 40s filed the most complaints.

Sid Kirchheimer is the author of Scam-Proof Your Life, published by AARP Books/Sterling.

Scams vs. Reality

Electronic hotel room keys contain your personal information. Since 2003, email warnings have claimed that your credit card number and home address are stored on the magnetic strip of your hotel key — and harvested by identity thieves when you leave the card in your room or toss it in a lobby trash can.

Reality: Hotel keys contain coded information for only the room number and check-in/out dates, says Chad Callaghan of the American Hotel & Lodging Association. If you use a key to charge dinner at a hotel restaurant, it's billed to your room, but "credit card information is stored on another machine," says Callaghan.

Hide your car's VIN or thieves can get a replacement key and steal the vehicle.
Yes, the easily viewed vehicle identification number on your dashboard and doorjamb reveals what standard key will fit your car.

Reality: Reputable dealerships and locksmiths require proof of ownership to issue a replacement key. In any case, obscuring a VIN is unwise — and may be illegal, because police rely on the numbers to identify stolen cars.

Your cellphone number is being released to telemarketers. Since 2004, emails have been warning that your number will be turned over "this month," and unless you register it on the federal Do Not Call Registry, you'll be bombarded with sales calls.

Reality: Register your cell if you want, but it's not necessary. Plans for a public cellphone directory were discussed but scrapped years ago — and even that proposal was only for folks who wanted to "opt in."

The feds are going to tax every debit card and ATM transaction (or every email sent).
False claims that a 1 percent tax is likely to be levied on all financial transactions are one of the top urban legends, says legend research site Snopes.com.

Reality: A lone congressman introduced such a bill several times as a deficit reduction measure, but it has died every time. As for a pending 5-cent surcharge on each email, that tale started in 1999. It's still spread by (tax-free) email and lists a phony sponsor and bill number.

PROTECTING YOURSELF FROM SCAMS AND IDENTIFY THEFT

How to avoid fraud

Seniors are often the target of fraud. However, with some basic understanding of how scam artists work, you can avoid fraud and protect your hard earned money. Learning how to invest safety can mean a huge difference in your retirement years.

Seniors are particularly vulnerable to tactics of scam artists who are "nice" or attempt to develop a false bond of friendship. Scam artists prey on seniors who are polite to others and have difficulty saying "no" or feel indebted to someone who has provided unsolicited investment advice.

What can I do to avoid being scammed?

- Ask and check out the answers
- Research the company before you invest
- Know the salesperson
- Never judge a person's integrity by how he or she sounds
- Watch out for salespeople who prey on your fears
- Take your time-don't be rushed into investment decisions
- Be wary of unsolicited offers
- Don't lose sight of your investments
- Question why you cannot retrieve your principal or cash out your profits
- Never be afraid to complain

Red flag warnings of scams

- If it sounds too good to be true, it is.
- "Guaranteed returns" aren't.
- Beauty isn't everything. Don't be fooled by a pretty website; they are remarkably easy to create.
- Pressure to send money RIGHT NOW. If it is that good of an opportunity, it will wait.
- Con artists are experts at gaining your confidence. So be certain to treat all unsolicited investment opportunities with extreme caution. Whether you hear about the opportunity through an email, phone call, or a fax, be certain to check out both the person and firm making the offer and the investment they are pushing.

Types of Fraud

- "PONZI" and Pyramid Schemes
- Oil and Gas Schemes
- Promissory Notes
- Prime Bank Fraud
- High Return or "Risk Free" Investments
- Internet Fraud

When dealing with these types of fraud look to State Regulations, Financial Industry Regulatory Authority, and Additional SEC Resources.

Scams

1. **The grandparent scam** - con men ask for money posing as the grandchild. https://www.youtube.com/watch?v=KpgwhdA0Wbg

2. **Lottery scams**- unexpected emails/calls or mailing claiming that you have won a prize **https://www.youtube.com/watch?v=1o1n5Bpcyvo**

3. **Reverse mortgage scams** - scammers take advantages of the elderly who own their homes. The scammer would send a government letter charging a fee to assess the value of the home. They then offer a free house in exchange for the title of the victim resulting in the loss of the victim's home.

4. **Investment schemes** - scam that targets seniors who have been saving their money for retirement to invest in fraudulent companies.

5. **Internet fraud**- the victims of this scam generally see a pop-up for fraudulent virus protection or receive emails asking to update personal information.

6. **Telemarketing** - scammers use fake telemarketing calls to older individuals. Since there is no face to face contact it is very hard to trace. Ex. Charity scams

7. **Fraudulent anti-aging products** - Botox scams are dangerous health wise. Fake Botox distributors could make up to a million dollars in profit. Some may have actual botulism neurotoxin, but a bad batch can be very harmful to the human body

8. **Funeral and cemetery scams** - the scammer looks through the obituaries for elderly widows. They claim to be from a company to settle fake debts. Other scams in this area involves funeral homes requiring an expensive casket for cremation when a cardboard casket will do.

9. **Counterfeit prescription drugs** - generally victims of this scam go to the internet for cheaper prescription drugs and instead receive a placebo.

10. **Health insurance fraud** - the perpetrator will disclose themselves as a Medicare or health insurance representative in order for the victim to give up their private information. https://www.youtube.com/watch?v=Bnt4QtdQ6ac

Identity Theft

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your social security number can use it to get other personal information about you. Identity thieves can use your number and good credit to apply for more credit in your name. Then, they use the credit cards and do not pay the bills. You may not find out that someone is using your number until you are turned down for a credit or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your social security number and assuming your identity can cause a lot of problems.

Your Social Security Number is confidential

The social security administration protects your social security number and keeps your records confidential. They do not give your number to anyone, except to you or when authorized by law. You should ask why your number is needed, how it will be used, and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your social security number.

How someone can steal your number

- Stealing wallets, purses, and your mail.
- Stealing personal information you provide to an unsecured site on the internet, from business, or personal information in your home.
- Rummaging through your trash, the trash of a business, or public trash dumps for personal data.
- Posing by phone or email as someone who legitimately needs information about you, such as employers or landlords.
- Buying personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.

What to do when your identity is stolen

If someone has used your social security number or other personal information to create credit or other problems, social security cannot resolve these problems. But there are several things you should do.

- Go to www.idtheft.gov and report the identity theft to the federal trade commission. Or, you can call 1-877-idtheft (1-877-438-4338) or (1-866-653-4261). The website the best places to get national resources to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.
- You also may want to contact IRS. Identity thieves may also use your social security number to file tax returns to receive your refund. People can also use your social security number in order to get a job.

What to know and what to do

What is Identity Theft? Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- Go through cans and dumpsters to steal bills and documents that have sensitive information.
- Work for businesses, medical offices, or government agencies, and steal personal information on the job.
- Misuse the name of legitimate businesses, and call or send emails that trick you into revealing personal information.
- Pretend to offer a job, a loan, or an apartment, and ask you to send emails that trick you into revealing personal information to "qualify".
- Steal your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information.

How to protect your information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. To order, go to annualcreditreport.com
- Read your bank and credit card statements. If a statement has mistakes or doesn't come on time, contact the business.
- Shred all documents that show personal information before you throw them in the trash.
- Don't respond to email, text, and phone message that ask for personal information. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.

If Your Identity is Stolen...

1 .Flag your credit reports
2. Order your credit reports
3. Create an identity theft report

You have the power to stop identity theft

1. Stop identity theft
    a. there is type of identity theft using the internet called "phishing"
    b. they can do damage to your financial history and personal reputation that can take years to unravel

2. How phishing works
    a. if you provide the requested information you may find yourself a victim of identity theft.

3. How to protect yourself
    a. never provide your personal information in response to an unsolicited request
    b. if you are unsure whether a contact is legitimate, contact the financial institution
    c. never provide your account information and/or password over the phone or in response to an unsolicited internet request
    d. review account statements regularly to ensure all charges are correct

4. What to do if you fall victim
    a. **http://www.ftc.gov/bcp/edu/microsites/idtheft/**
    b. 1-877-IDTHEFT (1-877-438-4338)
    c. **www.naag.org**

Consumer Fraud by phone or mail

When phone calls and postcards are bringing you offers to buy...

- "Shares" or "interests" in foreign lotteries
- Low-cost vacations
- Magazine subscriptions
- Office supplies or promotional items
- Club memberships
- Sure-fire investments
- Vitamins

Do they say...

- You've just won a contest and only have to pay "shipping and handling" or a "small gift tax" and it's all yours?
- Or do they want your credit card number?
- If so, you may be the victim of a boiler room fraud

Direct Marketing vs. Boiler Room Fraud

- Direct Marketing is the sale of goods and services by direct contact with the consumer, by phone or mail.
- Boiler room fraud is the use of phone or mail by unethical companies that only want to take your money.

What do they salespeople say?

- "You've been specially selected to hear this offer."
- "You'll get a wonderful free bonus if you buy our product."
- "You've won a valuable free prize."
- "You've won big money in a foreign lottery."
- "This investment is low-risk and provides a higher return than you cannot get anywhere else."
- " You have to make up your mind right away"
- "You can put the shipping and handling charges on your credit card."

What are boiler room companies?

- Calls usually from firms located out of state.
- Sometimes they send an enticing or official-looking letter or postcard in the mail urging you to call them
- 900 numbers are often used, so you'll be billed just for calling them, even if you decide not to purchase what they are selling.

What if you fall for a boiler room pitch?

- You never receive any "winnings" from the foreign lottery you entered
- The merchandise you bought is overpriced and of poor quality
- The "free gift" never arrives, or it's worth just a fraction of the "shipping and handling" or "gift tax" you paid.
- The investment turns out to be nonexistent or a loser
- The donation you thought was going to charity goes into the fundraiser's pocket
- Unauthorized charges start appearing on credit card bills
- Con artists call and offer to help you get your money back... for a fee of course

How can you protect yourself?

- Hang up!
- Take your time… don't rush into accepting an offer
- Don't buy something merely because you'll get a "free gift"
- Get all info in writing before you agree to buy
- Check out the caller's record with your state's Attorney General's office and the Better Business Bureau
- Don't give your credit card or checking account number to anyone who calls on the phone or sends you a postcard
- Check out a charity before you give them any money. Check to see how much goes to the needy.
- Be extremely cautious about investing with an unknown caller who insists you make up your mind immediately

Watch dog alerts

- Stay up to date on the latest scams and get access to a network of people who can show you how to avoid being scammed. As criminals develop new ways to target victims, they will provide you warnings and critical information so you can always be on your guard.
- AARP Fraud Watch Network
- AARP is launching the Fraud Watch Network- a campaign to fight identity theft and fraud and give you access to information about how to protect yourself and your friends and family. Non-members and members alike can get our watchdog alerts, learn about active scams, and find resources about what to do to spot and avoid them.
- They're inviting anyone, of any age, to participate in the conversation free of charge just by visiting our website. Before fraud occurs, they are providing you with information about how to safeguard against identity theft and fraud. If you have been victimized, they are here to help you.
- Inside the Con Artist's Playbook
- Before fraud occurs, AARP Fraud Watch Network provides you with information about how to safeguard against identity theft and fraud and how scammers think so you can build up your defenses against the kinds of tricks con artists use.

SCAM TEST

1. You see an ad on television advertising gold coins. Is it a legitimate offer?
   - ❍ No, because gold coin sellers are notorious for exorbitant markups.
   - ❍ Maybe, maybe not.
   - ❍ Yes, because the station wouldn't run the ad if it were a scam.
   - ❍ Yes, because the price of gold is going up.

2. You get a call from this government agency. You don't believe it is legitimate. You could be right because more scammers pose as employees of this agency than any other.
   - ❍ The Internal Revenue Service
   - ❍ The Social Security Administration
   - ❍ The U.S. Postal Service
   - ❍ The Federal Unemployment Agency

3. Some websites charge $9.95 for voter registration or to change your political party. Is this a reasonable fee?
   - ❍ Yes, some sites charge as much as $20.
   - ❍ No. Many sites charge less than $5.00.
   - ❍ No. They can both be done for free elsewhere.
   - ❍ Yes, it's not the best rate, but it is reasonable.

4. A lot of scammers try to get your money via the charity route. It's a good idea to avoid donating to any charity that is not familiar to you. Which form of charitable solicitation is least likely to be a scam?
   - ❍ By e-mail/Internet
   - ❍ By phone
   - ❍ Door to door
   - ❍ By mail

5. The incidence of bedbugs is on the rise lately and so is the number of bedbug control scammers. Research entomologist Richard Pollack suggests this is the best method for ridding your house of bedbugs.
   - ❍ Ionic or ultrasonic devices
   - ❍ Aerosol "bug bombs"
   - ❍ An insecticide "cocktail"
   - ❍ Electromagnetic devices

6. According to Scam Alert, what type of organization is the most frequently victimized by hackers?
   - ❍ Hospitals
   - ❍ Large universities
   - ❍ Law enforcement agencies
   - ❍ Financial institutions

7. Congratulations! You just won $8,000,000 in the Jamaican lottery! You got that e-mail, you bit, and you wired them $400. That was a mistake. But it would be a much greater mistake if you did this.
   - ❍ Dialed the call back number for further instructions.
   - ❍ Notified the IRS of your good fortune.
   - ❍ Contacted the Jamaican Lottery.
   - ❍ Called the Better Business Bureau.

8. Scammers actually have a way to create a phone number that's familiar to you, such as your bank, appear on your Caller ID. This might cause you to reveal information that could lead to identity theft. What's this technique called?
   - ❍ Caller ID spoofing
   - ❍ The Phone Dupe
   - ❍ The Friendly Fakeout
   - ❍ Dial-a-Dope

9. You get a call from someone claiming to be from the electric company saying your electric bill is overdue. They ask for your account number for verification purposes, and your credit card number. Why is this probably a scam?
   - ❍ You're pretty sure you paid your last bill.
   - ❍ A representative would have your account number on screen.
   - ❍ You don't recall getting any past-due notices.
   - ❍ A representative would never ask for a credit card number.

10. According to the FBI, older Americans are frequent victims of Internet scammers because they have nest eggs and because of this.
    - ❍ They are not as adept on the Internet as younger people.
    - ❍ They tend to leave their computers on for long periods, making access easier.
    - ❍ They frequently are not even aware they have been swindled.
    - ❍ They are less likely to report being swindled.

ONLINE SAFETY TIPS

Keep a Clean Machine

- Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other webÐenabled devices also need protection from viruses and malware.
- Plug & scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information

- Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.
- Write it down and keep it safe: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Connect with Care

- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- Get savvy about WiÐFi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- Protect your $$: When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Be Web Wise

- Stay current. Keep pace with new ways to stay safe online. Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- Back it up: Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- Safer for me more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- Post only about others as you have them post about you.
- Help the authorities fight cybercrime: Report stolen finances or identities and other cybercrime to **http://www.ic3.gov** (Internet Crime Complaint Center), the Federal Trade Commission at **http://www.onguardonline.gov/file-complaint.**

Visit **http://www.stopthinkconnect.org** for more information.

PROTECTING YOURSELF FROM COMPUTER MALWARE

What is Malware?

- Malware is short for malicious software.
- Malware is software that is intended to damage or disable computers and computer systems.
- Malware is a broad term that covers a variety of different types of harmful software.
- Examples include adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms

Common Types of Malware

- **Ransomware:** is a form of malware that essentially holds a computer system captive while demanding a ransom. The malware restricts user access to the computer and displays messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer. Ransomware typically spreads via a downloaded file or through some other vulnerability in a network service.
- **Rootkit:** is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. A rootkit makes it possible for a malicious party to remotely execute files, access/steal information, modify system configurations, alter software, install concealed malware, or control the computer.
- **Spyware:** is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting, and more.
- **Trojan Horse:** commonly known as a "Trojan," is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer.
- **Virus:** is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.
- **Worms:** are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Worms have the ability to self-replicate and spread independently by sending mass emails with infected attachments to users' contacts.

Malware Symptoms

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves
- Strange computer behavior
- Emails/messages being sent automatically and without user's knowledge

Malware Prevention

- Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.
- Keep software and operating systems up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.
- Be vigilant when downloading files, programs, and attachments. Downloads that seem strange or are from an unfamiliar source often contain malware.

Malware Removal

1) Remove all floppy disks, CDs, and DVDs from your computer, and then restart your computer.
2) If you are using Windows XP, Vista or 7 press and hold the F8 key as your computer restarts. Please keep in mind that you need to press the F8 key before the Windows start-up logo appears.
3) If you are using Windows XP, Vista or 7 in the Advanced Boot Options screen, use the arrow keys to highlight Safe Mode with Networking, and then press ENTER.
4) Delete Temporary Files. Doing this may speed up the virus scanning, free up disk space, and even get rid of some malware. To use the Disk Cleanup utility included with Windows, select Start, All Programs, Accessories, System Tools, Disk Cleanup.
5) Run a scan with a malware scanner. If you don't have a malware scanner on your computer you will need to download one
6) Once the scan is done you will want to remove any malware that the scanner has found. Remember, no antivirus program can detect 100 percent of the millions of malware types and variants.

Malware Scanner Programs

- Malwarebytes Anti-Malware
- Availability: Windows 8.1, Windows 8, Windows 7, Windows Vista (32-bit, 64-bit), Windows XP (32-bit), Android
- Price: $24.95
- BitDefender Internet Security
- Availability: Windows, Mac, Android
- Price: $79.95 per year for three PCs
- Panda Free Antivirus
- Availability: Windows
- Price: Free
- Spybot Search & Destroy
- Availability: Windows
- Price: Freeware
- Ad-Aware Free Antivirus+
- Availability: Microsoft Windows 8/8.1 , Microsoft Windows 7 , Vista , Microsoft Windows XP SP3
- Price: Free

NATIONAL 4-H COUNCIL

About 4-H

4-H, the nation's largest youth development organization, grows confident young people who are empowered for life today and prepared for career tomorrow. 4-H programs empower nearly six million young people across the U.S. through experiences that develop critical life skills. 4-H is the youth development program of our nation's Cooperative Extension System and USDA, and serves every county and parish in the U.S. through a network of 110 public universities and more than 3000 local Extension offices. Globally, 4-H collaborates with independent programs to empower one million youth in 50 countries. The research-backed 4-H experience grows young people who are four times more likely to contribute to their communities; two times more likely to make healthier choices; two times more likely to be civically active; and two times more likely to participate in STEM programs.

Thank you!

We would like to thank the following contributors from the University of Georgia 4-H

Mentor Up Team:
Cheryl Varnadoe,
Principal Investigator Georgia 4-H Mentor Up Grant, Extension 4-H Specialist

Pamela Bloch,
Gwinnett County Extension Agent for 4-H and Youth Development

Jeremy Cheney,
Douglas County Extension Agent for 4-H and Youth Development

Learn more about 4-H at **www.4-H.org**

National 4-H Council
7100 Connecticut AveNUW.
Chevy Chase, MD 20815