Digital Safety & Security for Teens

Prepared for the Westminster Institute

By Cecil Rice

Overview

As far as information and collaboration, there has NEVER been a better time in history to be alive than there is today! With a smartphone some of you may have in your pocket, you hold all of the stuff that I would have had on the left when I was your age!
Unfortunately, because of this, a small mistake in judgement today could be MUCH more costly than ever before.

We've never been able to connect with each other better than we can today, but, we need to make sure to use a little caution and common sense to make sure that we don't get taken advantage of. Today's class will go over some of the different tools we can use to make ourselves safer in the digital world of today.

Plan and Path

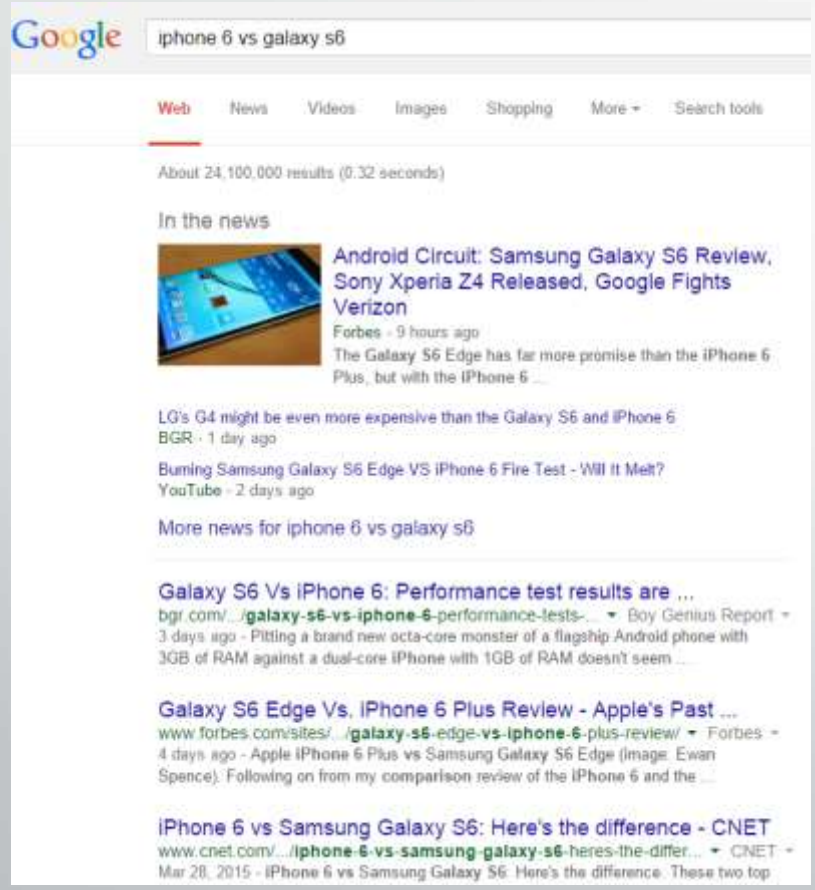
- ✓ Helping Out
- ✓ Personal Information
- ✓ Viruses & Digital Bugs
- ✓ Free Can Really Cost

- ✓ Smart Phones Need Smart Decisions
- ✓ Online Do's & Don'ts
- ✓ Social Media

Helping Out

In a lot of households today the best and the brightest when it comes to technology happen to be the folks more along your age than those along mine. Because of this, many teens are given the opportunity to help out around the house in ways that weren't possible before. Everything from what phones and TV's to buy to how to fix the washing machine can be found on the web and YOU can help be the superstar of the house by showing a few web saavy tricks that will make sure you don't get taken for a ride because of a flashy web page or you tube trickster.

Helping Out (continued)

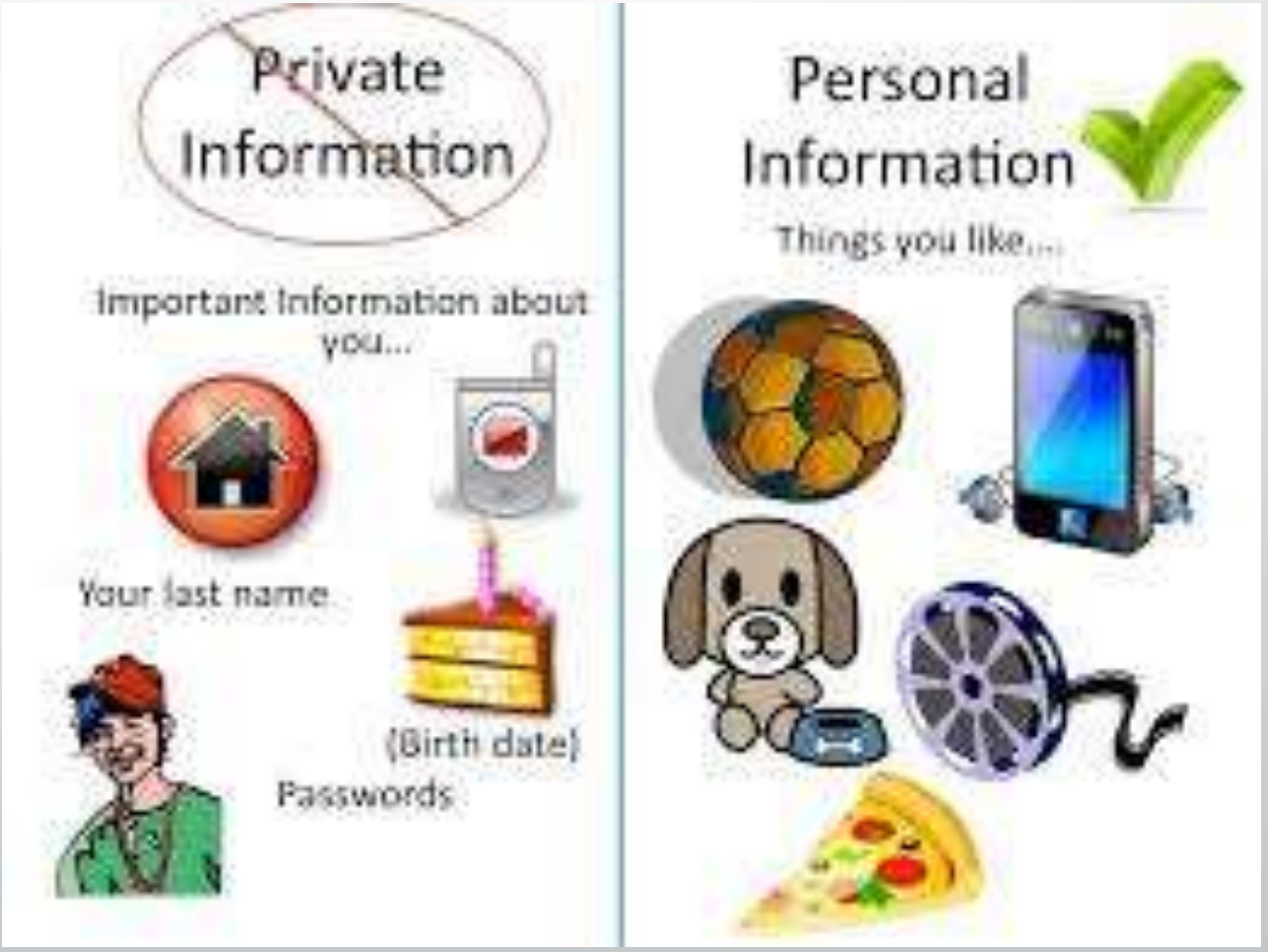


- ✓ Type specifically what you're wanting to find (for example, in the left I'd typed "iphone 6 vs galaxy s6" into the search box.
- ✓ Don't just look @ the first review, and always look to see WHERE the review came from! (in the example that I'd typed, there's articles from everyone from Forbes to BGR to PCTimes to SmartPhoneReviews.
- ✓ Read more than ONE review before making up your mind.
- ✓ If there's a bunch of negative reviews (not just one) then, there's usually something to be said for that.
- ✓ These search tricks work for phone numbers, mail, homework research, and many other questions that come up each and every day!

Personal Information

You'd never give out a bunch of personal information to someone that came up to you on the street and just started asking questions, but, you'd be amazed how many folks do JUST THAT when they're visiting a web site or signing up for a free app or download.

There are some tricks that you can use to help keep you safe, and, we'll go over them on the next slide, but, the MOST important trick is to ALWAYS get your mom or dad's "OK" before giving out ANY information on a new site or for a new app.



Personal Information (continued)

- When creating an e-mail address, make sure the address is something that you would be comfortable being called!
- Use 3 different passwords …
  - ONE only to log into your computer and email
  - ONE only for things that cost money
  - ONE for things online that don't cost money
- DON'T give out your passwords to ANYONE other than your parents.
- Never give out your address, phone number, or birthday to any site without asking your parents FIRST.
- Anything that you wouldn't be comfortable sharing with a stranger on the street, don't share on-line.
- Whenever you get e-mails asking to click on links, first, open up a search window and either copy and paste or type the subject from the e-mail into your search browser to see if it's a scam!

Some of this may seem a little "over the top" but, unfortunately, many kids have had their "online identities" taken over and their reputations run through the mud simply because they shared their password with a friend or entered personal information into a site they trusted only to find out later that the site (or the friend) wasn't what they'd expected.

Viruses & Digital Bugs

I considered putting this up with the "Helping Out" section, but, chose to put it here because, unfortunately, many of the sites that we were trying to ward you off of from the previous couple of slides are the ones that would share these wonderful bugs with you, so, think of this as "2 fold" … a reinforcement to the last section AND a way to be a superhero in your family ☺ …

First thing's first … every computer, smart phone, and tablet in your house SHOULD be running some sort of antivirus software … Second … NO computer, smart phone, or tablet in your house should have MORE than 1 antivirus software installed. (some recommendations for these are on the next page.)

Second … "free" stuff (whether it be software OR downloaded music/videos) have a MUCH higher chance of having viruses along for the ride!

Viruses & Digital Bugs (continued)

(below are some recommendations and where to get them)

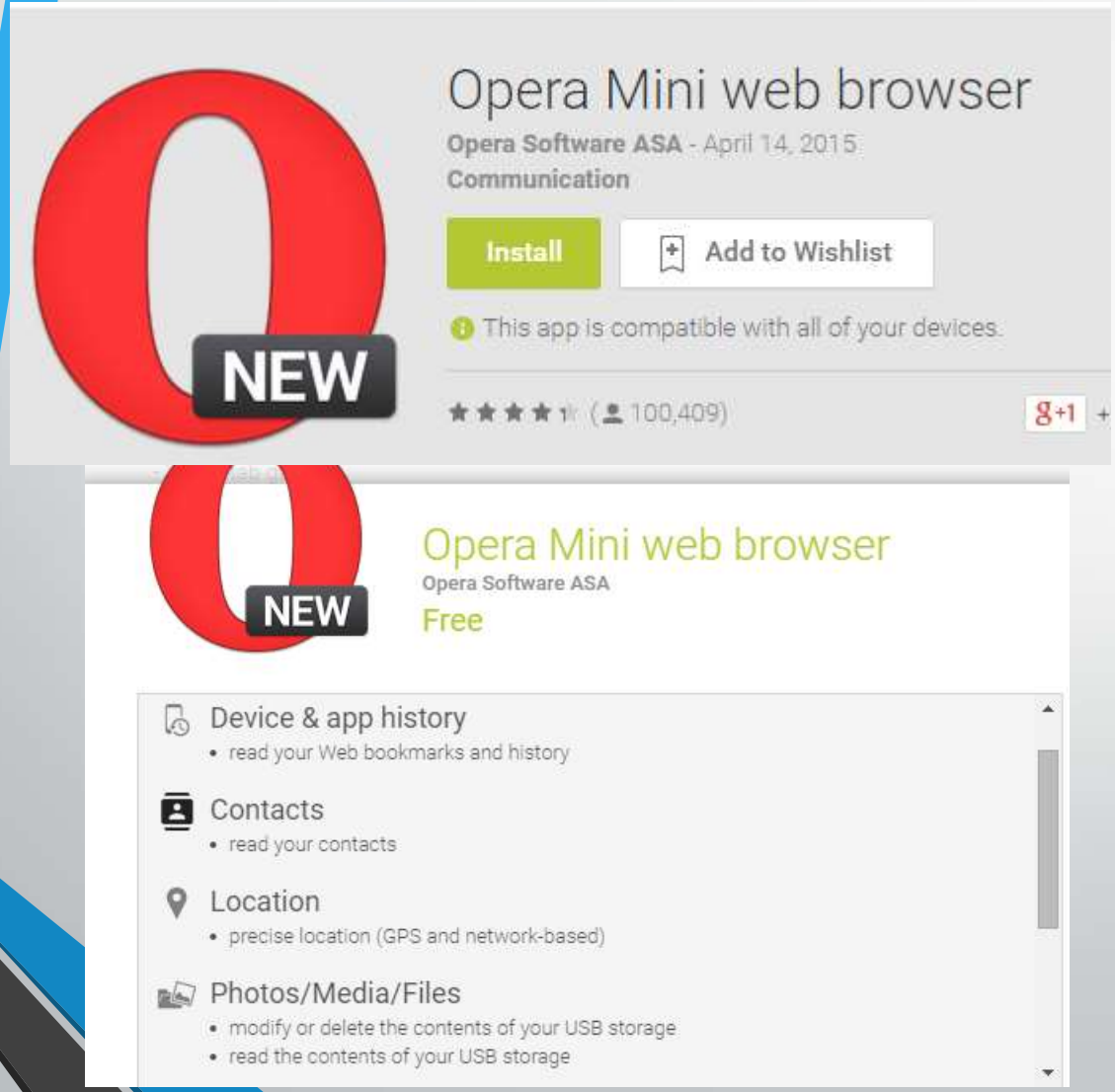
- ✓ Antivirus for Windows Vista and 7 – Microsoft Security Essentials
- ✓ Antivirus for Windows 8 – Windows Defender (already installed, you may have to remove pre-installed AV to enable it, to do that, simply go to a search window and type "remove {whats installed on your pc} from windows 8" … you'll be taken to uninstallers that will remove the pre-installed McAffe, Norton, or Kaspersky.
- ✓ Antivirus for MAC and Linux – ClamAV
- ✓ Antivirus / Security for Android – CleanMaster or LookOut
- ✓ Antivirus / Security for iPhones and iPads - LookOut
- ✓ Rescue Disk (for ALL Windows MAC and Linux) – Kaspersky Rescue CD
- ✓ Search Engines – Google, Yahoo, Wikipedia, Snopes

Free Can Really Cost

PLEASE remember that if you're not paying for an app with cash, then, they're making money some OTHER way … in 99% of the cases it's completely "ok" and above board, but, in that other 1% of the cases, that "free app" may do many things that you DON'T want it to do, such as spam your friends and family, redirect your internet searches through one of their servers, take the photos off of your phone, or, even worse, take CONTROL of your phone and take photos, record audio, or take videos from your phone without your knowledge!

On the next page, we'll go over a few helpful hints to make sure that your phone, computer, or tablet doesn't get "sick" because of a free app ☺ ….

Free Can Really Cost (continued)



- ✓ Check out how many downloads the app has had. This is usually located on the main screen of the app. If the app has 1000's of downloads, then, you know that others have downloaded it as well.
- ✓ View the apps requested permissions BEFORE downloading the app. These can always be found below the description of the app from the app store or google play store.
- ✓ Make sure that the app permissions make sense (for example, does an MP3 player really need to have access to your contact list?) … if the permissions don't make sense, move on and find a different app.
- ✓ Enter the app name into your search engine and see what comes up. The first few entries will usually be from the manufacturer, but, if the app has known issues, then, you'll also see a LOT of negative posts.

If you take 3 minutes and do the above 4 checks, there's a REALLY good chance that you WON'T be downloading malicious apps. The example I used on the left is a well known browser that does NOT have any malware.

Smart Phones Need Smart Decisions

First and foremost, everything that applies in this section ALSO applies to any tablets or other internet connected devices ☺ …
Today we live in a world where entertainment, communication, productivity, and documentation can ALL be handled by a single device, a device that many of us keep in our pockets, in purses, or on hips every day. It makes our lives SO much easier and gives us access to a wealth of information and entertainment no matter where we are.
Smart Phones DO make life easier, BUT, they can also open the user up to many negative consequences if they're not careful. This isn't to scare anyone away, just make you aware …

On the next page we'll go over some basic "do's and don'ts" for smart phones and tablets. If you do these things, you'll be much less likely to ever see any of those negative consequences.

Smart Phone / Tablet Do's and Don'ts

- ❑ DO keep a password, pattern, or fingerprint lock on your phone at all times. Have the timeout no more than 15 minutes.
- ❑ DON'T share your password with anyone other than family.
- ❑ DO keep antivirus software installed on your phone.
- ❑ DON'T download apps without first doing the 4 steps we'd talked about in the previous section.
- ❑ DO have contact information listed in the "screen lock," so, if you DO loose your phone and an honest person finds it, they can contact you (by e-mail) so you can get it back.
- ❑ DON'T list your address on this screen lock screen!
- ❑ DO leverage the cloud (iCloud, OneDrive, or Google) to store your documents, pictures, contacts, and calendar information.
- ❑ DON'T give out your password to the cloud to anyone other than family!
- ❑ NEVER have any "inappropriate" pictures on your phone or tablet, this can lead to life long consequences.
- ❑ NEVER text and drive.

Online Do's & Don'ts

In the next section we'll be talking about Social Media, so, we won't really cover it here, but, there are still a LOT of things to think about with online safety, namely e-mails, searching, scams, and, unfortunately, the newest one is the "pop up phishing" that's really causing lots of issues.

On the next page, we'll go over some basic "do's and don'ts" that should keep you pretty safe (and, these you'll want to share with your folks!)

Online Do's & Don'ts

- DO make sure that every device that can connect to the internet has antivirus protection on it.
- DON'T install more than ONE antivirus product on any device (this doesn't make it better, just slower and, in some cases, ineffective!)
- DO keep "pop-up blocker" in effect at all times on any browser you're using.
- DON'T click on ANY part of a pop-up that makes it's way through the pop up blocker (usually these come with a severe warning like "Your PC is Infected" or "This License Isn't Valid" … if you click **anywhere** on these warnings, it could install malicious software around you're A/V that you've installed!) … simply use CTRL+ALT+DEL and select "Task Manager" and then start killing any tasks that you don't recognize, as well as any ieplorer tasks.
- NEVER click on a link without "hovering" over it first to make sure that the link is going where it SAYS it's going to go (for example, what if I had on a webpage – visit our site at http://coolstuffforfree.com to win a prize, if you hover over that link, you'll see that it actually would take you to a completely different web site!
- NEVER click on any links that come from e-mail … even if they come from friends … instead, copy them and then paste them into your internet browser's address button.
- NEVER reply to an e-mail from a friend that looks like it didn't come from them … In many cases, "phishing companies" will get ahold of address books (see the section on "Free Can Really Cost" to find out how!) and then send out e-mails to everyone in their address book, pretending to be them. If you respond (even to say you're not interested, then, that company could have those responses redirected and now they have VALIDATED that you are a real person! … Instead, if you get one of these e-mails, delete it and then e-mail your friend directly and let them know … they can then change their passwords and also let everyone know NOT to open e-mails that don't look like they're coming from them!

Social Media

Whew … we've made it to the end, but, we have definitely saved the best (and worst!) for last … Social Media … Social Media has taken off wilder than anyone could have possibly expected. It allows us to be more connected with friends and family than we've ever been before, and, it's a GREAT think, heck, our church uses at least FOUR forms of social media each and every week to share the Good News and our church family events!
On the next slide, we'll go over some basic rules that, if you follow, you'll have a GREAT experience and no regrets later on!

Social Media Suggestions

Like we'd mentioned on the previous slide, Social Media has quickly become an intricate part of society and, as time passes, NOT being "plugged in" could lead to you missing out on things (for example, there are several things that we share on our church Facebook page that can't be found in fellowship hall even today!) Social Media CAN be misused, but, as long as you remember a few simple pointers, you should be just fine…

- Take the time to go through the Privacy settings on any site you wish to join. Make the "public" profile very limited and only allow "friends" or "circles" to see your posts and pictures. Also, it's a good idea to NOT allow your friends to repost your pictures.
- Any site you wish to join, talk to your parents about it. We strongly recommend that your parents join as well as become a "friend" or join your "circle" … Not to snoop on you, but, to keep you safe.
- NEVER put anything on a site (even in private messages) or on text messages that you wouldn't want your parents, your preacher, and your principle to read. We're not saying that any of the 3 would read them, BUT, once you've put it out on the internet, it's there for LIFE. You may be looking for a job after college and be turned down because of a picture you posted on Facebook while on a "wild spring break" weekend.
- If you're being bullied online, don't be afraid to let your parents know … this is a very serious problem today and if we all work together, we can stop it.
- Don't accept friend or circle requests from folks you don't know. If you're not sure, then, check with your parents first (your great aunt from Montana may want to friend you, which would then be "ok" ☺) … If your parents are friends with you or in your circles, this makes this step very easy!
- Finally, never post really private information (such as your address, phone number, or where you'll be) on ANY public message board.

For your time today ☺ … if you ever have any questions about what's listed here or anything else on-line, don't hesitate to e-mail me (webmaster@wbts.org) or message me on Facebook and I'll always give you my honest, unbiased, opinion ☺ …