

Digital Citizenship

Safely navigating the digital landscape



Agenda

- How Predators Gain Entry
- 5 Good Digital Habits for Families
- Video Game Safety
- Tips and Tools for Online Safety
- More Resources

github.com/davemehi/internet-safety

Technology and our daily lives





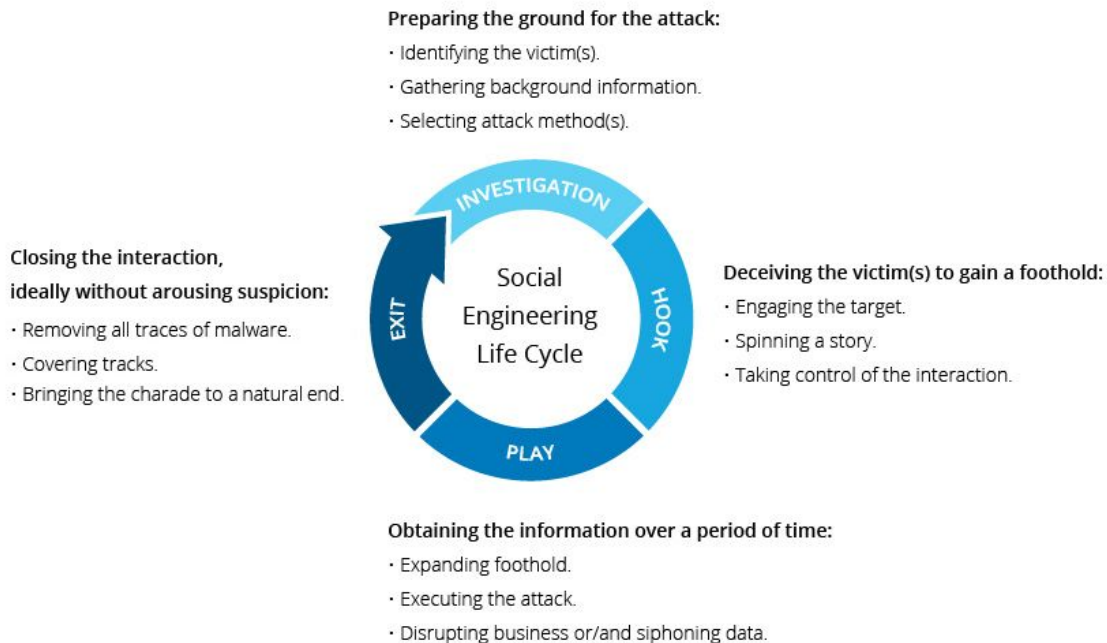
How Predators Gain Entry

How Predators Gain Entry

- Social Engineering
- Phishing
- Smishing
- Vishing
- Sadfishing
- Malware
- Unsecure WIFI and Websites

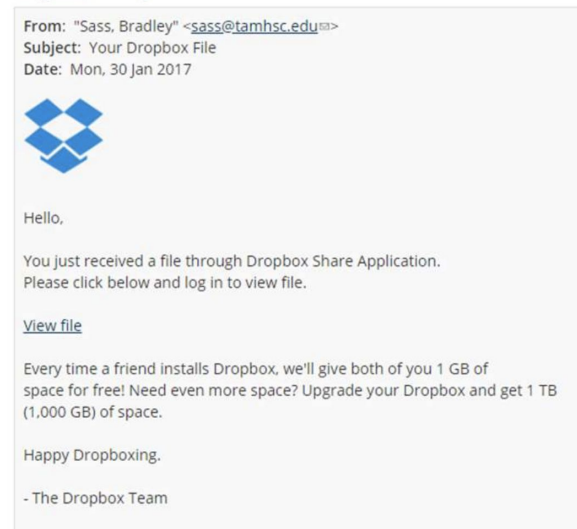
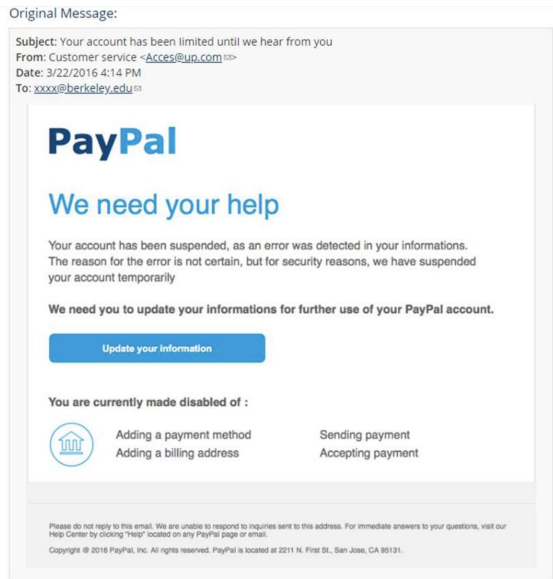
Predators: Social Engineering

A broad range of malicious activities using psychological manipulation to trick users into making security mistakes or giving away sensitive information.



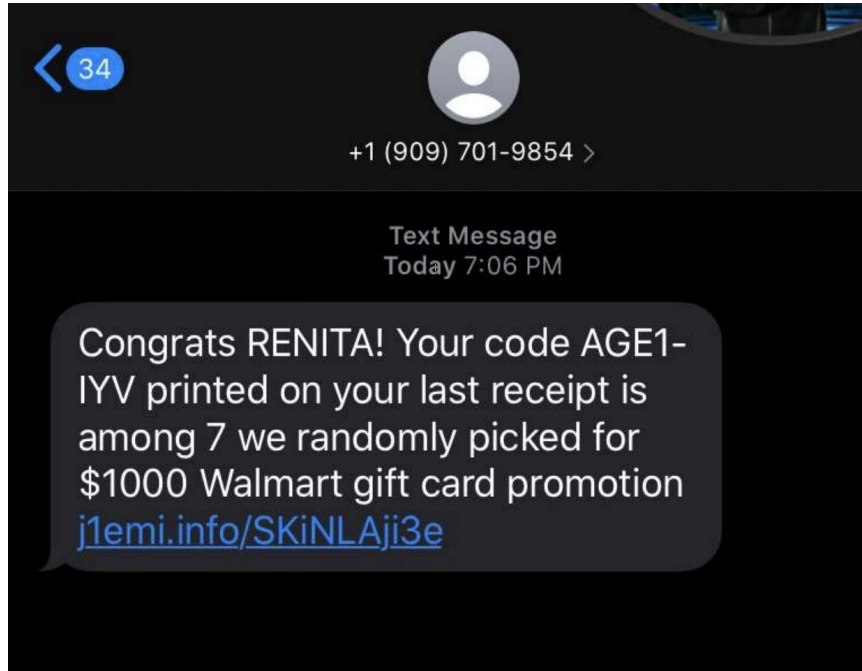
Predators: Phishing

Attacks typically involves cyber criminals impersonating a person or organization and using various tactics to extract information or compel the victim to perform a particular action.



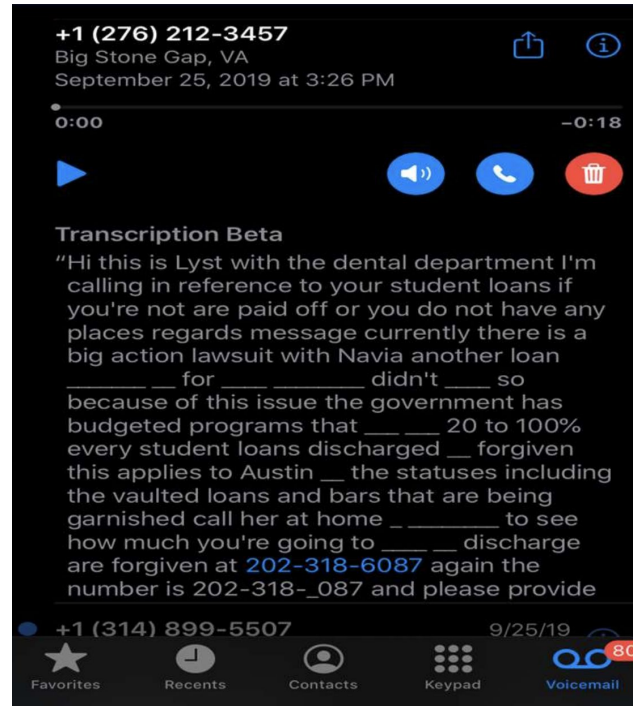
Predators: Smishing

Fraudulent practice of sending text messaging purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.



Predators: Vishing

A form of scam that aims to get prospective victims to share personal or financial information over the phone.



Predators: Sadfishing and Other Tactics



Sadfishing is a term used to describe the behaviour of someone making **exaggerated** claims about their **emotional state** to gain sympathy. Hackers can take advantage of this.

"I'm really in a bad spot right now

... 🙄 😡 ... I could really use some help 😭"

"Guess what! I got an A on my final exam! YES!!!! I'm so HAPPY!"

Predators: Malware

Software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system.

9 Types of Malware and How to Recognize Them

- Standalone piece of software
- Reproduces itself
- Spreads from computer to computer

Worm

- Piece of computer code
- Inserts itself within the code of another standalone program
- Forces programs to take malicious action
- Spreads itself

Virus

- Program
- Does not reproduce itself
- Acts like something the user wants and tricks them into activating
- Once activated it does damage and spreads

Trojan

- Computer software
- Secretly gathers data on an unsuspecting user (computer use, and data sent & received)
- Sends information to a third party
- Great for stealing passwords

Spyware

- Computer program or, more often, a collection of software tools
- Gives hacker remote access to and control over a computer or other system

Rootkit

- Computer software
- Forces internet browser to redirect to web advertisements
- Tries to download more malicious software
- Piggybacks onto tempting "free" programs like games or browser extensions

Adware

- Software
- Encrypts hard drive's files
- Demands a payment, usually in Bitcoin, in exchange for the decryption key

Ransomware

- Crypto mining software that infects your computer
- Uses computer CPU to mine Bitcoin for attacker's profit.
- Runs in the background on the operating system or even as JavaScript in a browser window.

Cryptojacking


- Uses legitimate ads or ad networks to deliver malware to unsuspecting users' computers
- Code in the ad either redirects them to a malicious website or installs malware on their computer
- May also be embedded in an ad and execute automatically without any action from the user


Malvertising



Predators: Unsecure WIFI and Websites

- Beware of Public WIFI - offered in many public places like coffee shops, libraries and airports.
- Be very careful to use WIFI connections that do not use a password.
- Look for **https** in the web address of every page they visit . (The “s” stands for secure.)
- Look for the small lock icon next to the web address.
- Always log out of your account or website
- Be careful about letting your browser save your username and password
- Free games, apps, music, and other downloads can hide malware.
- Don't download anything unless you trust the source.



 google.com



5 Good Digital Habits for Families

Be Internet Awesome.

<https://beinternetawesome.withgoogle.com>



5 Good Digital Habits for Families

- **Smart**, Share with Care
- **Alert**, Don't Fall for Fake
- **Strong**, Secure Your Secrets
- **Kind**, It's Cool to Be Kind
- **Brave**, When in Doubt, Talk It



Be Internet Awesome.

<https://beinternetawesome.withgoogle.com>

Be Internet

Smart

Tips to help you be smart online



- Be a positive presence online, just like in real life
- Think before you post. **Ask yourself: Should I really post/share this??**
- **Activity: Talk as a family about what is and is not allowed to be posted and shared**
 - What can you share with family?
 - What can you shared with people outside the family?

Be Internet Alert

Tips to help you be alert online



- **Figuring out what's real and what's fake is vital to online safety and citizenship.**
- Double check a site for safety and credibility.
- Learn to differentiate between an advertisement and real content
- Be aware of offers that sound too good to be true
- Learn how to search and verify information before sharing
- **Activity: Talk about fake articles, do search exercises**

Be Internet

Strong

Tips to help you be strong online



- **Avoid sharing personal information online** (SSN, addresses, birthdates, Maiden names, etc)
- **Create a screenname that does not include personal information**
 - jessicaparra2005
 - pumpkinpie123
- Create strong passwords. Do not re-use passwords on multiple accounts



Activity: Sit down as a family and create a good set of screen names and strong passwords for practice.

Passwords:

- Has 10 characters or more
- Includes numbers, upper case, lower case and symbols
- Use memorable phrases mixed with numbers and symbols

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Be Internet Kind

Tips to help you be kind online



- Treat others how you want to be treated, both online and in real life.
- **Define what positive behavior means in your family.**
- **Activity: Have a discussion on what kinds of actions and behavior are important.**
 - **Think about what that looks like digitally: texts, posts, comments, photos, and videos.**

Be Internet

Brave

Tips to help you be brave online



- Found something negative? Say something!
- **It takes courage and bravery to speak up**
- Report and/or block inappropriate content
- **It's important for kids to understand that they're not on their own**
- Discuss family attitudes and policies about what is and isn't acceptable usage of devices and media, and when.
- **Activity: Discuss online situations and how they should be handled**



Video Game Safety

Video Games Then vs Now



Video Games Now

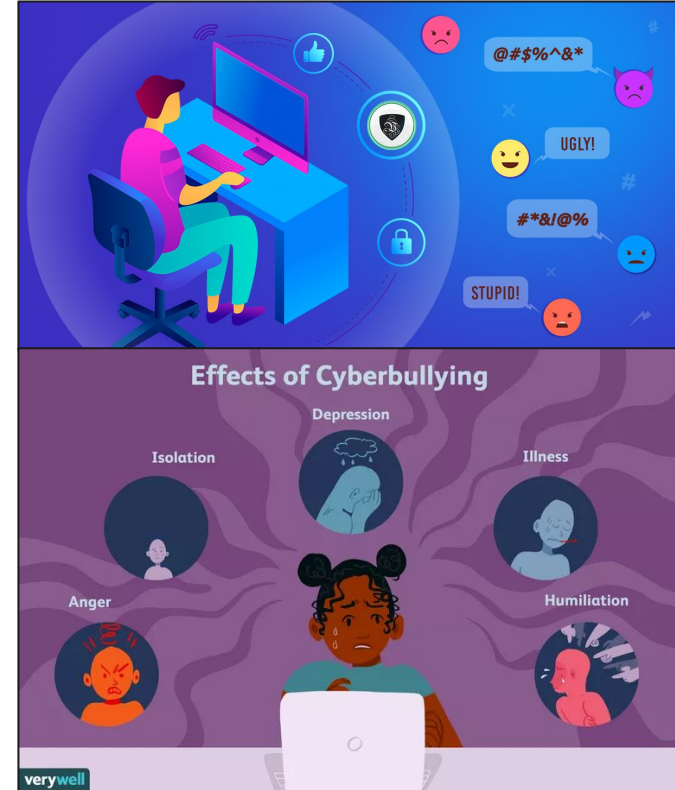
Games today are ...

- Online and integrated with the internet
- **Designed to be social, multi-player**
- Trendy and incorporate popular music, movie characters and celebrities
- **Epic Adventures in new virtual worlds**
- Creative gameplay



Video Game Risks

- Cyberbullying
 - Griefing - Making the game less enjoyable
 - Kill stealing - Stealing targets, coordinated efforts against players
 - Whispering - Bad-mouthing players in chat
 - Doxxing
- Privacy
 - Screen names
 - Delete info before disposing or selling
- Personal Information
- Webcam worries



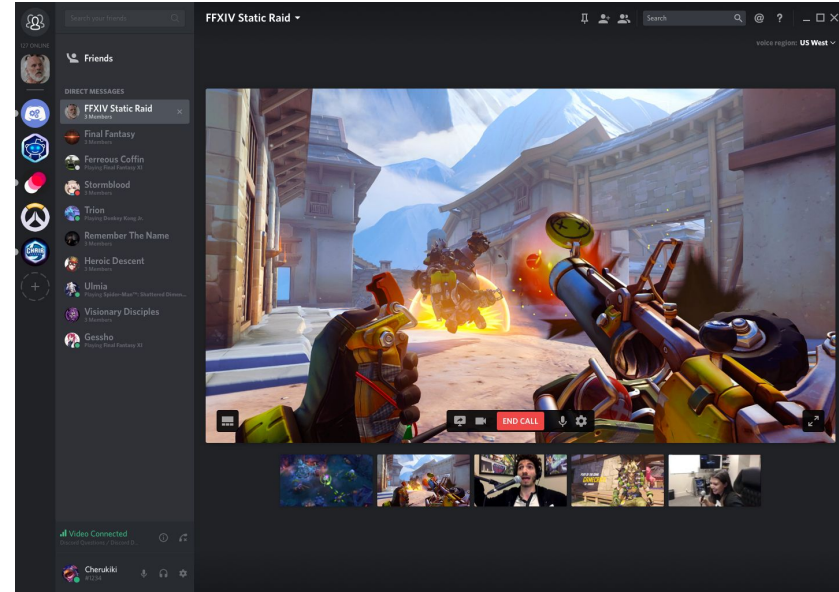
Video Game Risks

- Malware
 - Downloading unknown games from unknown sites is a risk
 - Check recent reviews, cyber-security programs, research
 - Beware “cracked” games or “cheats”
 - Consider keeping the gaming computer for gaming purposes only
 - Install cyber-security software



Video Game Risks

- Online chat
 - Giving away personal information
 - Engaging with strangers
- Online predators
 - Shared experiences
 - Build relationships through “understanding”
- Squads
 - Racist language
 - Sexist language



Video Games Financial Risks

- Due to the pandemic, the **Video Game Industry is bigger than the movie and sports industry combined! \$180 billion in sales in 2020!**
- The eSports is growing very fast. Total esports viewership is over 500 million people.
- eSports on track to earn over \$1 billion
- **Many games offer ‘In-game’ or ‘in-app’ purchases (Freemium)**
 - Expanded functionality, virtual currencies, weaponry, special abilities and even new dance moves!
 - Beware giving out credit card and saving it in the game
 - For Apple/Google stores, use password confirmation on purchase
- Be aware of purchasing in-game items or game help from people online

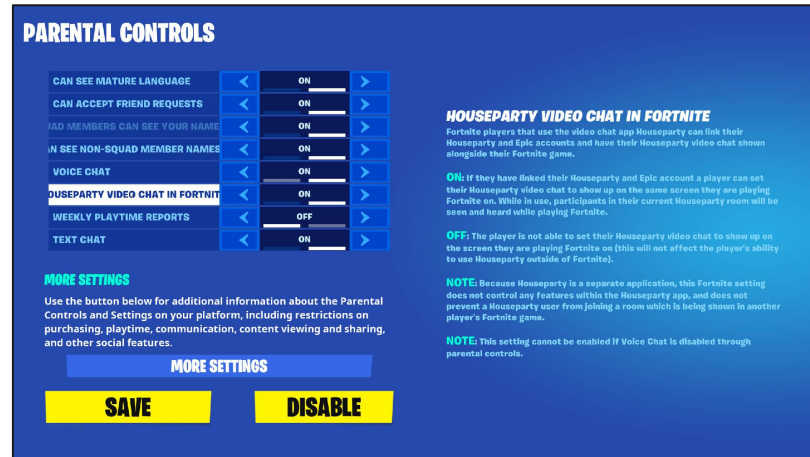
Video Games Health Risks

- Gaming Addiction
- Mainly sedentary - encourage movement and motion
- Take breaks and move around
- Dealing with stress and anger
- Effects of Cyberbullying
 - Depression and Anxiety
 - Sleep disturbances
 - Academic decline



Video Games Security Settings

- Most games have privacy settings and parental controls - find them and configure them
- Disable chat
- Disable webcam
- Review game ratings
- Be careful of credit card information
- Find parental guides to many games/apps here:
<https://nationalonlinesafety.com/>



PARENTAL CONTROLS

CAN SEE MATURE LANGUAGE	<	ON	>
CAN ACCEPT FRIEND REQUESTS	<	ON	>
AD MEMBERS CAN SEE YOUR NAME	<	ON	>
IN SEE NON-SQUAD MEMBER NAMES	<	ON	>
VOICE CHAT	<	ON	>
HOUSEPARTY VIDEO CHAT IN FORTNITE	<	ON	>
WEEKLY PLAYTIME REPORTS	<	OFF	>
TEXT CHAT	<	ON	>

MORE SETTINGS
Use the button below for additional information about the Parental Controls and Settings on your platform, including restrictions on purchasing, playtime, communication, content viewing and sharing, and other social features.

HOUSEPARTY VIDEO CHAT IN FORTNITE
Fortnite players that use the video chat app Houseparty can link their Houseparty and Epic accounts and have their Houseparty video chat shown alongside their Fortnite game.

ON: If they have linked their Houseparty and Epic account a player can set their Houseparty video chat to show up on the same screen they are playing Fortnite on. While in use, participants in their current Houseparty room will be seen and heard while playing Fortnite.

OFF: The player is not able to set their Houseparty video chat to show up on the screen they are playing Fortnite on (this will not affect the player's ability to use Houseparty outside of Fortnite).

NOTE: Because Houseparty is a separate application, this Fortnite setting does not control any features within the Houseparty app, and does not prevent a Houseparty user from joining a room which is being shown in another player's Fortnite game.

NOTE: This setting cannot be enabled if Voice Chat is disabled through parental controls.

MORE SETTINGS

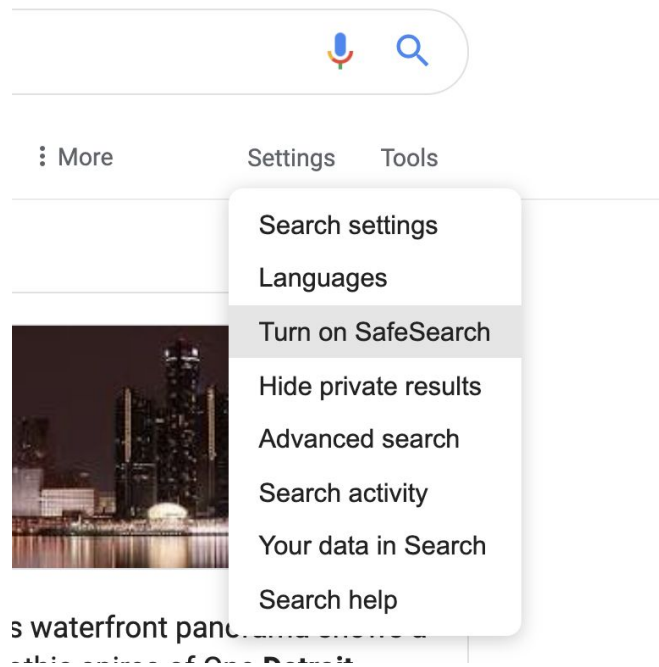
SAVE **DISABLE**



Tips and Tools For Online Safety

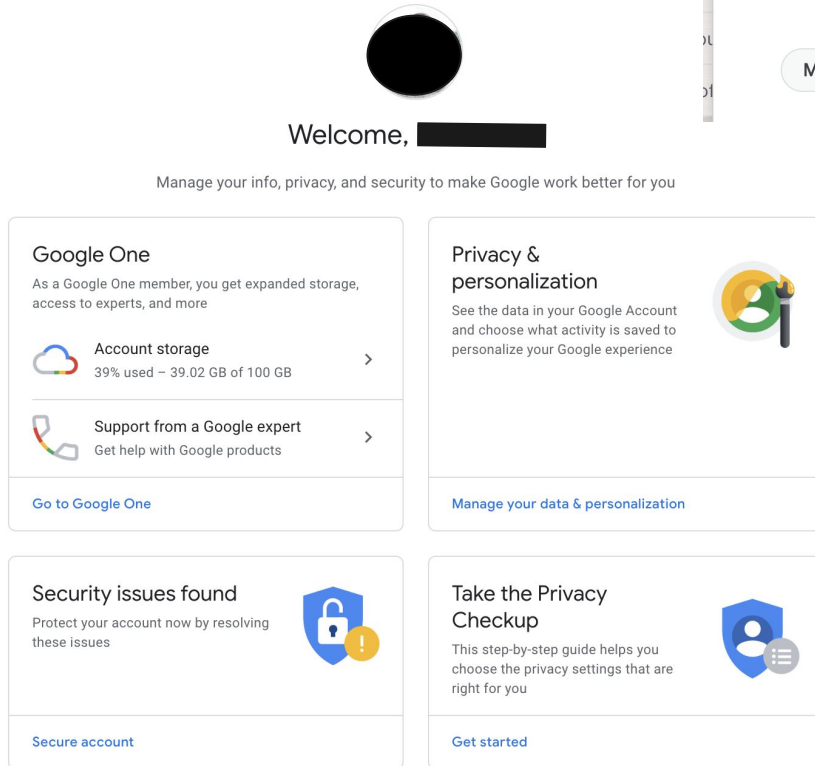
Google Safe Search Settings

- Turn on **safe search** for your account
- When SafeSearch is on, it helps filter out explicit content in Google's search results
- While SafeSearch isn't 100% accurate, it's designed to help block explicit results, like pornography
- SafeSearch turned on automatically for users under 13



Google Account Privacy Settings

- Click upper right photo of yourself (need to be logged in)
- Click “Manage Your Google Account”
- Click “Privacy & Personalization” to see the data and activity that is saved.
- Click “Take the Privacy Checkup” to see your privacy settings.





Welcome, [REDACTED]

Manage your info, privacy, and security to make Google work better for you

Google One

As a Google One member, you get expanded storage, access to experts, and more

 **Account storage** >
39% used – 39.02 GB of 100 GB

 **Support from a Google expert** >
Get help with Google products

[Go to Google One](#)

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

[Manage your data & personalization](#)

Security issues found

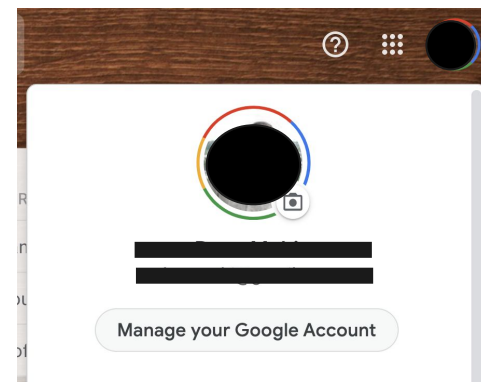
Protect your account now by resolving these issues

[Secure account](#)

Take the Privacy Checkup

This step-by-step guide helps you choose the privacy settings that are right for you

[Get started](#)




Google Security Checkup

- Tool to check security of your Google account

<https://myaccount.google.com/security-checkup>

Security issues found

Protect your account now by resolving these issues







[Secure account](#)




Security Checkup

1 issue found

	Your devices Remove your account from Google Chromebook Pixel (2015)	▼
	Recent security events No events in 28 days	▼
	2-Step Verification 2-Step Verification is on	▼
	Third-party access 3 apps with access to your data	▼

Password Checkup

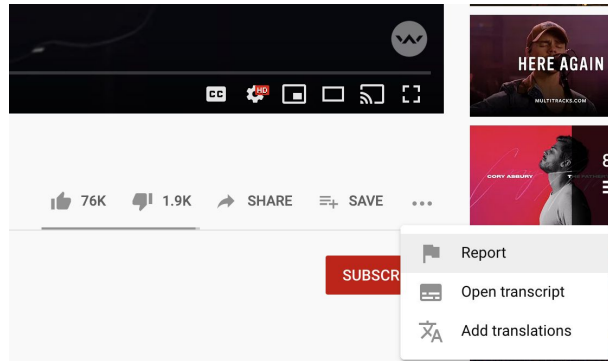
Check your 161 saved passwords for security issues



Youtube Settings

- Restricted Mode (Safe Mode) is an optional setting that screens out potentially mature content
- Click Account Photo at the top right
- At the bottom, click “Restricted Mode”
- Click “Activate Restricted Mode”

- Report content as inappropriate



← Restricted Mode

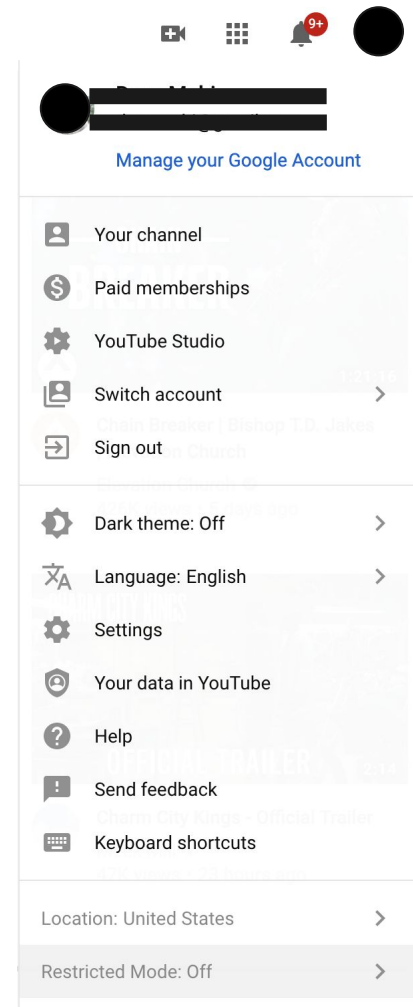
This helps hide potentially mature videos. No filter is 100% accurate.

This setting only applies to this browser.

ACTIVATE RESTRICTED MODE

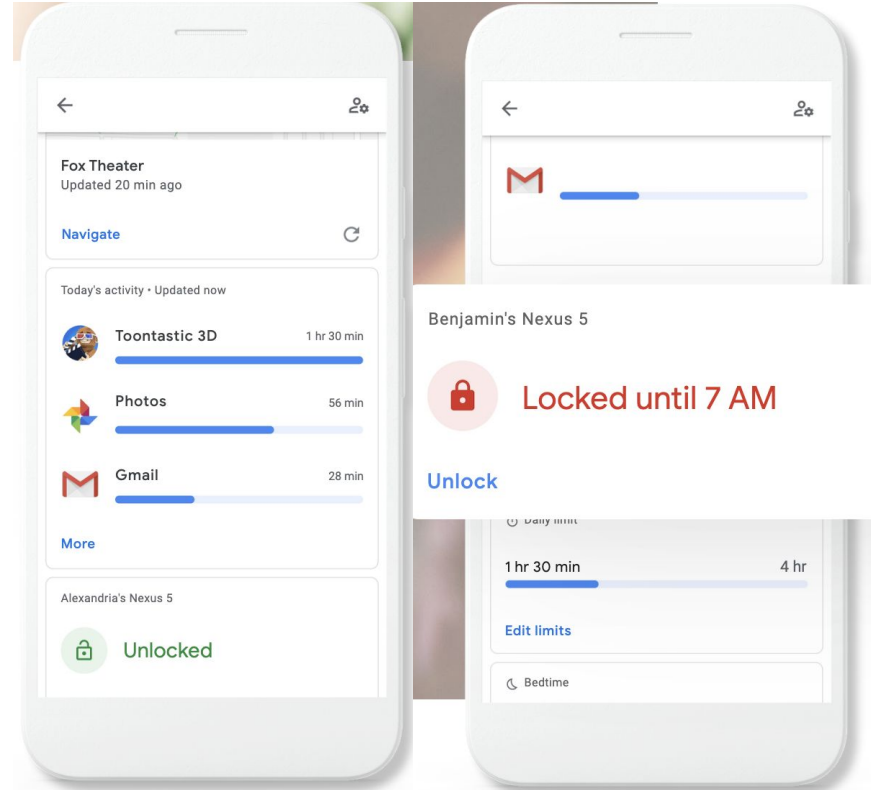
Restricted Mode lock prevents others from changing the Restricted Mode settings on this browser.

Lock Restricted Mode on this browser



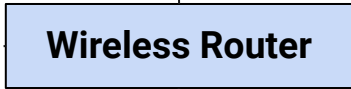
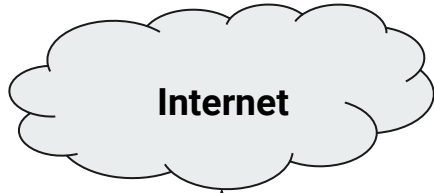
Family Link / Qustodio

- Family Link is an app by Google that will help set digital ground rules
- Keeps an eye on screen time
- Remotely lock devices
- See where they are (geolocation)
- App download warnings and approvals
- Available for both Android and iPhone
- <https://families.google.com/familylink/>
- Qustodio is an alternative free software to monitor your children's device usage

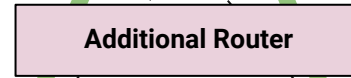
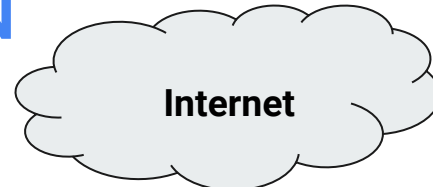


Security Setup: Home Routers / VPN

Default



**ATT
U-Verse
Xfinity**
(Limited
Parental
Controls
available)



**Recommended
Approach**

**(4) Additional
Parental
Controls**

**(3) Parental
Controls
available**

**(1) Security
Software
installed on
devices**

**(2) Configure
game/app
security
settings**

No Silver Bullet - Use a Layered Approach for Security

- Use software like FamilyLink or Qustodio that is installed directly on the phone or device.
- Use parental controls on the home WIFI router. If your provider does not have one, you can buy another wireless router that does
- Use a VPN that filters content
- Use random checks
- No private use of devices in the bedroom
- Seek out game or app specific security settings

It is complicated, but it's too important not to spend time to figure it out.

Privacy Tips

When you're on a website, try to remain as anonymous as possible. That means keeping all private information private. Private information that you should never allow the public to see includes:

- Your full name
- Location sharing
- Any type of photograph (even of your pet!)
- Your current location (some phones have automatic GPS apps built in that may need to be turned off)
- Home or school address or the address of any of your family or friends
- Phone numbers
- Social Security number
- Passwords
- Names of family members
- Credit card numbers

Additional Security Tips and Tools

- Apple/Android - Password check when downloading apps
- 2-Factor Authentication (2FA)
- Cover for the webcam (laptops)
- How to remove personal information from Google
 - <https://support.google.com/websearch/troubleshooter/3111061#ts=2889054,2889099>
- Phone
 - Location sharing
 - Popular apps and sharing data
- Virus, safety software
- Lifelock - Identity Theft
- Emails
 - Don't open from those that you don't know
 - Use Gmail, or other reputable email provider



Additional Resources

Other Apps to Be Aware Of

- Snapchat
 - Messages disappear, Location tracking on by default
- Tik Tok and similar apps
- Chat-based apps
 - Chatspin, Chat Master, Among Us, Kik
- Social Media
 - Facebook, Instagram, Ask.fm
- Twitch and other live broadcasting apps
- **Use the security setting to need approval to install an app.**
- There are too many apps to list and new ones are being created all the time
- Must keep on top of the latest

Tips for Parents

Stay involved, Learn, Join In

Keep talking and stay interested in what they're doing. Don't be afraid to bring up challenging issues like sexting, pornography and cyberbullying. It could be embarrassing, but you'll both benefit from the subjects being out in the open.

Keep their information private

Your child can set privacy settings on most social networking sites so that only close friends can search for them, tag them in a photograph or share what they've posted.

Stay safe on the move

Use safe settings on all mobile devices but be aware that if your child is accessing the internet using public WiFi, filters to block inappropriate content may not be active.

Tips for Parents

Be responsible

Talk to your teenager about being responsible when they're online. Children often feel they can say things online that they wouldn't say face-to-face. Teach them to always have respect for themselves and others online.

Talk about online reputation

Let them know that anything they upload, email or message could stay around forever online. Remind them they should only do things online that they wouldn't mind you, their teacher or a future employer seeing. Get them to think about creating a positive digital footprint.

Show you trust them

If you can afford to, give them a small allowance that they can use for spending online so they can download apps, music and films for themselves, from places you agree together.

Real Parent Stories

A teenage girl (15) sent my son's cousin (16) a very inappropriate video. He sent it to my son (13) and other kids. My son deleted the video but didn't tell me at first. Soon the video went viral in the school. The girl's parents found out and called the police. The detective said he has a huge pile of similar cases on his desk and can't get to them all. The son was cleared but his cousin may get in real trouble for distributing child pornography.

My 12yo daughter was getting a few messages from guys in their 20's on snapchat. These were friends of friends. One kept bugging her for the Netflix/Amazon passwords. Others asked borderline questions like what time does she go to bed and when does she go to the library. She didn't respond and we blocked them. We have had lots of talks about social media safety

Lots of periodic checks on their phones. We have a no-shaming policy at our house. No screen time and everything is off by 8pm. 2 hour time limit. The rule is we can check at any time and we always have their passwords. But most important is real discussion about the impact of social media. We really talk with them about when it can be harmful, what should set off a red flag, what you should never do since you can't take it back, and respect of yourself and others.

This is difficult with ever-changing new apps and trends. We do random phone checks regularly. We didn't know Snapchat had a location tracking feature until one of our boys was being followed by a young girl!

“

At the end of the day, no law or regulation can take the place of parental engagement and guidance. Companies, parents, teachers, civil society groups and policymakers must work together in a cooperative and collaborative way to address specific challenges that minors face online and to promote best

“

practices for online safety.

Important Resources

- https://beinternetawesome.withgoogle.com/en_us/
- <https://safety.google/>
- <https://www.internetmatters.org/advice/14plus/>
- <https://www.internetmatters.org/resources/monitoring-apps-parents-guide/>
- <https://nationalonlinesafety.com/> - Features guides to many popular apps/games
- <https://nationalonlinesafety.com/training>
- <https://smartsocial.com/app-guide-parents-teachers/>

Use Technology for Good

- Don't be afraid of technology
- We need software developers, graphics designers, story tellers
- Many learn young
- Use the technology for good
- Have a positive impact to the world around you



Use Technology for Good





Thank you