15 DIGITAL SAFETY RULES EVERY HOUSEHOLD SHOULD FOLLOW

TECHNOLOGY RULES 101

A publication by uknowkids.com

Table of Contents

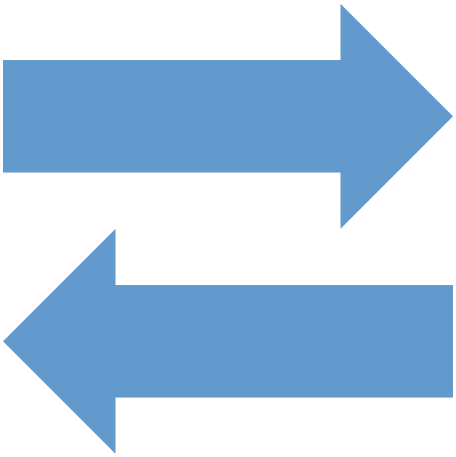
INTRODUCTION

The Basics

There are so many worries for a parent today when it comes to keeping kids safe online. The good thing is that with good communication and clear rules, you can easily help kids establish boundaries.

The basics for your child:

- Don't add people to your social network whom you don't know in real life.
- Don't download or purchase anything without permission.
- Don't use inappropriate language in a post or include rude comments, bad language, or improper pictures, and, if others post those things, remove them from your account.



Trust goes both ways. Your kids will trust you if they know you trust them, too. Good communication will ensure that your teen doesn't feel the need to lie about Internet activity, and monitoring online behavior ensures that you're not missing something critical. Monitoring your children is important, if for no other reason than to have an accurate picture of what your kids are doing online and how much they're doing it.

Remember, it is your job to defend your children and guide them into making the best decisions in life, and that sometimes requires that you interfere to resolve a potentially dangerous situation. Giving your child privacy should not mean complete lack of parental involvement, and ensuring safety is more important than his or her desire for privacy.

ONE

Lock Down Privacy Settings

So many personal profiles — so little time. But one thing you definitely need to make time for is checking your children's privacy settings on their social media accounts, from Flickr to Tumblr to Facebook, Twitter, and more. Settings likely default to *public*, so this is a very critical rule.

And locking down your teen's information isn't as easy as just clicking "private." For some teens, having as many friends as possible is a status symbol. They may have hundreds of "Friends" on Facebook, some of whom are really only distant acquaintances or complete strangers. If this is the case, then selecting "Only Friends" isn't enough. Talk to your kids about restricting their Facebook friends to only people they know personally, and teach them how to customize security settings.

Applications that run through Facebook, such as photo sharing and games, can access users' personal information unless you change the application security settings. And Facebook updates their policy frequently, so you can't

just check once and be done. Double-check them every six months or so, just to be safe.

Remind your kids that Facebook posts and tweets are public, so they should not put anything up that they wouldn't say to someone in person or would be embarrassed to have their school principal read.

TWO

Limit Personal Information Online

It might seem like common sense to never give out your private password to anyone but sometimes kids need a reminder.

Never post, put in an online profile, or share with someone you don't know in real life the following things:

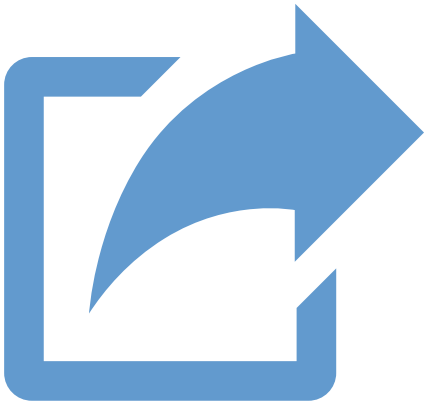
- full name
- address
- telephone number
- parents' work address/telephone numbers
- school name and location
- names of siblings

Children should never post identifying information such as a sports team that they play for, the names of their pets, or the names of siblings, all of which could be used by a predator to fabricate a connection with the family and gain your child's trust.

Children should never discuss on public forums specific places that they will be or things that they will be participating in at certain times. Predators or stalkers can get a significant amount of information, such as where a child lives or hangs out, from simply looking at the background of a picture.

THREE

Don't Overshare: Posts are Permanent



This next rule is one of the most important rules you can enforce. Don't overshare. Posts are permanent. Even after you've deleted them, people can dig up unflattering photos and opinions if anyone, anywhere has downloaded, captured, reposted, or shared them.

Why does it matter? A photo of underage drinking could prevent a child from getting a job years in the future. Mean words your child posts about a peer can have terrible consequences. Children and teens don't have the long-term perspective to imagine that small actions now could haunt them later.

Your children might think it is cool or popular to share every detail on social media sites and blogs, but you need to reinforce that not everything is meant for the public eye. You should have your child imagine how he or she would feel if his/her teachers, classmates, grandparents, or future employers visited his/her blog or Facebook page?

FOUR

You Don't Really Know Someone You Have Never Met

Let the experience of college football player Manti Te'o, who was duped in an online relationship, serve as a warning to your children. Until they have actually met someone, they don't really know that person, even if they have spoken on the phone and interacted online.

Kids need to be aware that the possibility exists that the person on the other end of the profile isn't really what he or she claims.

Predators (and even just ordinary, mean people) can use a false persona to build up relationships with children and teens online and eventually set up a time to meet them. Tell your child to be skeptical of every person they do not personally know and have not met in person. Photos can be taken from someone else's profile or from various other sources, and personal information can be made up. If something or someone seems too good to be true, that might be the case.

Advise your child to stay away from strangers, not just on the street but also online. Ask how your kids know each person on their friends list, and monitor additions. They should never go unaccompanied to meet someone they don't know.

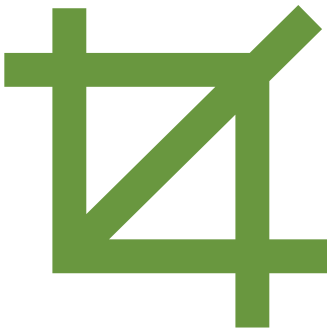
FIVE

Privacy in Photos & Videos

Sharing photos is a fun way to interact through social media, but of course, as with anything else that goes online, there should be considerations before posting.

Tell your children to abide by these rules before posting:

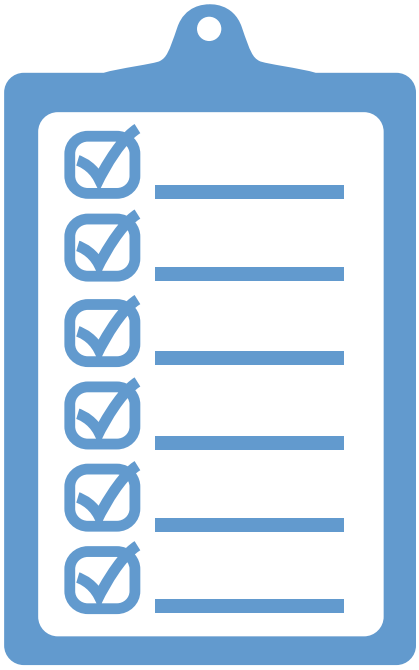
- Don't send a photo of yourself to anyone you don't know in real life.
- Abide by the "grandma" rule. If you wouldn't show the photo to Nana (or your boss — prospective employers *will* look you up online), don't send it in a text, private chat or post it to social media. Racy photos could possibly make their way around school, and you can't get them back if they accidentally go to the wrong person. In some states, if the photo is explicit enough, it could be considered illegally distributing pornography.
- Remove geotagging from pictures taken with your phone. Information automatically embedded includes latitude and longitude of where the photo was taken. Someone could figure out where you live, work, go to school, or spend time. A stalker could study the pictures and establish travel patterns.



- Crop out or blur any location-specific information in the background. You don't want your house number in any videos that might turn into a YouTube sensation.
- "Untag" photos of yourself posted by others to limit who can see photos of you, and don't tag others without permission.
- Restrict sharing to "friends only," or better yet, a small list of close friends or family — if an acquaintance in your wider friends list has a public wall instead of locked-down privacy, the photo could get wider distribution than you planned.
- Do not include location-specific information or identifying information such as full names and birthdates in captions.

SIX

Facebook Cautions



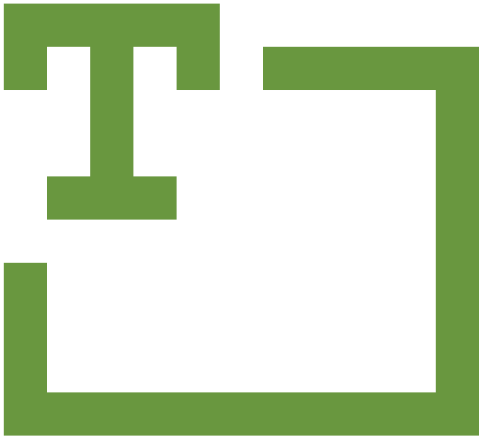
All of the above rules apply to Facebook, but here are a few guidelines and tips that you and your child should consider when logging into the social network:

- Turn on "tag review" in your child's privacy settings, and Facebook will notify him or her of any tagged photo before your child's name is displayed alongside the photo.
- Facebook exposes kids to adult content. The majority of Facebook's users are older teens and adults who may post suggestive photos or use inappropriate language. Keep this in mind before allowing your child to have a Facebook account.
- Facebook allows users to put their location on every post. Tell your children not to do this, and change their privacy settings so their friends can't check them in (and thereby give away their current location), either.
- Facebook has thousands of third-party apps and games. Before using any app on Facebook, your child has to agree to the app's privacy policy that outlines what information it will collect and how it will be used. Tell your child not to click "Allow" without actually reading and understanding the privacy policy.

- Facebook's policies and default privacy settings are always subject to change, so keep up on changes. Visit the Facebook Safety Center, continue a dialogue with your child, and responsibly monitor his or her social networking account and privacy settings.

SEVEN

Texting Considerations



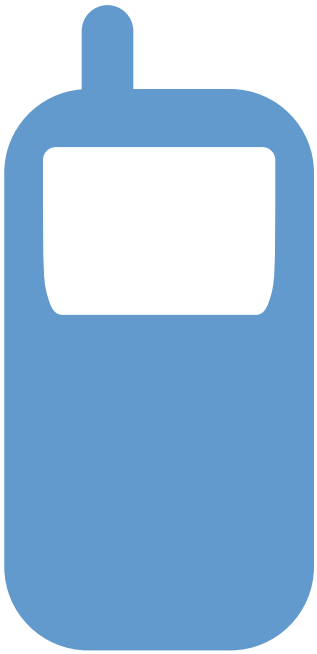
A Pew Internet & American Life Project study found in 2012 that teens send an average of 60 texts per day. Older girls send an even higher amount, 100 per day, where as boys of any age tend to send closer to 50. Frequent texting is a reality of the kind of life our kids live, but when it gets in the way of normal functioning, parents need to set limits. Texting friends when your child should be doing homework or sleeping can affect a child's ability to function in school.

Draw up a list of times when your child isn't allowed to text. Common times might be during school, dinnertime, homework time or after a certain hour in the evening. You also might need to make other rules, such as "no checking or sending texts when you're having a face-to-face conversation with me" or "no texting me when I'm within shouting distance."

If your teen is having trouble focusing, understanding concepts discussed in class, or completing homework in a reasonable amount of time, try taking his or her cell phone during school hours or for a period of time at night. You might find that they will focus better in school and be more efficient while finishing homework and tasks.

EIGHT

Cell Phone Rules for Kids



So you're ready to give your kids their own phones? The good news is that the cell phone is indeed a valuable tool in keeping kids in touch with their parents and out of trouble. The most common use of the cell phone for kids in the 6-12 age range is calling their parents, followed by calling friends, emergency purposes, text messages, and gaming.

Many phone manufacturers are now producing kid-friendly phones geared toward the 6-12 age bracket. Some allow calls only to numbers preprogrammed by mom and dad; others block texting capabilities and Internet connectivity. If it's a smartphone, it needs the same online safety rules as the computer.

Bottom Line: Don't hand it over without rules.

Parental monitoring tips for your child's cell phone:

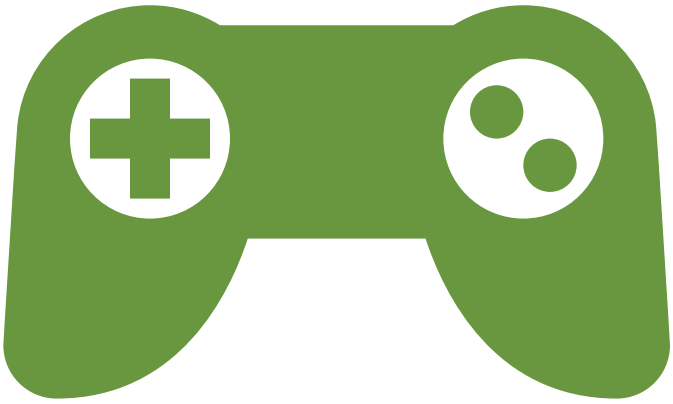
- Lay out the times and durations when phone use is acceptable and establish a monthly limit on texts.
- Specify what times are "off limits" for phone use.
- Decide on a consequence for breaking the rules.

- Familiarize yourself with the features and capabilities of the phone.
- Talk about what's acceptable to text and forward.
- Think about installing additional *parental controls* on the phone.
- Regularly check phone activity.
- Review the contacts and watch for strangers or cryptic contact names.
- Review phone history for late-night calls or calls at odd times of day.
- Teach kids not to respond to texts from people they don't know or give their number out to people they don't completely trust.

NINE

Gaming Goes Online

Online gaming isn't accessible only by computer anymore. Video game consoles hooked to your TV also connect to the Internet now, which means that safety rules that apply to your computer also come into play here.



Remember:

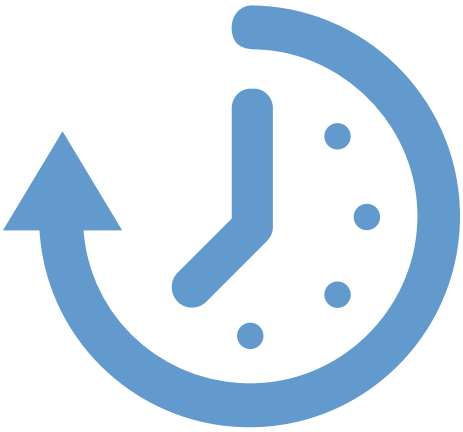
- Keep identifying info (name and city) out of your child's gamer tag ID and chats.
- Tell your child not to chat privately with people he or she doesn't know.
- Deactivating the console doesn't lock out the account. It's not console-specific.
- Gaming consoles can interact with Facebook and Twitter accounts.
- Kid-level accounts have more privacy restrictions than adult accounts, so if a parent didn't set up the account, it could be rated "adult."
- Review the ratings on the games your child plays. "M" is for "Mature" and should generally not be played by children.

- Listen when your child is gaming online; be aware of the topics discussed and language used, and be prepared to talk to your child about what would be inappropriate and why.

Most people gaming online will likely be teens and young adults, but there is always the possibility of predators or people looking for others' personal information such as names, addresses, emails, credit card numbers or bank account numbers, birthdates, logins, and passwords. Keep kids informed and safe.

TEN

Screen Time Limits



When kids have moved many of their activities — games, social lives, and homework — online, they end up spending a lot of time in front of some type of screen, and screen time needs parental monitoring.

So how much is too much? The American Academy of Pediatrics organization says that kids should have no more than two hours of screen time per day, that kids under two years old shouldn't have any screen time at all, and that there should be screen-free zones in the house, such as children's bedrooms.

Problems associated with too much screen time:

- shortened attention span
- lack of ability to concentrate
- depression

In addition to those problems, sitting in front of a screen for more than two hours a day means your kid is not playing outside and getting the exercise he or she needs.

Health issues associated with a sedentary lifestyle:

- heart disease
- stroke
- obesity
- diabetes

Making screens off-limits at certain times — at the dinner table, in church, or after 9 p.m., for example — could be even more important than setting a maximum amount of time per day. Limit screen time, and maximize your child's time with real-life friends and family members instead.

ELEVEN

Shut It Off & Get Some Sleep!

If as parents you're considering setting a screen time limit, you might also want to consider an "available hours" limit as well, as texting and gaming can affect teens' sleep patterns — and eventually their health if gone unchecked.

Teenagers actually need more sleep than elementary school children: about 9.5 hours per night. Your teen's obsession with checking texts the second they are received doesn't turn off after lights-out, and plenty of their friends are texting them after hours. Despite this obvious intrusion to their sleep schedule, most teens are reluctant to ignore a call.

Sleep-deprived kids exhibit these behaviors:

- listlessness, moodiness or irritability
- inability to stay awake all day
- inability to concentrate and focus
- dropping grades
- headaches

- physical weakness

Long-term consequences:

- migraines
- type 2 diabetes
- hypertension

What to do:

- Set acceptable hours of usage (these may vary between weekdays, weekends and summer).
- Leave any distracting technology in a family room or kitchen. Maintain the bedroom as a place of relaxation, not disruption.
- Consider having friends over for sleepovers follow the same rules.
- Follow through with punishment if your children are breaking pre-determined rules.

TWELVE

Golden Rule & Cyberbullying

Some basic rules about life also apply to social media, especially the golden rule, “treat others how you wish to be treated.” Social media is fun, but just like in real life, you want to hang out with positive people and portray a positive image.

Here are some rules for your child to follow:

- Don’t spread rumors and gossip.
- Don’t join in with taunting or teasing.
- Block senders of mean messages, and file a report with the website, cell phone service, or police if people are bullying you or making threats.
- Report bullying. If your friends are cyberbullying someone and you stay silent, you’re just as guilty as they are. Speak up and keep your friends in check.
- Don’t say things online that you wouldn’t say to someone’s face.

Consider having your children take this pledge:

I will not post anything rude, offensive or threatening, send or forward images and information that might embarrass, hurt, or harass someone, or take anyone's personal information and use it to damage his or her reputation.

THIRTEEN

Save It & Report It

The bad thing about posts and texts is that you can never really get rid of them after they have been sent. The good thing about posts and texts is that they can be easily saved and used as evidence if someone sends your child a demand or threat, bullies your child in a chat room, or sends unwanted racy pictures to them.

Consider having your children take this pledge:

If someone makes me feel uncomfortable or if someone is rude or offensive, I will:

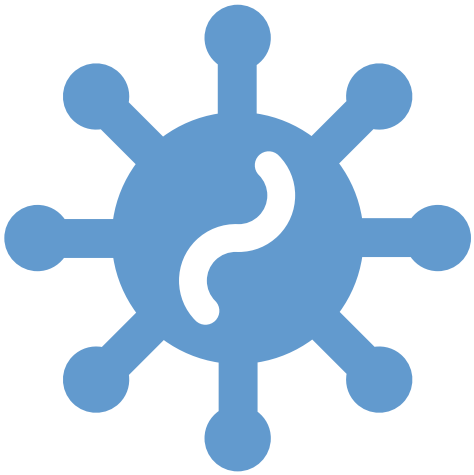
- not respond
- save the evidence
- tell my parent, guardian, or another trusted adult
- report to the website, cell phone company, cybertipline.com or the police

Make sure your child remembers:

- If you feel physically threatened at any time, do not hesitate to call the police.
- If something feels weird, stop.
- Never allow anyone into your home if your parents are not home.
- Always be honest about your activities online — even if you have done something against the rules. If you feel that you may be in danger, it is important that you are upfront about the situation.
- Never meet anyone in person that you met online without having your parents with you the entire time.

FOURTEEN

Don't Trust It, Click It, or Spread It: Identifying Phishing, Scams, & Hoaxes



In simplest terms as possible, remind your child not to believe anything that encourages you to forward to your friends and family. This includes virus warnings, privacy and copyright issues on Facebook, and maybe very believable or heart-tugging stories. Tell your child that they can check the validity on Snopes.com or Google before forwarding anything. If an email from a company your child is not aware of mentions a prize or free money, he/she should be suspicious. Remind your child that he/she can always come to you if they need clarification.

Tell your teen that:

Reputable companies will never ask you for a password. In addition, you should never give personal information to a company representative unless you are 100% sure it is legit.

Never click on a link in an email from someone you don't know or an email that looks very fishy from one of your contacts. It could be a sign that your contact's account was hacked. Watch for "https" in browser windows before typing in personal info. That means the site is secure.

You can be duped in an online action or Craigslist scam. If someone buys something from you online and sends the wrong amount, it could be a bad check scam where you're not only out the item but the sale price plus the refund. Be careful purchasing things online and come to mom and dad if you have any reservations.

FIFTEEN

Don't Text and Drive

The idea of shifting focus from the road to a screen seems so obviously dangerous, but teens need to be constantly reminded that texting and using their phone while driving is NOT ok.

Legislation banning the practice hasn't necessarily made the roads safer, either. In a 2010 study by the Highway Loss Data Institute, researchers found that there was no reduction in the amount of collision insurance claims filed after the passage of antitexting legislation in a state; in fact, the frequency increased by 7 to 9 percent in three of the four states studied.

Aside from your teen's safety and the safety of everyone else on the road, the practice has ramifications for your insurance liability and potential financial ruin. Before giving the child the keys, let him or her know that driving is a privilege that can and will be revoked for reckless behavior.

A good way to stop the texting impulse is by taking away the temptation altogether. There are several apps that have solutions for texting while driving, and should be used on your child's phone if you think they don't have the will power to refrain on their own.

Textecution for Android Phones ($29.99) cuts off all texting ability if the device is moving faster than 10 MPH.

AT&T DriveMode for Android and BlackBerry (Free) automatically sends a customized reply to incoming texts, just like an “out-of-office” autoreply. It also disables all ingoing and outgoing calls and Web browsing.

BOOK

Contributors

Tim Woda - Tim is co-founder and resident Child Safety Advocate at uKnow.com. Tim originally conceived of uKnow.com following his own child's encounter with an internet child predator. While his son was thankfully unharmed, the incident inspired him to become a passionate advocate for empowering families and helping them to protect their children from today's scariest digital dangers.

Cathy Jones - Cathy Jones is a freelance writer that has been in publishing for nearly 20 years in positions ranging from small-town newspaper reporter to editor of K-12 nonfiction for educational publisher

Edited by **Callie Harris**.

Design Layout by **Julie Csizmadia.**

BOOK

References

Weinschenk Institute: 100 Things You Should Know About People: #8 — Dopamine Makes You Addicted To Seeking Information. http://www.theteamw.com/2009/11/07/100-things-you-should-know-about-people-8-dopamine-makes-us-addicted-to-seeking-information

My Nationwide Magazine: 3 Apps to Stop Texting While Driving. http://www.mynationwidemagazine.com/3-apps-stop-texting-while-driving

Automotive Fleet Magazine: 6 Mobile Applications to Prevent Distracted Driving Accidents. http://www.automotive-fleet.com/channel/safety-accident-management/article/story/2011/08/6-mobile-applications-to-prevent-distracted-driving-accidents.aspx?prestitial=1

Highway Loss Data Institute: Texting bans don't reduce crashes; effects are slight crash increases. www.iihs.org/news/rss/pr092810.html

American Academy of Pediatrics: Media and Children, http://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Pages/Media-and-Children.aspx

ScienceDaily: Curb Kids' Screen Time to Stave Off Major Health and Developmental Problems. http://www.sciencedaily.com/releases/2012/10/121009112138.htm

Scholastic: Set Limits on Screen Time. http://www.scholastic.com/parents/resources/article/your-child-technology/set-limits-screen-time

Science Daily: Teens With More Screen Time Have Lower-Quality Relationships. http://www.sciencedaily.com/releases/2010/03/100301165614.htm

New York Times: The Web Means the End of Forgetting. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=0

Washington State Office of the Attorney General: Internet Safety for Teens. http://www.atg.wa.gov/InternetSafety/Teens.aspx#.UTOx_Rlk8Xg

Microsoft Safety and Security Center: How to recognize phishing email messages, links, or phone calls. http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

United States Computer Emergency Readiness Team (CERT): Security Tip (ST04-009): Identifying Hoaxes and Urban Legends. http://www.us-cert.gov/ncas/tips/ST04-009

CBS News: Teens are Sending 60 Texts a Day, Study Says. http://www.cbsnews.com/8301-501465_162-57400228-501465/teens-are-sending-60-texts-a-day-study-says

AT&T: Don't Text While Driving Documentary. http://www.youtube.com/watch?v=DebhWD6ljZs

BOOK

Resources

uKnowKids: Keeping Kids Safe: An Internet & Mobile Safety Workshop.
www.uknowkids.com/communityprogram

National Center for Missing and Exploited Children: Net Smartz Kids.
www.netsmartzkids.org

FBI: SOS: Safe Online Surfing.
https://sos.fbi.gov

Disney: Disney's Surf Swell Island.
http://home.disney.com.au/activities/surfswellisland

AT&T: Safety Land.
http://www.att.com/Common/images/safety/game.html

Carnegie Mellon University: Carnegie Cyber Academy.
http://www.carnegiecyberacademy.com/

IMAGE

Credits

Safety designed by Lemon Liu
No designed by Unknown Designer Collaboration by Roger Cook & Don
Arrows designed by Alex Fuller
Lock designed by Unknown Designer
Privacy designed by Lars Kloster Silkjær
Profile Information designed by Márcio Duarte
Discussion designed by factor[e] design initiative
Share designed by Giles Dickerson
Friends designed by Rob Schill
Polaroid designed by Johan H. W. Basberg
Education designed by Chris Matthews
Crop designed by Unknown Designer
Checklist designed by Michael Young
Text designed by Henrik Lund Mikkelsen
Cell Phone designed by Unknown Designer
Game designed by Unknown Designer
Time designed by Richard de Vos
Sleep designed by DonBLC 123
Social Media designed by Joris Hoogendoorn
Save File designed by iconoci
Virus designed by Márcio Duarte
Click designed by Rohan Gupta
Car designed by Unknown Designer Collaboration by Roger Cook & Don Shanosky