avast

What Grown-ups Need to Know About

Online Safety for Kids

Having “the talk” with your kids

The world is different from the one we grew up in. Children learn how to use a mouse and swipe a touchscreen before they can read or write, but just because they’re “digital natives” doesn’t mean they’re naturals at navigating the cyberworld safely. We’re parents too, and since we’re in the online security business, we’d like to help you talk to your child — whether they are 5 or 15 — about staying safe online.

Mothers and fathers, grandparents, and even older siblings are the trusted authorities in the home. You are the go-to resource to help keep the internet a safe place for your family.

To protect your children from making irreversible mistakes or trusting the wrong people online, you need to stay informed about current issues and understand the social networks and devices that your children use.

Children whose parents talk to them regularly about what they do online will likely be more responsible when alone and unsupervised.

Table of contents

Chapter 1: Stay safe online

Before anyone in your family connects for the first time, be sure that all the Wi-Fi enabled devices in your home — computers, mobile phones, tablets, and even routers — are secure. Malware on any of these devices can put your family's personal information at risk.

Viruses and malware

Keep your devices free of malware

Once malware (malicious software) is introduced to your device - be it computer, cell phone, or tablet — settings can be changed, systems can be remotely controlled, adware can trigger annoying pop-ups, browsers can be switched, websites re-directed, keystrokes logged — and that's just a few scenarios. In short, any number of terrible things can happen. Protect yourself!

Use up-to-date security software. Fortunately, a high-quality antivirus program can protect you against all these baddies easily. Avast Antivirus offers free antivirus protection as well as several levels of paid protection. Compare Avast's suite of antivirus solutions.

Keep your software, operating system, and apps updated. Vulnerabilities in software provides an open door for hackers — so why make it easy for them? You can either update your software manually, or use tools like *Avast Software Updater*, which can easily or automatically update your software and keep you safe from unwelcome visitors.

- Half of all children eight years and younger use an internet-connected device
- 88% of teens ages 13 to 17 have access to a mobile phone of some kind, and a majority of teens (73%) have smartphones

Safe surfing

The internet is great, but it has a dark side, too

Curious kids explore the internet using the same browser that you do. But they are more likely to misspell a word, make a poorly-phrased search, click on a pop-up, or follow an untrustworthy link that can result in accidentally seeing pornography or other… ‘grown-up’ stuff. And the conversations that follow those discoveries are not something we can help you with.

Keep an eye on kids when they surf the internet. The best way to do that is to place your home computer in a central location, like the kitchen or family room. Since that’s not always possible, consider installing parental controls. Your internet service provider (ISP) probably has them, and sometimes browsers have settings or extensions that can put some blocks in place. You can check your smartphone’s settings for password protection, as well. By and large, parental controls can be found on most internet-enabled devices, such as game consoles and DVD players.

- 70% of children have accidentally seen online pornography
- 44% of pre-teens watched something online that their parents wouldn’t approve of
- 32% of parents admitted that their child has accessed adult content using a mobile device

Privacy

Teach your children to share wisely

Parents teach their children to share with others, but in some circumstances, sharing is not necessarily a good thing. Anything that is shared online — messages, photos, social updates, check-ins, and of course, home addresses, phone numbers, and financial information — can fall into the wrong hands. At best, you have a damaged reputation to deal with, and at worst, full blown identity theft.

Talk to your kids about what's okay to share and what should be kept in the family. In some cases, extra steps may be required. You can increase the strictness of parental controls, or get third-party monitoring software like Net Nanny to keep a closer eye on what your child might attempt to give away.

Receiving credit cards, checks, pre-approved credit card offers, bills or bank statements in the name of your child is an indication that someone has used your child's social security number. Investigate immediately.

Phishing

Don’t fall for the clever disguises of online criminals

Clever cybercrooks go “phishing” for victims by using what looks like authentic emails, texts, and pop-up messages to trick people into sharing their personal information. These fool more than just children: even adults can get hooked!

Teach your kids not to reply to unknown texts, open attachments in emails, or click on pop-ups. Eavesdropping malware might get installed, or they can be tricked into revealing personal info in a fun “survey” that gets them more than they bargained for.
If you or your kids were tricked by a phishing scam, file a complaint at ftc.gov/complaint.

- There were more phishing attacks in the first quarter of 2016 than in any other three-month span since tracking began in 2004.

Passwords

Speaking of things we shouldn't share...

These twins have the same face, clothes, and maybe even a few mannerisms, but they shouldn't have the same passwords. Encourage your kids to use unique, strong, long passwords for every site and network they log onto — a lesson most adults could stand to learn too! It's never a good idea to re-use passwords on multiple sites or create passwords from familiar terms, like names or birthdays. They're far too easy for hackers to crack.

We know it's not easy to remember all those long passwords, but it's equally important you don't store your passwords in your browsers: they're unencrypted, so if someone hacks your computer, they can easily steal them. If you want the convenience of auto-filled logins with none of the risk however, then it's a good idea to invest in a password manager. As it so happens, we have one: *Avast Passwords*, a tool available in Avast Free Antivirus, Avast Pro Antivirus, Avast Internet Security, and Avast Premier.

- Nearly 50% of parents know the password to their teen's email account
- One-in-three parents are privy to their teen's social media passwords

Most used passwords

- 123456
- password
- 12345678
- qwerty
- 12345

- Downloading illegal music robs $12.5 billion from artists and industry workers every year.

Downloading and file-sharing

Is it okay to download the latest hit song for free?

Nope, but it sure is tempting. Many illegally downloaded songs and movies come through a peer-to-peer (P2P) file-sharing network, which is riskier than a trustworthy, legal website. Files from a stranger can hide malware, spyware, or pornography. Since file-sharing gives other users access to the files on your computer, your family's sensitive information could be stolen in the process, as well.

Streaming sites are popular because you can view content at your convenience with no need to download or store an illegal file. Either way, when you get content from a pirate site you are breaking the law, and lining the bank account of a cybercrook.

Use common sense. If you're downloading or streaming the latest blockbuster, for example, you are stealing content from the creators, and that's wrong (not to mention against the law). Parents can be held liable if their kids download copyrighted material.

Avoid risky download sites. You are safer when you use official download sites and steer clear of P2P sites, social networks, and untrustworthy blogs or forums.

Scan downloaded files with antivirus software. Use *Avast Antivirus* to check downloaded files to ensure they're safe before you hit "play".

Chapter 2: Social media

Your kids are part of the social generation; where tweeting, posting on Facebook, sharing over Snapchat, and using Google or Wikipedia for research is a natural part of everyday life.

Since social media plays such an important role in the modern world, especially for our children, it's crucial to make sure that they stay safe while they make the daily rounds on social media platforms.

Social networks and instant messaging

Eavesdropping on your online conversations

While social networking can be a powerful tool for meeting like-minded people and making new friends, it's also a convenient way for less-than-friendly people to steal your personal conversations and info.

Although we love the convenience that instant messengers provide, not all instant messaging tools are created equal. It's important to take a look at a service's security and privacy measures, as only around half of today's most popular instant messengers provide users with complete encryption.

To avoid being spied on, especially while using free Wi-Fi, you can connect using a VPN service. And yes, we have one of those as well: *Avast SecureLine*, which is an easy-as-pie way to make sure that hackers or nosey eavesdroppers can't listen in.

- Ease younger kids into messaging apps with safe, kid-friendly Kuddle or Marimba Chat

Oversharing

TMI: No delete button on the Internet

They aren't called the "Selfie Generation" for nothing. Sharing compromising photos or posting questionable status updates can hurt your child's reputation now, put them in danger, and even cause problems in the future when applying for jobs or schools.

Talk to your kids about what they post online, and make sure they realize that sharing personal information like their full name, Social Security number, address, birthdate, phone number, or place of birth, can not only harm them, but the whole family. In the wrong hands, that info can give someone the chance to steal your child's identity or stalk them in the real world.

Set privacy controls on social networks. Many platforms have privacy policies that allow you to limit who sees your child's content.

- 71% of teen girls and 67% of boys have shared sexually suggestive content with a boyfriend or girlfriend
- Experts speculate that Kim Kardashian shared too much information on social media which may have lead to a robbery of $10M worth of jewelry

- Nearly 43% of kids have been bullied online. 1 in 4 has had it happen more than once.
- Girls are about twice as likely as boys to be victims and perpetrators of cyberbullying

Cyberbullying

Cyberbullying hurts

Cyberbullying is exactly like normal bullying, except the bullies hide behind email accounts, social network profiles, and anonymous text messages. It can consist of threatening messages, shaming, or sharing content designed to humiliate your child with other people, and as you can imagine, it can be extremely hurtful. You may have heard some horror stories about cyberbullying, but don't panic: with a calm and level head, talk to your child if it's happening to them, or if you suspect they might be doing it to others. Here's how you can help manage this difficult conversation:

- **Listen and treat your child seriously.** This is not about you; it's about your child, so give them the time and space to talk.
- **Give them your unconditional support.** Your child is strong enough to survive cyberbullying, even if they don't think they are. Offer them whatever help they need, and help them realize they're more than capable of enduring their troubles... but that doesn't mean they have to do it alone.
- **Start working together on a solution.** Think of the plan together. Listen to what they've tried in the past, and work from there. Sometimes, bullies don't realize they're being hurtful, and asking them to stop is enough. Other times, ignoring them completely will make the bullies grow bored. But if the bullying continues, you can block the person or report it to the site or network where it is occurring.

Cyberstalking

Watch out for the creeps

It’s great when we can meet new friends on social sites, but sometimes discerning a real friend from an imposter with bad intentions is difficult. Sexual predators lure their victims in uniquely devious ways, often using flattery, sympathy, gifts, money or the promise of a job, to gain their trust. At some point, the predator may suggest a private chat, or to meet in person.

One of the creepiest forms of cyberstalking is called “digital kidnapping”, and it’s only possible due to the ubiquity of social media. In this unsettling scenario, predators steal pictures of children from the profiles of their family members and use them on their own profile, pretending that the child is their own. This twisted form of privacy abuse is especially frightening due to the fact that in most cases, cyberstalkers face few to no repercussions. Digital kidnapping remains a legal gray area, so it’s especially important to think carefully about the content you post online and to whom you share it with.

- 57% of teens have met a new friend online
- 20% of all teens have met an online friend in person

Chapter 3: Mobile security

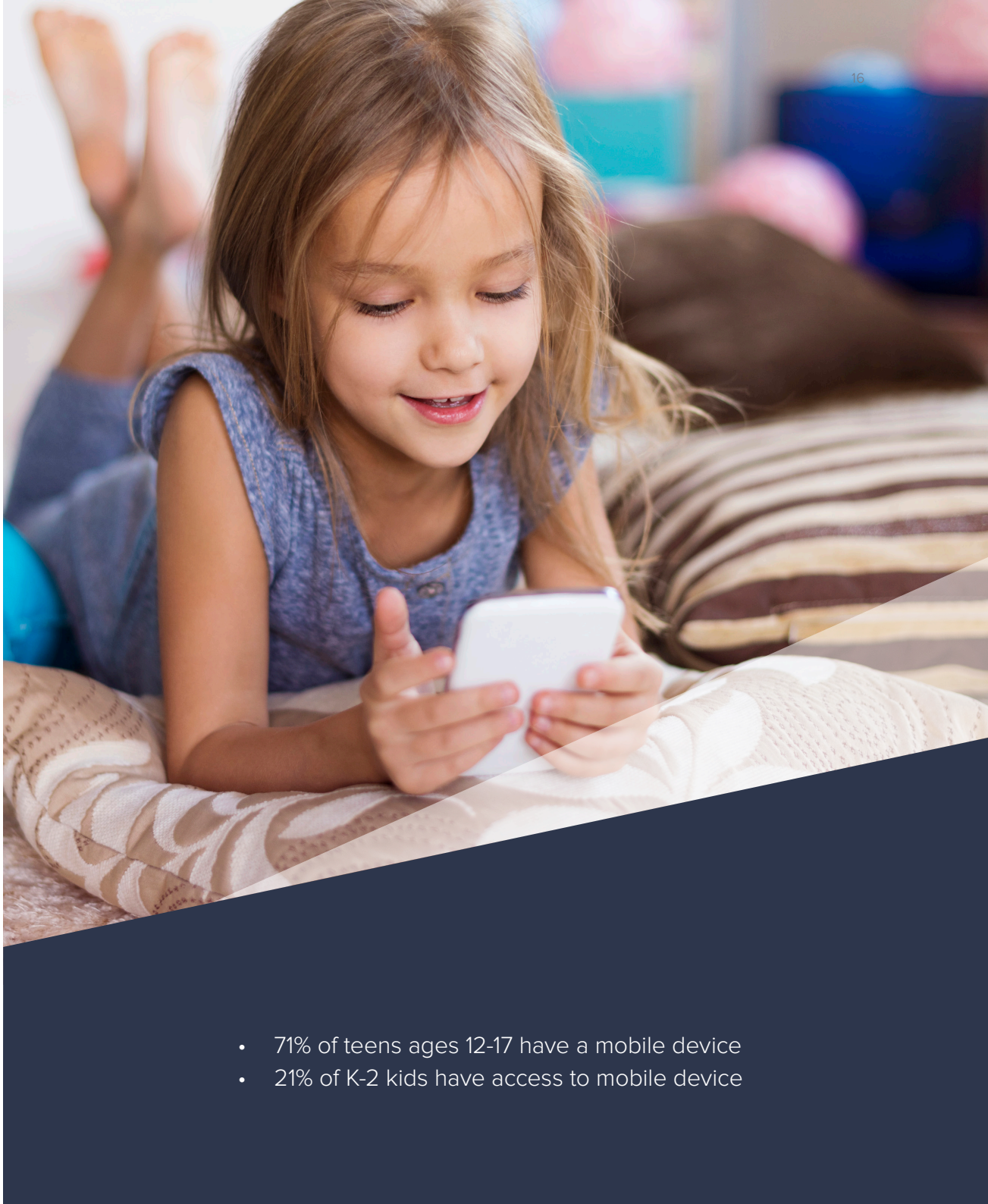
These days, many young people seem to be attached at the hip to their smartphone. With the ever-increasing functionality of mobile devices, it's incredibly important to keep malware off of your kids' smartphones and for them to stay educated about the best mobile security practices.

MALWARE and SPYWARE

Protection against online threats

You've always protected your children, whether it meant checking for monsters under their bed or bundling them up before they left the house. Now, it's our turn to protect them against a different kind of monster. Threats to mobile devices aren't quite the same as the threats PCs face, but problems such as ransomware, annoying adware, and phishing continues to increase as devices become more prolific.

Avast Mobile Security runs a thorough scan of your apps, files, and text messages to stop nasty malware and spyware and protect children and grown-ups alike from every threat.



- 71% of teens ages 12-17 have a mobile device
- 21% of K-2 kids have access to mobile device

Mobile apps

Know which apps your kids use

Young kids use their parents' smartphones and tablets to go online, making it a simple task to monitor what kinds of apps they use. Always make sure that your child downloads apps from trustworthy app stores like Google Play or iTunes, since third-party stores have less security checkpoints in place. Even reputable app stores can harbor fake apps, so double check before anything is downloaded.

Also be aware that apps can cost upwards of $10 per installation, so unless you want a surprise on your credit card bill, instruct your child to ask permission beforehand. Any apps that have banking or credit card information saved in them should be password protected.

- 80% of parents share their mobile devices with their kids
- Kids download 30% of the apps on their parent's phones

Sexting

A “sexy” joke can ruin lives

Sexting, is using a mobile device or computer to send or receive a sexually explicit image, video, or text message, typically starring the sender. Most teenagers say they do it as a joke, but some girls admit that they feel pressured by their boyfriends to participate.

The ramifications can be serious, ranging from ruined reputations, legal trouble, or even your child unwittingly finding their picture or video on adult websites. To curtail this problematic trend, more and more states are making sexting a misdemeanor, with punishments growing more severe with each offense.

Keep your kids from doing something they’ll regret by talking to them about the dangers and consequences of sending nude or suggestive images. Set rules and follow through with punishment, like taking away their mobile devices, blocking features, or limiting minutes or data, to keep them on the straight and narrow.

- Girls send more sexually explicit messages than boys
- Almost 20% of high school students between 14 and 18-years old admit to sexting
- 15% of teens sent a sexually explicit picture to someone they don’t know

Driving and texting

Take a break from the phone while you drive

Texting is the leading cause of teen driving deaths. AAA says that young, inexperienced drivers are distracted from the road nearly a quarter of the time they're behind the wheel, because their attention is split with their phone.

Talk to your teen driver about assigning a designated texter, so the driver stays focused on not crashing. If that's not working, then find an app that can stop texting while driving. You can also make your teen turn their phone off, or silent it, while they drive, so the beeping doesn't tempt them while their eyes should be on the road.

- More than 3,000 teens die each year in crashes caused by texting while driving
- More than 50% of teens admit to texting while driving

Public Wi-Fi

Use a VPN when on public Wi-FI to keep out prying eyes

We get it: it can be a lot of fun using Skype to keep in touch with friends and family, especially when we're out and about. Kids might be tempted to use the public wi-fi at their favorite hangouts to connect with their long-distance pals, but if they do, it's crucial that they make use of a Virtual Private Network (VPN) to keep unwanted eavesdroppers from listening in.

Fortunately, we've got just the ticket: *Avast SecureLine VPN* makes everything you do online safe and secure by encrypting the data as it travels across the net. This allows your kids to chat with people without fear of being eavesdropped on by cybercrooks and prying eyes. Download SecureLine VPN for Android and iOS devices.

- Nine out of ten people use unsecured Wi-Fi every month.
- Only 6% of Americans protect their data by using a virtual private network (VPN) when using public Wi-Fi.

- 49% of smartphone users don't backup their data, yet 80% are concerned about losing it.

Backup mobile data

Keep your most valuable data within arm's reach

Murphy's Law states: "If anything can go wrong, it will." Since a wild, unpredictable universe presents endless opportunities to test that theory, it's good practice to keep backups of your PC and mobile device's data fairly regularly.

What data should my family back up? Ideally, all of it. But if you have to choose, then simply pick the data that's most important. It could be documents on your computer, photos and music on your daughter's smartphone, or even web browser bookmarks saved on your son's laptop.

How do I backup my data? Typically you backup files using an external drive, or with a third-party internet service such as Dropbox, Google Drive, or iCloud.

How frequently should I backup my data? You should back your data up whenever you create new files or make changes to existing files that would be difficult to recreate. So, in an ideal world, every day. But for most of us, at least every few days or once a week should be adequate.

Mobile loss or theft

Keep control even if you lose your phone

Losing a phone or having it stolen is never fun to think about. However, as more and more kids own a smartphone, it's imperative to have a plan in place if it gets lost or stolen.

And there's no better plan than Avast Anti-Theft, an app that locates missing Android phones and tablets. The app's remote recovery options help you keep control of your device, recover data, or even wipe the machine even if it's lost or stolen.

- In 2015, 2.1 million Americans had phones stolen and another 3.1 million smartphones were lost.

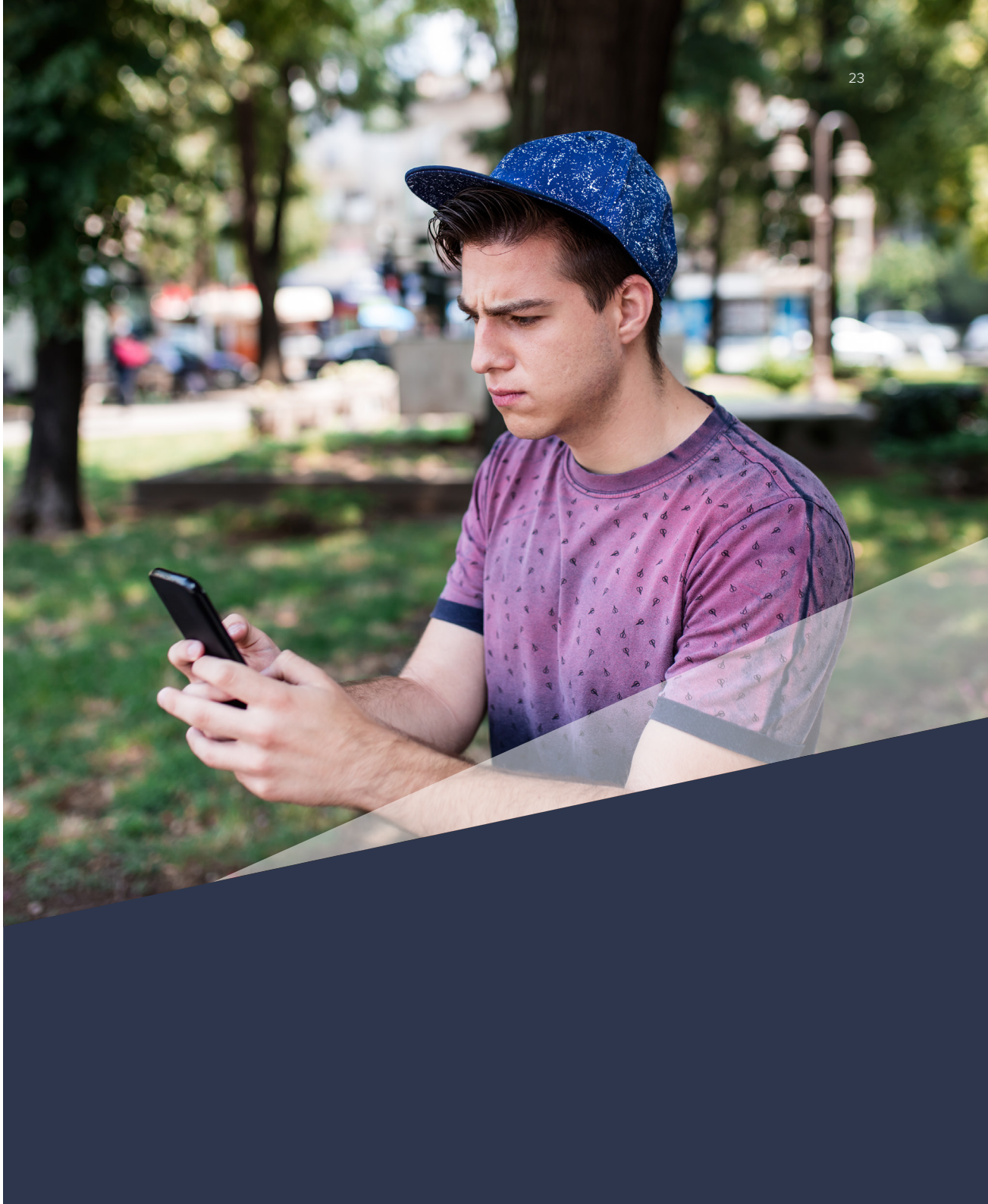
Saving battery power

You can’t catch Pokemon if your battery’s dead

The more kids play games on their phones, the less battery power they’ll have to do something important if the need should arise. Fortunately, you don’t have to outlaw fun to make sure your kids phones stay charged through the day.

With apps like Avast Battery Saver you can squeeze up to 20% more power out of a fully-charged battery. This useful app automatically adjusts settings to save energy without affecting how you or your loved ones use their mobile devices. A simple dashboard shows how much juice your battery has left, so you always know if there’s enough power for important calls, sending messages or using apps.

On top of that, Avast Battery Saver can even detect and permanently stop power-draining apps. Your phone will last longer — we guarantee it!



- Many retailers have a buy-back program or you can use a service like Gazelle to get cash for your old devices.

Phone disposal

Safely dispose of old devices

Your kids have just upgraded to the latest and greatest device on the market — what should you do with the old smartphones you no longer need or use?

Worry not, as there are multiple ways to responsibly and safely dispose of unneeded smartphones. Let's walk through the options:

- **Resell them online.** Even if a phone is no longer useful to you, there are plenty of people out there who are searching for cheap, second-hand devices. Just be sure to properly erase all data from your phone before selling it to someone else, lest they find private photos — or worse — saved on its memory.
- **Don't throw them in the trash!** Throwing away old electronics is more than just wasteful, it can be downright damaging for the environment. Recycle your devices at your local electronics retailer instead.
- **Give your devices to a good cause.** Donate your smartphones to a non-profit organization. Many charities offer free mobile phone recycling and sell all donated devices to either electronic restorers or a recycler. The proceeds from the donated phones are often used to supply calling cards to soldiers, veterans or people in need.

Avast is here to help

We're ready and willing to provide you and your kids a safe, secure way to explore the internet without any fear. Make sure to protect your family's devices with the lightweight, powerful protection of Avast Antivirus.

To keep up with Avast on a daily basis, follow us on Facebook, Twitter, YouTube, and Google+ where we keep you updated on cybersecurity news every day.

Protect your PC with
Avast Free Antivirus Nitro Update

Protect your Android phone and tablet with
Avast Mobile Security

Protect your Mac with
Free Mac Security Nitro Update

Keep track of your Android smartphone with
Avast Anti-Theft

Sources

http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/

http://www.pewinternet.org/2009/08/19/teens-and-mobile-phones-over-the-past-five-years-pew-internet-looks-back/

http://www.pewinternet.org/2015/04/09/a-majority-of-american-teens-report-access-to-a-computer-game-console-smartphone-and-a-tablet/

http://www.guardchild.com/statistics/

http://www.scmagazine.com/apwg-report-phishing-surges-by-250-percent-in-q1-2016/article/498867/

http://www.optimist.org/internetsafety/ikeepsafe-statistics.pdf

http://www.parenting.com/article/keeping-your-child-safe-on-the-internet

https://www.dosomething.org/us/facts/11-facts-about-cyber-bullying

https://blog.avast.com/2014/06/01/kids-use-their-parents-smartphones-not-to-call-grandma-but-to-visit-sites-with-adult-content/

http://nobullying.com/is-sexting-illegal-maybe-in-your-state/

http://safety.trw.com/global-texting-while-driving-statistics-fuel-driver-distraction-debate/0418/

https://www.aaafoundation.org/distracted-driving?gclid=CNPx1OnXp8wCFVAvgQodtWYOwA

http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm

http://www.komando.com/happening-now/375362/did-oversharing-on-social-media-cause-kim-kardashians-robbery

avast