One parent to another

Managing technology and your teen

By Tony Anscombe

Copyright

Acknowledgements

Without my family, friends, and many countless other fellow parents, this book would never have been written. Over many years, parents have asked me for advice on laptops, phones, tablets, antivirus software and general concerns they have about their family computer or what to get their kids as a first device. I dedicate this book to them all as, without their continual requests, I would not have been driven to write something for all parents who may have an interest in this topic.

The most important people that I need to thank are, of course, my wife Caron and son who have both proofread and given feedback throughout the process and even allowed me to take time out of a family vacation to write. I would also like to thank Pete Gade who helped me get my words into a readable and logical state. Thanks, Pete, for all the assistance!

Author profile

Tony Anscombe is a father and Ambassador of Free Products for AVG Technologies. Tony's role at AVG is to bring to our growing population of free users the products and solutions that allow them to enjoy their online experiences while trusting AVG to help provide them protection from malware and data loss. Tony is also instrumental in relationships with third-party testers of antivirus products which help AVG to continue with its focus on delivering product quality and excellent security.

Tony joined AVG in August 2009, bringing over 20 years of IT experience in total with the last 12 years being focused in security. Before joining AVG Tony worked for German-based antivirus company Avira and was responsible for the consumer product division that included both paid and free antivirus products.

Prior to moving into the consumer antivirus market, Tony worked with a number of companies that provide authentication, data leakage prevention, and the more complex environment of government certified encryption technology. The experience of multiple technologies all in the security sector and a technical background make Tony well placed to understand the requirements of this very fast-moving sector of the industry.

tony@tonyanscombe.com

Tony

One parent to another

Managing technology and your teen

By Tony Anscombe

Contents

7 Chapter 1 Who should read this book?

12 Chapter 2 What are connected devices?

18 Chapter 3 Connectivity and communications

32 Chapter 4 The smartphone chapter

38 Chapter 5 Everyone on their best behavior

49 Chapter 6 Parental controls

58 Chapter 7 Cyberbullying

64 Conclusion The big things to keep in mind

Chapter 1

Who should read this book?

When you're in middle school, the school dance is a pretty big deal. For most kids that date on the calendar conjures up an absolute mish-mash of feelings. Sometimes they wonder whether or not they should go, so they consult a good friend on the matter . . .

"You gonna go to the dance?"

"I dunno. Maybe. Are you gonna go?"

"Yeah, uh, maybe. I guess."

Most kids end up going, if only to hang out with their friends and take part in what really can be a fun event. They're trying hard just to be cool and have a good time, but all that can go right out the window when they're faced with a gymnasium full of tweens. Stirring up any fun memories yet? I hope so! I bring this up because two years ago my son's middle school held a dance for all the students. You can probably picture it in your mind, very much the typical soirée for kids aged roughly 11 to 13. But something happened at that dance that was entirely different from any dance I ever went to. You see, back in my day, there was a sort of unwritten rule about dances. No matter how awkward things got, or how many times the girls laughed at the boys, or how goofy someone looked when they got on the dance floor, no one ever talked about it afterwards. When I look back at that now as an adult, it strikes me as kind of strange. We had our own Vegas rules - whatever happens at the dance, stays at the dance. But that's not exactly how it went for my son.

When he came home from the dance I asked him how it went. He gave the usual answer to my questions, the stock "OK." As any parent knows, that's often all the feedback and storytelling you'll get at that age, but this was a big day, so I pushed my luck and asked a few more questions. "Who did you hang out with? Dance with any girls?" and so on - all the questions a dad can't help but ask. Meanwhile, my wife was sitting there smiling and saying, "Leave the poor boy alone." I'm glad I kept at it. Turns out that one of the kids he hung around with spent the entire dance on his mobile phone taking pictures and videos of the kids talking and dancing. "He did what? Really!?"

Now this was uncharted territory. It's kind of expected that if you give kids a phone in an awkward situation, they'll typically duck behind it for a little escape. But there they were in full color - pictures and videos of a school dance, all captured on a phone. Whoah! My mind immediately ran through all kinds of scenarios. What will he do with them? Where will they end up? Will they go on some social media site and stir up all kinds of grief and embarrassment? Meanwhile, it was clear that it had made my son and his friends feel very uncomfortable.

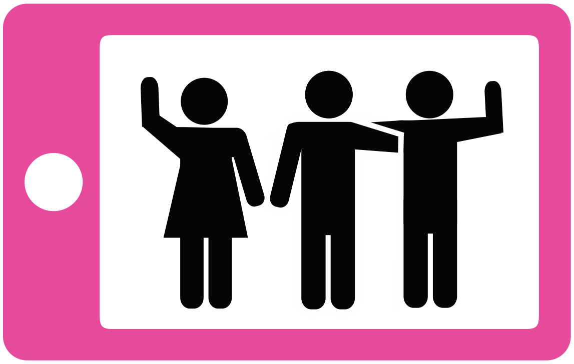
Did seeing a camera change the way they behaved?

Fortunately, those photos and videos never got posted. Either the boy thought better of it, or they were simply lost in the ether somewhere on this kid's phone. As you can guess, my concerns lingered. Did the boys talk about this when it was happening? Did they ask him to stop? Did seeing a camera change the way they behaved? My thinking is that it probably did change the way they behaved, and not in a way that was good for their development. Awkward as those dances can be, they're held for a reason - they're a tween's rite of passage, another step toward adulthood, all in a safe and controlled environment. Yes, there are stumbles, goofs, and gaffes, but that's something they can learn from. In many ways, that's the point!

Bottom line: there is a time and place for technology and this was not one of them. Regardless of school protocol, strict Vegas rules should have been in effect. What happens at the dance stays at the dance - and most certainly shouldn't end up on Facebook!

Did this get resolved? Yes. It was a really simple thing. A quick email to the school principal about our kids needing to be kids, including a sentence or two about the Vegas analogy, and he quickly agreed that technology should be banned from school dances. The next dance was different. A clear message was sent that no phones were allowed. This time, there were no photos or videos, no capturing of the minute and personal details of what happened at the dance. I felt good for the kids that they had their space and that they were free from the fear of any record that could cause future embarrassment.

Ahh, it was almost like the old days again. Almost. Of course, the Internet has really left the old days in the dust. And, boy, does that feel like an understatement if ever there was one! That's why I've put together this book.



The Internet is shaping the way our kids grow up, and accordingly it has to shape the way we parent our kids. There's no avoiding it, and there's no looking back, even if we want to. The Internet is nothing short of an awesome, multi-faceted world. Through all the different devices in our homes, purses, and hip pockets, we can tap into a dizzying amount of content that's growing by the second. Now we can communicate with nearly anyone at any time, giving us a way to share our knowledge and feelings with people all over the world. Instantly.

Unsurprisingly, more and more of our day is spent online, thanks in large part to smartphones and tablets. It's so easy to get drawn into this digital world without even thinking twice. So, now is the perfect time to step back for a moment and think about that. With all this awesome ability comes the need to act responsibly. This includes instilling that same awareness in our children, so they can enjoy the Internet just as responsibly and just as safely for years to come.

We need to make a real and conscientious stand here because the Internet is ultimately a great place with a tremendous amount to offer. It's up to us to keep it that way through the decisions we make and the lessons we offer up as situations arise, just like the one at that school dance. As with all aspects of parenting, bringing up a child in a digital world is a series of learning moments. Some are big, some are small, but over time they all add up to a healthy, well-adjusted child - provided we keep engaged and are always ready to set a good example. That's the challenge, though, isn't it? The Internet is entirely new, and the rules can seem like they're being written as we go along. To some extent, they are. Keeping on top of what's right, what's wrong, what's safe, and what's sketchy, demands some real active parenting. The good news is that while the advent of the Internet is entirely new, good parenting has been around for ages. By looking back we can learn a few things, and maybe take a little comfort too.

For example, imagine being a parent after the turn of the 20th century. Up to this point, communication had primarily relied on the written form. Outside of telegraphs and telegrams, it took days or weeks to deliver a message to someone beyond your immediate vicinity. News came to you through the papers or a weekly magazine, and sometimes just through plain old word of mouth. Things moved at a certain pace. Slowly. Then along came radio, this magical and mystical means of listening to someone far away, and in real-time no less! News, sports, music, speeches - endlessly flowing from the radio. This would have probably seemed exciting and scary all at the same time. As a parent you'd see the way your kids loved to sit down and be entertained by this magic box, which was all fine and good, except for the times where you'd rather see them reading or playing outside. The radio was simultaneously both a welcome addition to the household and a disruption. Sound familiar?

The radio was simultaneously both a welcome addition to the household and a disruption. Sound familiar?

This radio example is just one of many we could use. We could also look at the invention of the automobile. Critics at the time said that it would never be safe to drive faster than just a few miles per hour and that it would never be reliable over long distances. Some newspaper pundits of the day even declared drivers to be crazed, public menaces. Just decades later, the arrival of rock and roll music was declared by some as a lawless and immoral influence on anyone who listened to it. Then there's television . . . the list could go on. My point is that, while it may feel like we're the first generation to feel like things are changing too quickly, we aren't. Media, technology, and culture have been evolving rapidly for generations. Anyone who has raised or cared for a child in times of change has had to face unique challenges - and find unique solutions. The Internet is our challenge, and likewise we've come up with a few solutions of our own. In other words, you're not alone.

In a nutshell

This book is designed for, and inspired by, parents, aunts, uncles, grandparents, teachers, caregivers, and anyone who helps raise children.

With this in mind, I have created this guide that uses real-world examples drawn from my family, my friends, and people just like you. Together, we all share responsibility for their well-being. We're the role models. We're the ones who give them the tools, knowledge, and wisdom that will set them on the right path of life. Through us, they learn to cross the road safely, how to deal with strangers, and simply how to enjoy a happy, healthy life. Today, we live in an online world. My hope is that you'll find some of the solutions in this book inspiring, put them to use, and then pass them along.

Even if you take only one piece of advice you'll still be one more family who's safer than they were before - and you'll be one more family who can be an example for others. The approach is time-tested and direct: advocate good morals, and practice what you preach.

That's the way we'll all stay safer online.

Chapter 2

What are connected devices ?

It seems like just about everything connects to something else these days. It's been that way for some time actually and, increasingly, these connections are made wirelessly. The days of pesky wires and cables are passing us by and entering the age of wireless. Look around. Our computer connects to the printer. Our TV connects to the Internet. And our phone connects to the toilet.

Yes, I did say the toilet.

Trust me, I wish I was kidding, but I'm not. In fact, the BBC News posted an article on a luxury toilet designed to play music, dispense fragrance, and flush - all by remote control using a smartphone app. While you might think they wanted to run that article for laughs, there was actually a serious issue with the luxury toilet in question. The thing is, this "connected toilet" could get hacked.

Here's what went wrong: every toilet used the same wireless access code of 0000, which couldn't be changed, so that anyone in range of the toilet could take control of it with their own copy of the smartphone app. Now, imagine your surprise when, in your most private moment, your toilet starts blasting Beyoncé while dousing the room with a lemony fresh scent - all because of a hacker.

It's all terrifically funny until we start thinking about what this really means. Like it or not, this is the beginning of a trend. More and more devices, even appliances, are connecting to the Internet and other devices. For example, it's become increasingly common to see people controlling their lights, their heating systems, and even their home alarms with smartphones, tablets, and computers. The implication is that we need to understand how our connected devices work so that we can protect ourselves from any nasty surprises.

With all this in mind, let's start with the basics. Let's get a really clear sense of how all these connections are transforming our homes, particularly the wireless connections. So, what is a "connected device"? That's not too hard. Two of the most common ones that readily come to mind are smartphones and computers. Now think about all the different ways you can connect them to the Internet, whether at home, at work, in a hotel, or with your cellular phone signal. Then think about all the different things you can do once you make that connection. You can browse websites, chat with relatives on Skype, send email, shop for clothes, stream videos, post a snapshot of your burger, or even play a game while you're in line at the store. The list of what we use the Internet for is endless, and in an ever-connected world, there are more and more ways to access it.

It's changing the way we get through daily life, where we find ourselves constantly drifting in and out of the Internet dozens and dozens of times a day. For example, when's the last time you actually used a paper roadmap in your car?

If you're like most, you fire up your smartphone or consult the built-in navigation on your dashboard and off you go. It's that easy, and we often do it without giving it a second thought.

So, those are two examples of connected devices and what we can do with them. Now let's build on that by playing a quick game. Try listing all the devices in your household that have an Internet connection:

- **The family computer**
- **The family tablet**
- **Your laptop**
- **Your spouse's laptop**
- **The laptop(s) your children use**
- **The smartphones**
  Whether for you, work, or the kids.

If that looks like your household, you're not alone. In 2013, the average household in the United States had 5.7 connected devices — more than twice the number of people per household (NPD Group, March 2013). That's a pretty sizable figure, but we're not done yet. Have you thought about these devices too:

- **Your television**
  Many connect to the Internet and even let you download apps.
- **Game consoles**
  They connect to the Internet too, with full browsing capabilities and ways of streaming content like movies and shows.
- **Handheld game consoles**
  Just like their bigger siblings, they're powerful computers too.
- **Printers**
  The newer ones can let you scan documents and photos directly onto the Internet for storage (popularly known as "storing your photos in the cloud").

That list just got a bit longer, didn't it? Guess what, there's more . . .

- **Wi-Fi connected cameras**
  Many new cameras now have Wi-Fi so you can share the picture on social media sites like Facebook.
- **Home phones**
  Many phone services now use data lines for voice connections (known as VoIP phones).
- **DVD players**
  Many of them stream Netflix or have content services.
- **The refrigerator**
  You may be laughing but the new ones are connected.

- **The car**
  They're connected too, where many of the new ones have built-in systems that access the Internet.
- **Burglar alarm or camera systems**
  Many of these can be remotely controlled by PCs and smartphones.
- **Heating and cooling systems**
  Same as the above.
- **Internet radio devices**
  As the name indicates, these are standalone speaker systems that pipe Internet radio into your home.
- **The trash can**
  Only joking! But that's what I used to think about toilets too...

By now it's all pretty clear. It's hard to imagine a moment, let alone a day, without a connection to the Internet being more than just an arm's reach away. Now we're getting a sense of all the connected devices in our lives and you probably have a feeling in your gut about the potential risks involved, not just the privacy and protection issues they conjure up, but also just the risk of simply getting addicted to being connected.

So what are the risks? Are they truly real, and if so what do they look like?

The most straightforward answer we can give is that any time content or information is being passed between your household and the Internet, you need to be aware and exercise caution. It's up to you to crack open that user manual or the application settings to decide which features are right for you and your family. Put in the simplest terms, you need to know what those cool feature-rich devices are really capable of doing and what kind of information they're passing around. Sometimes you have to dig a bit to find out.

Let's take a look at a really practical example. Taylor is a young teen who is just starting to use social networks. She has a smartphone and is wandering around the house taking pictures and posting them. Beyond any concerns about inappropriate pictures, what's the risk? This is where we have to understand what's going on behind the scenes in that smartphone. With every picture taken, smartphones have the ability to store location information along with the picture (known as "geotagging"), and with little effort it's easy to determine where that picture was taken. This is great if you can't remember where a snapshot was taken, but not so good if your kids are posting pictures of the family bunny rabbit and anyone with a little gumption can look at that information and figure out where you live. That might not be something you want to put out there. The good news is that smartphones allow you to turn off such geotagging features, which keeps your photos free of location information in the first place. In the case of the bunny photos, that may be something you want to do before those photos find their way to the Internet.

Here's another great story I came across not long ago, something from Wired magazine. It's really interesting, but the implications are a little creepy. The journalist who wrote the piece went to Golden Gate Park in San Francisco and spotted a mother taking pictures of her kids. Later in the day, he searched for pictures taken in the park that same day. Guess what? He got a hit. He found the pictures that mother took posted on a photo-sharing site. Next, he looked for other pictures taken by the same person. It wasn't long before the journalist worked out where she lived and who lived there with her, just by looking at what she'd posted. That's geotagging at work on your smartphone. A little effort and a little searching can lead to a lot of information in the hands of a determined individual. It's a bit chilling if you'd rather the world didn't know that your house in Anytown, U.S.A. is probably empty while your family is travelling thousands of miles away.

Alright, so let's imagine that you already know about geotagging and that you've already made sure that your smartphone isn't tagging each photo with location information. You've told the kids, too. You've gone through the smartphone's settings together and made sure they know how to check that the location information is switched off for the smartphone's camera. Great. Everyone is up to speed. Then one day your kid asks, "Hey, can I use the "normal camera" to take a few pictures?" Well, it's not the smartphone. Of course, you think it's safer and say, "Sure." But oh dear . . . that new "normal" camera you bought has some pretty awesome features. It has Wi-Fi and stores the location information for your pictures too - just like your smartphone. If you use that Wi-Fi feature to store those pictures online (in the cloud) or post them directly to the Internet via Facebook or Instagram, guess what . . . that location data goes along with those photos by default.

This is another case where you have to get to know your device and what it's connecting to. Any time you acquire a connected device it's a good idea to go into your device settings, learn what's there and make a few adjustments to suit your idea of privacy.

Any time you acquire a connected device it's a good idea to go into your device settings.

You need to take a look in the preferences and settings of the services that your device will connect to (again, like Facebook or Instagram), and then make adjustments in those services too. Yes, it's extra work. Yes, it takes time. But it's a good idea to do this for each of your devices when they enter your home, making it part of your new purchase routine - just like turning it on for the first time.

In a nutshell

Bottom line: get to know the "ins and outs" of all your devices.

With every connected device, there are risks to some degree or another. Some are major, some are minor, and some really depend on what you believe is right for you and your family.

This is going to vary greatly from device to device. Obviously some devices are more feature-rich than others, and clearly a new PC is going to access much more of the Internet than your Wi-Fi enabled camera. In any event, you'll want to get to know those features.

Here's the good news, though: regardless of the device, there's a general rule of thumb that can help you determine and reduce your risk. Ask yourself three simple questions:

Where is the content stored?

Who can see it?

What data can they see?

WWW. Pretty simple to remember. Keep it in mind any time you purchase a new connected device - and always keep it in mind before you or your family post or upload any content to the Internet from any of your devices.

Chapter 3

Connectivity and communications

Wi-Fi, DSL, ISP, WAP, and so on. Even the simple act of connecting to the Internet seems like you need to learn a new language. But as you probably know, the technology industry loves its acronyms. Maybe even a bit too much.

Think about all those times you've set up a new device or when you set up your Internet connection running for the first time. You crack open your instruction manual, start reading, and you're quickly swimming in a sea of acronyms. Then, to make matters worse, the manual is using them in a way that assumes that you know exactly what they mean. If that sounds familiar, take a little comfort. Millions of people feel the same way.

Let's take this chance to talk about some of this stuff in simple language as we take a look at what happens when our kids want to access the Internet with their first device. From there, we'll cover some very specific tips on email, social media, sharing photos, and other things they'll want to do once they go online.

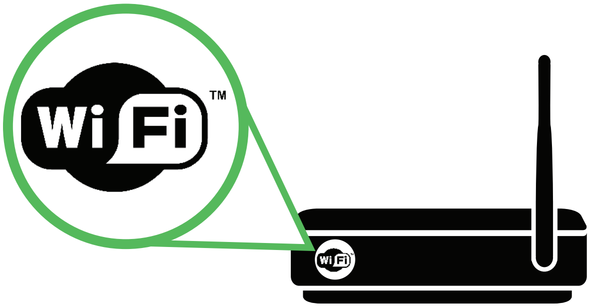
This is a very nuts and bolts kind of chapter in many ways, but even if you're already familiar with these subjects yourself, I still encourage a very close read. There's a good deal to learn about privacy and protection - for you and your kids.

Connecting to the Internet

The first thing they'll want to do is access the network at home. For many people that means a wireless connection via Wi-Fi. Ah, there's one of those terms again. You're likely well aware of this one, but here's a quick primer with a few more details. On the most basic level, Wi-Fi is a way of wirelessly sending information and connecting to the Internet using radio waves. Your Internet Service Provider (ISP), like the cable or phone company, will often provide you with a device typically called a modem or a router that connects to the Internet and that generates a Wi-Fi signal in your home. That signal typically has a range of 65 feet, creating a "hotspot" of internet access in your home. Things like walls, different floors, or the floor plan of your home can shrink it a bit, but that should give you a good idea of its reach. This hotspot allows other Wi-Fi devices like game consoles, computers, smartphones, tablets, and cameras to connect to the Internet and each other, such as when you print a document from your computer to your wireless printer.

Let's pause for a moment and think about that. What you have is a little broadcast network for all your digital activities and all your data - data you download from the Internet, data you upload onto it, and even files that you share within your own home.

Your world, your stuff, is all available on the network. Now throw in the fact that your Wi-Fi signal can spill out into the street, the apartment next door, or even into your neighbor's house, and, well, you get the picture. Network security is an absolute must, which is why you'll want to make sure your network uses encryption so that people can't access it unless they have the key. Because of this, the trade organization that certifies Wi-Fi products has adopted various encryption technologies. The most current one is called WPA2, or Wi-Fi Protected Access 2, an improved security protocol that is required on any device that bears the "Wi-Fi" trademark. To ensure that your product is certified, you'll want to look for this little logo somewhere on the product or its packaging (overleaf).



This brings us to the next important point: passwords. You'll want a password for your network. A strong one. What follows is good advice not just for your network password, but for all your passwords in general.

Setting a password

Start off by letting your kids know they need a strong password that no one else can guess, and they should never share it with anyone. A hacked or shared password can open up a world of trouble. A great example is what can happen with a password for a social media site. In someone else's hands, that password can create all kinds of damage. That person could completely take over your child's account, delete photos, remove friends, or simply make it seem like your child is saying all manner of nasty things. Whatever example you use to bring the point home, make it tangible. That password is directly tied to their personal information, their online profile, and ultimately their reputation. Help them understand the real-world consequences of someone getting access to all their "stuff" and possibly even stealing their identity with it. Play out a little worst-case scenario so that they can really understand the consequences when someone steals their identity. We'll cover more on this shortly when we talk about social media later in this chapter.

The next thing everyone in the family needs to know is that the "traditional" password is dead. You know, passwords based on your name, your pet's name, or even your birthday. Our instinct to use easy-to-remember words like these or to use numbers with a linear base as in 1,2,3,4 or even 5,6,7,8 has to change. Likewise, if user "Sally Mills" tweets on Twitter that her birthday celebrations are happening on the 5th of February and she subsequently uses "05FebSally" as her Facebook password, then this is not secure. Automated password cracker software has the ability to trace an individual's public web activity and make these associations, and ultimately compromise passwords relatively quickly.

What do we need to do, then? Here's a great little guide to creating strong passwords - you should use ALL of the following elements:

- **A mix of lower case and UPPER CASE letters**
- **An "alphanumeric" mix of both letters and numbers**
- **So-called "special characters"** such as @,£, $,^<, _, * or even { and | if your keyboard has them
- **If possible, words that are not common English** or any other language - or at least non-standard words and phrases ('nonsense' if you prefer the term)
- **Enter the passphrase!**

Put it all together and the more sophisticated password of today starts to look something more like this: AVGrocks4security!

Note that you can still create a personally meaningful password with this formula that's still complex and difficult to crack. So, for example:

- **For the English Premiership fan:** Man#Uwrkngwell4ever! (Manchester United Working Well Forever)
- **For dessert lovers:** IamdaKingof#1choc&iceKreme (I am the king of chocolate and ice cream)
- **Or for the runner:** Neil!luvs2jog

All of these examples are improvements upon password, admin, or 12345678 - passwords which are still used with alarming regularity. Your whole household should be taking this route to secure their social networking accounts, email accounts, and their cloud-based storage accounts such as Apple's iCloud service - anything that takes a password. As you can see, passphrases do not have to be 40 or even 20 characters long to be strong and effective. Another thing to consider using where possible is 'two-factor authentication.' Yes, that sounds really technical, but in fact it's something we use every day. In plain language it simply means that your security uses two different types of identification: one is something you possess and one is something you know. What is an example of this in everyday life? If you have an ATM card in your wallet then you use "two-factor authentication" every time you withdraw cash or pay by debit at the store. Your card is the "something you have" and your PIN is the "something you know."

This type of authentication to access something has grown in use in recent years. Banks were some of the first, and with the advent of the mobile phone its use has really taken off. Your bank may well use your registered mobile device as the "something you have," and when you're transacting online through a computer they will send you a text message with a code to your phone. Then, back at your computer, they'll ask you to enter the number displayed on your phone to authenticate that it's you making the transaction.

Why do I bring this up? Well, more applications and services are starting to use this method to stop passwords from being compromised. A great example of this is Twitter. You can select password resets to be sent to your mobile phone or, if you want to be even more secure, Twitter will send you a passcode to your phone when you want to access your account. This makes your account more secure, but it can prove painful if you lose your phone a lot.

I believe this method will become increasingly normal for our kids as everyone's use of mobile devices increases. In future years, we may even see this technology evolve so that you'll be authenticated simply by placing your mobile device near the computer. That's some way off yet, but things are moving in that direction. Think of it this way: our accounts at banks, social networks, and other organizations or institutions are all highly personal assets. You'll want to do all you can to protect them. And it's good to know that the industry is working hard to develop better security solutions on your behalf.

Email

The ability to send electronic letters and messages to each other is awesome, but of course it opens up our email inboxes to spam.

'Spam' is a somewhat playful-sounding term for the very real problem of unsolicited email. At its "best," spam is the digital equivalent of junk mail. At its worst, spam is designed to trick you into opening attached files or clicking on links that can open you up to security attacks in the form of malicious software (malware) or viruses.

A very common spam attack comes in the form of "phishing," which lures you to present personal information under false pretenses. A great example of phishing is where you receive an email from what appears to be an online retailer like Amazon. This phishing email may state that there's an issue with your account and that Amazon needs you to send your password to correct it. Of course, it's not Amazon. It's a phishing artist who wants to hack your Amazon account and harvest your personal and financial information.

While most retailers do an excellent job of telling you that they'll never ask for your password, imposters persist - people who prey on the fact that we're busy and may not give the validity of such an email a second thought.

What's more, some of these phishing attacks can be very sophisticated. It can take a discerning eye to determine that a phishing email is illegitimate - you'll need to take a close look at the address of the sender, the design and layout of the email, and then determine if it's legitimate. In other words, listen to your intuition. If it seems "phishy," it probably is. Here's the rub, though: your kids may be more prone to take such emails at face value and fall for the "phishing" lure. For that reason, we'll cover some ways that you and your kids can avoid phishing scams in just a moment.

For now, let's keep talking about the subject of email in general. As we consider the risks and potential pitfalls of email, we ask ourselves, "Do we want our children to have email?" The answer is that of course we do. Aside from using it to foster their relationships with friends and family, there simply has to come a time where we have to introduce them to this medium and educate them about safety as part of the process.

In fact, many schools today already give our children their own email addresses, offering them a first and protected step into this world. These are typically managed as a closed and controlled user group to protect them.

What this means is that John Smith who attends Big School would have an address of john.smith@bigschool.edu for use internally at school, but he could not send or receive email outside the domain of bigschool.edu. Lots of schools are using services like this as it's a great way for kids to email homework to their teachers or to simply reach out for a little extra help.

As for their own personal email account, there are many ways of getting a webmail account, which would allow them to send and receive email from a web browser. This is something you can do for your child yourself, or they can do it on their own. The most popular are Gmail and Yahoo! Mail, but there are loads of other reputable options to choose from, like Microsoft's Outlook service. The sign-up process for most email accounts is quite similar and very simple.

Click on it and select "sign up." Enter your chosen user name, if it's already taken you can pick one from the alternatives that are offered or think up another option yourself. From there, you can create a password. (Remember our guidelines!) That's pretty much it. Email, in just a few clicks.

Some email providers allow you to set up a feature known as forwarding. This feature forwards a copy of an email to multiple email addresses. For example, my email account at tony@sampledomain.com can also forward email to another email account, such as tony198237@webemailaddress.com. This way, I can provide one simple email address to my friends and family while still receiving their email in two different inboxes. What is the benefit of doing this for a child? When you configure the forwarding you can opt to send the email to more than one email account, such as your own, which would allow you to see all the email that's being sent to your child.

As you can imagine, deciding whether or not to do this is a big decision. If you choose to openly receive all their email, you should have a conversation about it first so that everyone knows where they stand. Do I do this in my household? No. My son and I actually have an agreement in place. While I do not intend to invade his privacy, he knows that I won't hesitate to check up on things if ever I suspect that something is wrong.

Now that we've talked about setting up an email account, let's go back to the subject of spam and phishing. There's some very specific advice I can offer up. First of all, you can count on it: your kids will get similar junk email or spam to what you get.

Fortunately, many email systems today have good filters that protect you from the bad stuff. Additionally, many full-featured security software packages will offer an additional layer of protection that will screen out even more junk. Still, spam will get through. Teach your kids the same "stranger danger" tactics you taught them earlier in life, because many of the same rules apply to email. If you don't know who it's from or it does not look right, then you should delete it without opening. If you have opened it, definitely do not open any attachments or click on any of the links that may be in it.

A good thing to do is show them some examples. Look online, or call them over for a look if one such email makes it into your inbox. Show them how these emails try to trick you into handing over personal information. Explain to them just how damaging this can be. Again, help them think the scenario through all the way, like imagining when they apply for a driver's license only to find that they have a police record because someone stole their identity years ago. While that may seem alarmist, it's reality. These things happen and we need to be careful.

Underscore the fact that phishing emails can look like they came from a friend or a popular website. They can be very convincing.

For example, imagine your daughter is using Twitter. One day, she opens up her email and sees an email that really looks like that it's from Twitter. The email says something along the lines of "We need you to update your profile . . ." and offers up a link she should click to do this right away. Given that this is a phishing attack, clicking this link wouldn't take your daughter to the Twitter site. Nope. It would whisk her away to a lookalike page where your daughter would be asked to type in her ID and password. If she starts filling in that information, it is mission accomplished for the scam artists. They would have the keys to her account . . . and her personal information.

Phishing emails can look like they came from a friend.

There are variants on the theme. A phishing scam can occur via text, instant messages, and so on. Either way, here's a quick checklist to help you and your kids nip those scams in the bud:

- **Trust your gut**
  If you get an email, text, or message that seems a bit odd, it probably is. Consider how the message looks, reads, and what it's asking you to do. Ask yourself, would Twitter, Facebook, my bank (or whatever the business or institution is) reach out to me this way? Again, show your kids examples of what spam and phishing emails look like, just as we described above. Help them develop a critical eye.
- **Don't click**
  Resist the urge to click the link that's in the email to see what's going on with your account or whatever it is they're asking you to do. Don't cut and paste the link into your browser either. That's just as bad. If you're curious, go directly to the website yourself to manage your account. Open a fresh browser, type in the address yourself, and check your information from there. This approach will help you avoid any trickery, and it will give you the peace of mind of simply checking with your account anyway to ensure that all is well.
- **Hold onto your personal info**
  Don't send it on the phone in response to a text message, and certainly don't send any by email.
- **Don't open attached files in email right away**
  If it's from a stranger, treat it with great caution, as it may contain viruses or spyware. Also, take a close look at attachments sent by friends. If the attachment is unexpected or comes attached to an email that doesn't seem like it's been written by them, it may contain a virus – sometimes our friends' email accounts can get compromised too!
- **Use security software**
  Look for security suite software that has email filters and the ability to scan email attachments for viruses. There are many reputable choices available.

Browsing and using the Internet away from home

There are plenty of opportunities to hop onto the Internet when you're away from home. There are public Wi-Fi networks you can log into while you're at a coffee shop or library, and you've probably seen "business centers" in hotels that have a row of PCs with access to the Internet. They're all very easy and convenient, but it's important to remind our kids (and ourselves) that these are public access points, which means we need to take a little extra care when using them.

Let's start with the hotel computer example. Say your kids want to pop in and check their email. Make sure your kids understand that they should always sign out of their email account when they're done checking their mail.

After that, they should close the browser down when they're done surfing around. This will make sure that the next person using the machine can't go back into the browser and continue their session.

Additionally, teach them to never store their passwords on a public machine. There is no need to do it, and doing so is a security risk - like leaving the combination to your school locker posted right on the door. A simple phrase sums up activity on public computers nicely: leave no trace.

As for logging onto a public Wi-Fi network at a coffee shop, library, or a hotel, you'll want to remember that these are networks, just like the one you have at home. The difference is that you're sharing the network with dozens and dozens of strangers.

A general rule of thumb is to minimalize making any sensitive transactions on a public connection – like online banking or anything else that involves sending passwords.

Naturally, security is very important here. What's great is that your Windows laptop takes care of this for you. When you're joining a network for the first time, your computer will ask you what type of network this is - home, work, or public. Be sure to select "public," which tells your computer to automatically "lock down" a number of network security settings for you to keep you and your data "hidden" from other people on the network. Meanwhile, on a Mac, make sure you have "File Sharing" turned off in your system preferences menu (System Preferences > Sharing > File Sharing), because you don't want to give others access to any of the files on your computer.

Beyond this, a general rule of thumb is to minimalize making any sensitive transactions on a public connection - like online banking or anything else that involves sending passwords. If you do, absolutely make sure that the banking, shopping, or webmail site you're visiting is using Secure Socket Layer (SSL), which is easily identified by looking in your address bar for an address that begins with https (note our emphasis on the "s"). This means that the site is using SSL, a set of protocols that provide an additional layer of security. It's very common to see SSL used on banking, shopping, and email sites. Keep an eye out for "https." It's a good thing.

Additionally, turn off your Wi-Fi when you're not using it. Simply shutting it down when you don't need it is the best protection of all. This is really easy to do.

On a Mac, you simply click the Wi-Fi icon in your menu bar and turn off your "AirPort" setting. In Windows, simply locate the wireless signal bar icon in your task bar and right-click to turn off your Wi-Fi. When you're ready to hop back online, simply go through the same process and turn those settings back on. Even better, lots of laptops have a little switch on the side that turns your Wi-Fi on and off. A simple flick and you're all set!

Photos

In Chapter 2 we talked about the concerns around geotagging, which is the location information that can wind up in photos. Let's build on that with some additional advice about photos in general, the sort of things we should all be thinking about when posting photos online.

The first is that we should all live under the assumption that any picture taken will end up on the Internet. With all the connectivity, the ease, and the impulse behavior regarding posting photos, it's a good way to look at the world. Get your kids thinking this way, and get them living this way too.

Live in the moment, but remember that the pictures can be forever. After all, later in life, your boss might see them! Also, think about what's in the photos themselves, all the little clues they may give away about your kids and your life.

For example:

- **Before posting any photo** make sure nothing in it gives away private details, such as the name of your child's school on a t-shirt or your address on a mailbox.
- **If you're on vacation** think about whether or not you're ready for a broad, online audience to know that you're out of town.
- **Go into phone or camera settings** disable any kind of geo-tagging features that might provide others with details of exactly where you are at a given time. Do the same for the settings of the social network site you're posting them on.

Social Networking

Some parents ask me, "Should I let my kid have a Facebook account?" Well, if your son or daughter meets Facebook's minimum age requirement of 13 or older and they want an account then the answer is "yes." Why the quick response? Well, if you say "no" they may very well do it without you. The best advice, and you'll see this throughout this book, is to be open and honest with each other. We have to embrace the fact that our kids are developing adults, with their own lives and their own need for privacy. Take pride in that, understand they may not share everything with you, but be ready to step in to support and parent as needed. It's like everything else when you are raising a child - knowing when to be at their side and knowing when to step back.

Broadly speaking, social networking sites like Facebook are a way of communicating with other people and sharing pictures, comments and experiences of everyday life. You are given your own page to customize. You can upload pictures, videos, play games, and companies will even encourage you to endorse their products to get discounts or offers. Specifically on Facebook, there are applications for reviewing books, films, and restaurants - in fact nearly anything you come across in day to day life. It's your personal place on the Internet to express yourself to a select group of friends. In many ways, it really is what you make of it.

There's also the ability to send instant messages or email - type messages, which offers our kids a little teaching moment about the things that they write and say online. For example, I did something very interesting with my son after he concluded an online chat session with a friend. I cut and pasted part of the conversation and asked him to read it to me. In isolation, it took on a completely different meaning than what he really meant in the context of the conversation. He soon understood that someone could misrepresent what he said, use it to cyberbully someone else, and make him look like the bad guy.

Good advice to kids: the things you say online could be used against you. Think twice about what you're saying, how you're saying it and how it may affect others (which is simply good communication advice in general).

Needless to say, there's a whole host of things to keep in mind with social media. So, let's assume that your kid is 13 or older and you've said "yes" to a Facebook account. Help your child set up the account, take an interest, and give a little guidance on how it works and how he or she should interact with others. That guidance should look a little something like this:

- **Don't share personal data like your birthday, town of birth, etc.**
  This information is also used by many organizations to validate your identity when they ask security questions, so keep this info hidden. Your friends already know when your birthday is, they don't need to be told by Facebook.
- **Who are your online friends?**
  Do you know them all? Does anyone really have 1000 friends? Even 50 would be a lot!
- **Who can find you and what can they see?**
  Imagine everything you send or receive being written on a billboard outside your house . . . yep, that's what happens when you don't manage your content and who can see it. Facebook has all kinds of great settings to limit who can see your content, like "just friends," "friends of friends," and "anyone." The "just friends" setting is best, because this ensures that strangers can't see what your kids post.

- **Use the Facebook tools that let you arrange your friends into different groups**
  With these groups, you can select which groups see different posts. Give your kids a little life example: you don't share everything with everyone, so don't share with everyone online.
- **Take a close look at your profile**
  Check your picture, your description, your latest round of pictures and posts. If someone looks at your profile, ask yourself what kind of impression it all makes. If some things look a little questionable to you, then imagine how it looks to others.
- **Decide if you want facial recognition turned on or off**
  This is the ability for Facebook to automatically tag you in a photo posted by you or someone else. While this sounds cool, some pictures may not be the ones you would want to have your name against. Turning this feature off won't stop such a photo from being posted by someone else, but it will keep your name from being automatically tagged onto it.
- **If someone does tag a picture with you in it**
  Ensure that you get the ability to review it before the tag appears. This is another feature that you can control from within Facebook's settings.
- **Switch off the Google indexing in your Facebook settings**
  This will keep your profile from appearing in search. Do people really need to see your profile in search results? Surely your friends already know who you are.
- **Make sure your profile isn't automatically shared by your friends' apps**
  Here I mean games or those little quizzes and polls that pop up in your Facebook page. If your friend is using an app and has access to your profile, then that app can see your data – unless you select your Facebook settings from stopping this. Also be aware that using some Facebook apps on your own will do this. Luckily, such apps take you to a warning page that notifies you of this before you use them.
- **Are you endorsing products personally?**
  If you "like" a company or product page, then your details may be used to endorse that product when it's being promoted to your friends through Facebook's ads.
- **Do all these things for your social media profiles too**
  If you don't do it, then how will your kids ever learn from you?

YouTube

Great site, great fun, YouTube is the place where the world watches more than 6 billion hours of video each month. Every minute, roughly 100 hours of video are added to it, from educational videos, comedy clips, product demos, reviews, rants on all kinds of subjects, fitness workouts, video game walkthroughs, movies, and on and on and on. Clearly, it's a top destination on the

Internet. Trust me, your kids will most certainly spend time there.

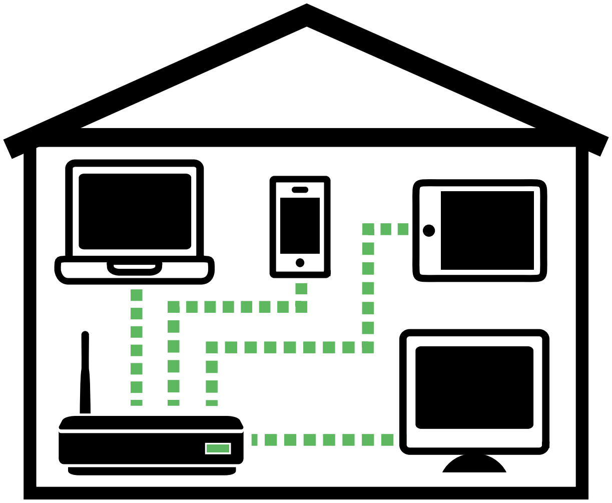
Now, with all those billions of hours of content, you have to expect that there's a fair share of it that's not right for your kids. While YouTube goes to great lengths to ensure that illegal and vulgar material don't make it onto the site, there are still some videos on there that push generally accepted boundaries of what's appropriate - let alone what you feel is appropriate for your kids. What's more, each video is accompanied by a comments section where some of the user comments on the videos can get vulgar and inappropriate too. What's a parent to do?

Set the ground rules. This is an opportunity to continue the ongoing conversation with your kids about what works for your family (and what doesn't).

Communicate your values. Be open about the kind of content that's welcome in your family, as simply forbidding the use of YouTube closes off an absolute wealth of some really useful, educational and entertaining content. Plus, forbidding its use may simply drive your kid's viewing habits underground, which you don't want either. Encourage the use of YouTube's "safe search" feature that helps remove vulgar language in the comments and that helps block objectionable material.

Now here's the other side of the coin: your kids can also post videos to YouTube. Much like Facebook, it's very easy to create an account and start posting videos of your own. With built-in video cameras on smartphones, tablets, and computers, the barrier to entry to getting videos online is very low. Anyone can be a producer.

So, should you let your kids start posting? Well, if they're at least 13, they meet YouTube's age requirement. But the real answer is found by asking what it is they want to share and why. Here's a checklist to help your family think this one through:



- **Watch their videos**
  Take a look at what it is they want to post. Get a sense of what they're trying to communicate and share with their videos. Are they recording video of a school soccer game, skateboarding tricks, or reviewing games? Remind your kids that 1 billion different people watch videos on YouTube every month. That's quite an audience. Is everything in their video okay for the entire world to see?
- **Play it safe**
  Think about the photography guidelines we discussed, specifically

how your kid should look to protect his or her identity by not revealing addresses, names, or anything else that could help unsavory folks track them down.

- **Be private**
  YouTube allows your kid to mark videos as "private" so that only their friends on YouTube can watch them. This is a great approach.

In a nutshell

We've covered a great deal of material in this chapter, and it's no surprise. There's a lot to consider when your child wants to go online, from getting them there safely to giving them the knowledge and tools they need to stay safe.

While configuring all of the settings, features, and sites the way we want is highly important, we need to realize that technology is only half the story. The other half is you and your relationship with your kid.

No filter, safety feature, or device is a substitute for you and your guidance. Of course, that very nearly goes without saying, but it's a vital reminder that we have to be just as engaged in our child's digital life as we are in their daily life. The lines between the two are absolutely blurring. Their actions in the digital world cast ripples into the physical world and vice versa.

Understanding this equation and your role within it will go a long way toward keeping your kids safe - and it will help you better prepare yourself should more serious problems arise, like cyberbullying, which we'll take a much closer look at later in Chapter 7.

Chapter 4

The smartphone chapter

The smartphone really has changed everything, hasn't it? The most common question for anyone with a 6th grade kid is "When to do the smartphone thing?" It's a big question, and there's no set answer as every parent and kid has a different idea of what the answer should be. It takes a bit of information-gathering, and even a bit of soul-searching, as we decide when the time is right.

Before we talk about the things that might help you arrive at your own answer, let's look at our own behavior with our smartphones. See if you recognize yourself in these scenarios . . .

- **You're at the restaurant** with the family or even on a romantic night out. Do you ever sneak a peek at your smartphone during the meal?
- **Wake up time.** Ever grab your smartphone to see what email or messages there are before you're even out of bed?
- **Have you ever avoided talking to someone** by sending them a text instead?
- **Oops!** How about those times when you've had a few glasses of wine and sent a text that you wished you hadn't . . . or posted something on Facebook?
- **Ever passed the phone to your kid** so you could have an uninterrupted conversation with someone or simply get through a shopping trip in peace?

Get the picture? As adults, our use of smartphones can leave a lot to be desired and, like it or not, sometimes the example we set our kids is not so great. So the first thing we need to do is try harder and start using our devices the same way in which we want our kids to use theirs. Now let's dive into a few specific issues that'll be top of mind when the time comes for your kids to make the leap to owning a smartphone. The first one is a biggie, as it's one that can leave you out of pocket - the data plan.

When you're using the Internet away from home, the phone is typically going to use the cell network to pull down all that data from the website you're browsing, the music service you're streaming, or the app store you're downloading from. That activity takes a portion of your data plan, which is usually a set limit, along with penalties for going over that limit. Now add your kid into the equation. Ker-CHING! How do you get around that? For starters, curb your data usage when you're on a cellular network. Keep track of it too. Many carriers provide apps and websites that make it easy. Plus, keep an eye out for public Wi-Fi networks that you can connect to - the experience will be faster, and it will usually be free, such as in coffee shops and libraries.

It's good to keep this in mind, because there's a big financial benefit to tapping your smartphones into a Wi-Fi network when possible, to keep costs down and to save that data plan for when your family needs it. Be aware of one thing, though: if your cell phone carrier has a content filter to help keep inappropriate content off your kids' phones, know that it will not filter the traffic over Wi-Fi. For example, in the United Kingdom adult content is blocked on the cellular network by default. It does not work on Wi-Fi connections, whether that's your network at home or Wi-Fi networks in public, again like coffee shops and libraries.

So, now for the big question: What age is the right age to get a phone? My opinion on this is to hold out as long as possible because phones, particularly smartphones, change the way our kids communicate, and not always for the better. Texting makes a lot of communication very simple but it also drives us not to speak to each other, as do many of the other digital communication methods you'll find on smartphones.

Let me use my own son as an example: There were 20 children in his 7th grade class, and at the start of that year about half of them had their own mobile phone. Interestingly, just a year before that, at his 6th grade birthday party, only one child had a smartphone. For a while it was like a compelling little magnet that everyone was drawn to, but happily it did not rule (or ruin) the party.

But things changed quickly in that year between 6th and 7th grade, at least at my son's school. Lots of kids had them by then. So, 7th Grade seemed about the right time, right around the age of 13, to get that full-on smartphone. That doesn't mean that my son waited until 13 to have access to a mobile phone. We had a family flip phone that we shared so that when he went out with friends we had a way of getting in touch with each other. Of course a "boring" flip phone isn't as cool as a smartphone, but it did just what we needed it to: make calls.

My son's birthday is towards the end of the academic year, so the pressure was on towards the end of 7th grade as many kids started getting phones when they turned 13 that year. At Christmas, guess what was number one on his list? Yep, a smartphone. We made a bargain - wait until you're 13. I got away with that one and we waited until his birthday.

Of course not all parents wait this long or hold out, but just remember the earlier you issue a phone the more you are ushering your kids into an adult world. So perhaps sparing them that and keeping them innocent as long as possible is a good thing. That's a major point to consider when the inevitable smartphone conversation comes up, or if it's already in full swing.

So what happens when your child gets his or her first smartphone? What are some guidelines you can put in place that help set your kid off on the right foot? Well, let me start off with one of my own. We have a rule in our house that seems to work well for us, and the feedback from other parents who've tried this is positive too: have a location in the house where phones live. Ours is on the kitchen worktop. We call this "The Basket." Phones live in the basket during meal times and after 9pm in the evening, and when they're in the basket they're either silenced or disconnected. This goes for me too. You need to lead this one by example, and it's not easy! But the payoff in our family has been great.

Some parents have gone down the route of a contract. I am not sure I agree with needing to have a written document, but if that's what works for you, then go for it. Below is a sample. If you go with things this way, I strongly recommend that you precede it with a conversation about what's acceptable and what's not. So if you're thinking about a contract or verbal agreement, here are the important elements - both for kids and parents alike:

The child . . .

- **The phone is a privilege not a right.** Bad behavior or conduct with or without the phone will result in the removal of the privilege.
- **Text messages will say only what I would say out loud or in person.** There will be no threatening or inappropriate behavior.
- **At 9pm the phone will be in the basket.**
- **At meal times the phone will be in the basket.**
- **Charging my phone is my responsibility.** I will not blame you when it's not charged.
- **I will monitor my usage and make sure I don't run up a huge bill.** I will stick within the plan.
- **The phone is expensive.** I will cherish it and care for it.
- **I will be respectful of where I am.** I'll switch off the phone if needed, like at school, church, the library, and other places where it's just not appropriate to have it on.
- **I understand that my cell phone may be taken away if I talk back to my parents.** The same will happen if I fail to do my chores, or I fail to keep my grades up.
- **I will obey any rules my school has regarding cell phones.** Just a note here, I think they should not go to school unless there is a solid good reason to take it. There are enough distractions from learning already.
- **If I receive suspicious or alarming phone calls or text messages from people I don't know, I will tell you.**
- **I will not take or send embarrassing photos of my family or friends.**

The parents . . .

- **At 9pm the phone will be in the basket.**
- **At meal times the phone will be in the basket.**
- **I will help to ensure that my child can achieve the agreed rules.**

Explain the rules in detail so there is no misunderstanding on either side. And don't stop with just your kids. Grandparents, friends, and relatives all need to understand the rules too. This will help you enforce them and also abide by applying the rules equally. If Grandma

gets her phone out at the meal table show her the basket!

Another guideline is to keep a close watch on which smartphone apps are being purchased and used. This is an entirely different dimension of the smartphone given the huge breadth of games, utility, and social media apps that are available. They're all delivering (and sometimes creating) content, and you'll want to keep an eye on that.

Listen in to what your kids and their friends are talking about, like when you're taxiing them to the mall or the soccer pitch. Find out what apps the kids in the car are talking about, and load up the apps in your own time to see if they are appropriate. I do it all the time.

Recently I drove a bunch of boys to a laser tag party and they were talking about some stick-man game. I loaded it up, and, man, is that game addictive! Now I'm stuck! My point is this: kids will find apps that you will not, so join in and try them out yourself. It will give you more understanding, and it will also keep you up to date on what they are all playing or using.

Another key area to have a discussion around is illegal content, specifically cases where the content infringes on someone's copyright. Prime example: downloading illegal music and movies. This may seem like you get it all for free, but think about the consequences. Imagine your child has an awesome talent and is driven by a dream to follow this talent and become a world famous rock star. They will work hard and have a schedule that will be very hard for the first years. Now imagine that no one paid them for their work. In fact, imagine someone stealing their work. Yep stealing someone's song means you are stealing their work. This is how they make a living and downloading illegal copies means that you are taking money right out of their paycheck. Explain this to your kids. The same holds true for writers, artists, anyone who puts their creative work out there in digital form. Ask your kids if they'd like it if someone stole from their allowance. We all know the answer to that.

Make no mistake, downloading illegal or 'pirated' content is a crime. Individuals can and will be prosecuted for downloading illegal content. It happens.

Look for more of those teaching moments that help them become a smart digital consumer.

On a somewhat related note, give your kids a budget for apps and music or allow them to manage that budget as part of their allowance or earnings from odd jobs. At 13, they need this responsibility. As I said, owning a smartphone is yet another entry point into the adult world, and managing a budget is a natural part of owning a smartphone. This budget does not need to be much, and can even be in the form of app store gift cards. Teach them the ins and outs of app stores, where some apps that appear to be free at first will hammer you for in-app purchases later on. Is that a good way to spend money? Help them decide. Look for more of those teaching moments that help them become a smart digital consumer.

There is one last subject I want to cover on this topic: smartphones have the ability to be located by either GPS (yes, that satellite navigation stuff you have in your car), or by triangulation of the phone signal. What this means is that the location of the phone can be pinpointed on a map.

Now this is an awesome feature if you lose your phone and want to find it. There are lots of apps that will allow you to do this, many of which can even let you lock and wipe the phone if it's been stolen. Should you use this technology to track where your kids are? "No" has to be the first answer. There's no harm in configuring this feature for the purposes of finding the phone if it's lost, or in an extreme emergency to locate your child. But should we know everywhere our kids go? Well . . . no. When I was a kid my parents did not know everywhere I was, they just had a general idea. If they always knew where I was, then I would not have got up to some of the great stories and learning experiences that are my memories today.

While we need to know what our kids are up to and where they are in general, we also need to give them enough space so they can find out who they are as well. It bears repeating: they're becoming adults, and we have to let them live and learn, be responsible, and earn a sense of self. Give them that space, without the "electric eye" of technology constantly hovering over their shoulder.

In a nutshell

Mobile phones/smartphones are here to stay, and to our kids this is just another part of normal, everyday life - even if it may still feel strikingly new or even a bit unsettling to us. Just remember this, make sure that whatever rules or practices you put in place, you live by as well. We're all learning how to balance all this technology in our lives. But while all of this technology may be entirely new, good old common sense is not. Think about some of the core parenting principles that were at the foundation of the advice in this chapter . . . like applying "stranger danger" to spammy emails, or to basic expectations of polite behavior at the dinner table.

So, when in doubt, go with your gut instinct as a parent. Take the good things you already know about parenting and see how it relates to all these new devices and situations. How much of it still works? You may be surprised.

Chapter 5

Everyone on their best behavior

A few years ago AVG coined the term "Digital Birth" to describe the moment that an online identity begins. It's an interesting term that was inspired by a striking piece of data: at least a quarter of today's children have a digital birth before their physical birth when excited parents post news of their pregnancy on their preferred social networks. This digital birth announcement is typically followed up with ultrasound images, perhaps an announcement of the baby's gender, and so on. In this way, our kids are "born" online.

So begins their story, and so begins the digital footprint they'll leave on this world. If that seems a bit early, then consider this: by the age of two, more than 80% of children have established a digital footprint thanks to their parents and social media. Think of all those pictures of "Little Miss Puddingface" making a mess in the highchair and all those updates about this milestone or that. Put it all together and it's easy to see that, right from the beginning of life, a person's digital identity can be largely out of their hands.

"Sharenting": When parents share details about their children's lives on social media.

This is something we call "sharenting," when parents share details about their children's lives on social media. It's a really important point to consider in the conversation about kids and technology. Just as our kids need to understand the consequences of their actions, we need to understand the consequences of our actions too. So far, we've talked about ways our kids can manage their digital identity to avoid embarrassment or employment issues later on. Now let's take a look at the things we can do to avoid leaving a trail of awkward content about them ourselves.

Sharenting

Here are a couple of examples of sharenting gone awry, one of which was a mistake and another one that was just plain embarrassing:

My son called me out one day, "Dad, why have you posted pictures of me with my full name on the Internet?" My quick defense was, "What? No I haven't." I've taught my son to Google himself on occasion so that he knows what is out in the public domain. He'd just done this and came across a result from Flickr, the photo-sharing site. I had posted an image with a tag using his first name in an album that was tagged with our last name. Turns out that Google had cleverly put the two together and, sure enough, there was his first and last name brought together in association with the photo.

It was easy to fix. A quick removal of the tag was all it took, and 24 hours later the photo in that album had been re-indexed by Google and no longer appeared. Lesson learned.

Like all parents, some of the pictures we have of our kids are cute and innocent but sometimes they're a bit embarrassing to them as they grow up. We have one such picture of our son that never made it to the Internet, but did end up on a projection screen in his school. In kindergarten my son was chosen to play the

Angel Gabriel in the school production - white tights and outfit, the works. He was so cute and really looked angelic. My wife was using a picture of this as a background on the laptop she was going to use for a presentation at his school. Fortunately my son asked for it to be removed before his friends saw it. Phew, he'd probably never hear the end of it! And neither would we.

Right there you have two examples of how our actions, even though innocent, could cause a problem. These are things we have to keep in mind when we're sharenting - the ways we naturally want to share about our kids. The considerations and risks are much the same as the ones that our children face when they decide what to share and what not to share. Our posts are at possible risk of becoming a permanent record of their formative years. Now that social media reviews are routine in employment, housing, and other types of advance screening, your kids may not be so happy when photos of bizarre haircuts and awkward prom dates turn up.

In a larger and more sobering sense, parents should always be aware that certain types of sharenting could violate their children's future privacy or imperil their long-term digital identities. Are images of your children getting harvested and used by strangers for other purposes? Do you really want to reveal your kids' whereabouts via geo-tagging? What seemingly innocuous but ultra-private information do you unwittingly reveal with an image of your child puffing an asthma inhaler? People can and will draw up all kinds of conclusions, ones that can have an impact down the road.

Of course that doesn't mean we shouldn't be proud parents or share moments online. So what are some good practices online when it comes to sharenting? Here's a list of things to keep in mind:

Be aware of privacy settings when you post information about your child online. Once you post it, are you giving these rights to the website owner? Many social media sites take ownership of the content, and while this may not cause a problem today this could be an issue in many years to come - particularly if you or your kids want that content removed.

Think about the consequences of what you're posting about your child. Will that picture still be funny when he or she is 12? Or 17? Or 35? I'm sure we all understand this one, and I know that my parents have pictures of me that I would not want in the public domain. Put yourself in your kid's shoes.

Set up a Google Alert with your child's name to make sure only information you want to be public about your child is available. It's very easy to set up, and it sends you a regular summary of search results related to your selected search term, like your child's name. Check it out at: http://www.google.com/alerts. You might be surprised by what it turns up, similar to what one family discovered when they were featured on a BBC program about Safer Internet Day.

Here's what happened on that show: A woman and her daughter shared their names and the name of the town they lived in with an Internet security expert who then dug up as much information as he could find on them.
Now keep in mind that this mother and

daughter considered themselves to be very careful folk. They believed that they had private profiles and that they were not guilty of "oversharing" a lot of personal information. The security expert later sat down with them and then told them some fascinating facts. He discovered that the mother had tickets to a concert on a specified date. He had also found her date of birth, her mother's maiden name, and her brother's name, along with where he lived too. The list went on. Imagine everyone's surprise! The information available online was way beyond what she believed was in the public domain. Wow, right!? I wonder what a researcher would find out about me or you?

The BBC story did not go into the detail about how information was found, but one can imagine that the data was available because certain settings were not locked down on some social media sites and possibly through other people who inadvertently shared details without thinking about the consequences.

So how do you go about auditing your own online profile? Put yourself outside your world and see what you can find out. Hop on a machine that isn't yours or a friend's, like a public PC at a library, and then start searching as though you are the security expert. Search for yourself, your friends, your family and see if there are people who don't have their profiles locked down. See if they open up a back door to your personal details.

The lesson here is that we really need to take care about what we share and the privacy settings we use on the devices and sites we use. In this day and age of digital footprints, it's important to be aware not only of what we share about ourselves but also our friends and family too. Think of it as a collage. No single piece of information is always interesting, but adding bits together can build a pretty thorough profile. Are you dropping bits and pieces of information for others to use, just like that security expert did?

Register your child's name as a domain name to ensure you own his or her Internet identity. Wait, really? A full dot-com or similar that I buy at domain registry sites like GoDaddy or one of those other domain registration sites? Isn't that a bit much? Isn't that expensive? Seriously, yes, you should do it. It's actually rather inexpensive and it's really a good idea. Here's why:

Several years ago in the UK, a fast food company ran a series of commercials about changing your name to match the license plate on your car. They promoted it as a cost-saving measure and then related it to the good value and low prices of their food. The commercial was funny because it suggested that changing your name to the unique identifier of "T510 XPR" might be the most practical and normal thing in the world. And why not? Celebrities have long been choosing outlandish names for their children that, to most of us, sound a little strange. Hello to singer Kanye West's daughter, North. Another hello to the daughter of international soccer star David Beckham, Harper Seven Beckham. Those who are famous enough to have a name that has become a household brand are aware of the issues that can arise when someone attempts to assume and misuse their identities online. When they name their children, they are also likely to register their domain name, and the availability of the

I regularly recommend to my friends that they register their child’s domain as we don’t know what lies ahead for them.

domain probably had a bearing on what name they chose for their child.

But there are lessons here for the non-famous among us too. I regularly recommend to my friends that they register their child’s domain as we don’t know what lies ahead for them - whether it is stardom in Hollywood or being the next president. Owning the domain now means that you have secured an important element of your child’s identity from the starting point, and it costs very little to do this. What format the domain takes or how many different ones you own comes down to choice. I have my domains registered as [firstname]anscombe.com,but I may also think about registering [firstname]anscom.be or [firstname]anscombe.net if I want to lock down some of the other domain options that are available. There are dozens and dozens of domain suffixes out there beyond the familiar dot-com and dot-net. Do a search on how many there are, the answer may surprise you.

Just registering the domain is a good start. Ownership gives you some options going forward and will certainly be appreciated by your children as they grow up. We don’t know what’s in store for our children, maybe even fame and fortune. But it’s just good sense to claim their own piece of digital real estate on the Internet so that they can protect their identity in the years ahead. A few dollars a year will make sure they have the basics covered. It’s a start, and who knows . . . perhaps we’ll start naming our children by domain availability. Perhaps being named “T510 XPR Dot Com” isn’t such a far-fetched idea after all.

As your child gets older take an interest in what he or she is doing online. We’ve talked about this a bit already, but this is super-important advice and it bears repeating.

So few of us actually seem to do this. Whether our kids are musicians, actors, or sports stars, we take time from our busy schedules to be interested and stand by their side as proud and engaged parents. I will share with you that my son plays soccer as a goalkeeper, and this position is not good for your blood pressure because you feel responsible for any goal scored against the team. You probably feel much the same way when your kids play or perform. So when we get back home, that muddy and disheveled kid cleans up and winds down, he often does so by disappearing into his room with a laptop, never to be seen again - until feeding time, anyway.

So there we are on the sidelines or in the audience as our kids pursue their childhood passions. Does that mean we have to hover over their shoulder and watch as they hop online? Of course not, but we have to get engaged, albeit in a different way.

Ask what they are up to even when they are not interested in showing you. You can even ask if they want a hand with what they’re working on, for example when they're researching a project or learning some new video editing software. It's a great way to naturally get involved. You might learn something too. I have a great example: My son spent hours doing some prep for school and, after some asking, he showed me a PowerPoint deck that included streaming video pulled down from the Internet. This was a couple of years back and was really quite novel at the time. It looked awesome. Once he showed me how to do it, I used it time and time again in my line of work. And here's what's really cool about all that - he felt clever. I learned something from him. In return, I got to keep tabs on what was going on in his digital life. Quite the win-win situation, right?

We also have a similar philosophy about the video game console. We play games together, which, let's face it, is fun. Plus it gives me an understanding of what he is playing.

I should point out that you shouldn't be surprised that you'll always lose. I think the games detect that a parent is playing and make you look bad just to build the kid's confidence. That's my conspiracy theory and I am sticking to it. These are just a few examples of the opportunities we have as parents, chances to participate in your kid's digital life without making it feel like you're intruding. Pick your moments, find out what works, and simply be a presence. That's the key.

Let's explore a few more topics about our online behavior, starting with a subject that can hit your family right in the wallet.

As you well know, countless scammers and legitimate companies have mastered the methods of duping children into turning down dark alleys and making questionable purchases, either from websites or app stores where parents might automatically be signed in. As we all know, depending on the payment method, weeks can pass before we notice our kids have ordered items or virtual currency that they can use in a game. It's something to think about, particularly as more and more parents let their young children use their smartphone to play games while the family is shopping or on a long trip.

These kinds of purchases have become an all-around concern. You may or may not know this, but I am a Brit living in the U.S. I keep my eye on what happens back in the homeland and I am extremely interested to see what happens with the Office of Fair Trading, which is the UK's version of the U.S. Federal Trade Commission.

They did an investigation into this very topic. Cavendish Elithorn, the OFT Senior Director for Goods and Consumer, said in the findings, "We are concerned that children and their parents could be subject to unfair pressure to purchase when they are playing games they thought were free, but which can actually run up substantial costs."

In other words, many ‘free’ games have in-app marketplaces built into them. The idea is that, by paying to purchase items or abilities, players can advance through the games more rapidly or unlock new aspects of play. The effect is that the “free” game can feel a bit underwhelming on its own and that players will feel the urge or the pressure to make a purchase. It’s an achingly common practice, and entire businesses have been built on this model of gameplay. So, if you’re handing over a device to your kids, whether temporarily or as their own personal device, be sure that you control access to the app store or other services that may have your credit card details stored. All these services have a logout/sign-out feature to protect you from this.

Here’s a quick story that made the news right around the time I was writing this book.

Imagine a man’s surprise when he discovered that he’d set the winning online bid for a car, a 1962 Austin Healey Sprite, even though this was the first time he’d ever seen the car. He suspected a scam but, when he logged onto the auction site with his account, there it was - he was the winner.

Then it hit him. His daughter, all of thirteen months old at the time, loved to play with his smartphone. She had placed the winning bid, all because his credentials were already loaded into the phone. With a few probability-defying taps, she’d made her way into his online auction app, placed a bid, and won the auction.

All’s well that ends well, though. The seller was really quite understanding about the whole affair, and it actually turned out that the sale went through by mutual agreement. What were the damages? $202. Thing is, this car was a bit of a project that needed a bit of work to say the least. Last report is that the dad set up a website to tell the story and raise funds to get the car up and running for her 16th birthday.

Fun story, and great grist for the news wire, but as with many great human interest stories, it has a moral: avoid the big debt that might be created by your kids by protecting your own login and passwords. Think twice when you hand over that device!

The written word

Ever received an email or read a social network post that you either misinterpreted or felt was something that should not have been written down? Our kids will probably relate to this better than we do because they are not masters of what they communicate just yet, as this is something we learn as we grow older.

We’ve all been subject to situations like this, whether at work or in our personal lives, where someone has used a keyboard to say something that maybe should never have been said at all. It could have been said to you. It could have been said about you. Maybe it was just poorly written and maybe the author never thought about the consequences of what they were writing and the effect it would have on others.

What typically happens next? The hasty response: the quickly read email makes you see red, you shoot off a reply that was not considered or proofread before sending, and then that email fires up an entire a stream of communication that should never have been started. It gets ugly and quickly turns into something much bigger than the originator ever intended. Yuk. We're all guilty of this one. We're only human, right?

Our kids are subject to this just as we are. What they think is a private communication can soon become a group email or even posted on a social network. The context of the content may not be understood or it may purposely be taken out of context to embarrass them or to bully them in some way.

Several years ago someone gave me the best piece of advice about writing things down. This person said, "Remember you are writing for the reader, not yourself." This has kept me in good stead when communicating, so I really want to pass it along. I would extend this advice a little further and urge you to teach your kids some simple rules when writing something digitally, and remember to abide by them yourselves as well! Here's a quick rundown:

- **Always read back what you have written.**
  Consider if you would be happy to receive it or to see it pop up somewhere.
- **Would you say what you wrote to the person directly face to face?**
  If the answer is no, delete it and start afresh.
- **Can you justify what you are writing?**
  If it's criticism, make sure you have the facts and the correct perspective. Even then, maybe it's better not to say it or to deliver the message in person or with a phone call. What you're saying really may require a conversation, not a bunch of back and forth emails.
- **Do other people need to be involved in what you are posting?**
  Is the message you are delivering best kept just between you and the person it involves? Think about that before posting on an open forum or a social network.
- **Something you find funny might not be considered humorous by all.**
  Again, think of your audience.
- **Is it worth responding to that message in the first place?**
  Or is it better to simply ignore it? You simply need to let some things roll off your back, or respond to them in a different way or at a different time.

My point here is that we should not hide behind digital delivery. This is a learning moment for our kids because developmentally they're at the point where the awkwardness of being a teen means that it's less stress to hide behind a screen. Such situations are an opportunity for them to grow. Simply put, we must keep communicating directly and embrace the skill of actually talking with someone instead of sending emails that we could regret later on. That thing in your pocket is more than a device to deliver text messages or email, it is also a phone and designed to allow us all to talk to each other. Make sure your kids get this!

Oversharing

Our last topic gives us the opportunity to talk about someone we know well: Santa Claus. To this day, the old holiday standard "Santa

The awkwardness of being a teen means that it's less stress to hide behind a screen.

Claus is Coming to Town" still strikes me as somewhat creepy:

He sees you when you're sleeping,
He knows when you're awake . . .

But at least I knew who Santa was and why he was checking up on me. The same can't be said for everyone who views our information on the web. In many cases, they do know when we're sleeping and when we're awake. They know, because we often tell them. We tell them that and so much more. Where we live. Where we are. Who our friends are. And we don't just tell them with words. We also use pictures and videos, which often give up much more about us than we want them to. This brings up the topic of oversharing, telling a bit too much, too often, about ourselves, our friends, and our families.

All this information we voluntarily give up to a world of strangers is combed by search engines, applications, websites, and people. This is along with other information we may not even be aware that we're providing - like where we go online, what we buy, and how much we earn. The more you put out there, the more there is to potentially aggregate and create a picture with. This isn't to say data collection is all bad. In many cases, your information is being collected by businesses to provide you with the best possible experience. It is indeed fun and rewarding to share with your friends on a social network, but you should still have some say in the matter. It's your information, after all. So, how do you keep from oversharing? Here are my "S.H.A.R.E." tips to help keep what Santa knows in check, along with everyone else:

S is for Sober: Sobriety isn't just about refraining from alcohol, it's a state of mind. If you're angry, excited, tired, or otherwise not at your best, you should avoid posting content on your social network.

H is for Hold on: Before posting anything, ask yourself if it's safe for the entire world to see. Even if your community is a small or private one, compromising content always seems to find its way into the wrong hands. People are drawn to it.

A is for Authorize: Set your social network's privacy settings and check them regularly, as they change periodically for many sites. This combined with a cautious approach in what and how you share will provide you with some control over your digital footprint.

R is for Reviewing: Sometimes what seemed harmless at the time could come back to haunt you. That's why a review of past updates is a must. Facebook's Timeline Review is a handy function that lets you look back on everything you've ever posted - not just on your profile, but on your friends' profiles too.

E is for Educated: The best way to protect yourself is to know all that's going on in the world of online privacy. Know what you have control over, what you don't, and how you can adjust your behavior to maintain some say in what the rest of the world is able to discover about you. Remember what we said a few chapters back about getting to know your devices and the websites you use? This is it. Look at the features, look at the settings, and decide what is right for you.

In a nutshell

The broader advice in this chapter is that our behavior all adds up - it creates a lasting footprint online, not just for ourselves, but for our friends and family too.

Whenever we act or interact online, we need to think about the impact these actions will have because everything we do online leaves a trail behind that nearly anyone can follow. It's a reminder that everyone needs to be on their best behavior, and that goes for us as parents too.

Chapter 6

Parental controls

Head over to your favorite search engine and type in the search term "parental controls." You'll end up with a lot of results, many for people who are trying to sell you something. Searching for good tools and information on parental controls for the devices your kids use can quickly become as confusing as the Internet itself.

The usual flurry of questions abound . . . What kind of controls are available? Which one meets your requirements? It can all be very daunting trying to work out what to do, all in an effort to figure out what's right for you and your child.

What kind of controls are available? Which one meets your requirements?

Let's look at why we should be thinking about parental controls in the first place. For this reason, I think it's useful to talk about three categories of parental attitudes:

1. **Your child is perfectly behaved and you feel you have no cause for concern.**
2. **In your eyes, controlling content is part of good parenting and you are being proactive by getting something in place.**
3. **Call the fire brigade! There's an issue and you need to do something right now.**

Parental attitude types 2 and 3 already understand the need for parental controls. What about the parent in the first category? My feeling is that there are probably two different subsets of folks within this category: those who have kids who are decently behaved and seem to be doing more or less OK; and then there are those who feel their kids are really well behaved and very rarely do anything wrong.

As parents, we all suffer from moments where we think our kids are perfect and can do no wrong, or that some problems only happen with other people's kids. But here's something you probably already know deep down inside: your kid is going to do some of those things too. After all, children are designed to explore and find out what life is about. Count on it. At some point an issue about Internet content will come up and, as parents, it's our job to guide them.

With this in mind, I want to take a look at what's happening, and at some of the tools that are available today that might assist you.

First off, be aware that there are different government regulations and industry self-regulations to help keep children safe. These can vary greatly, and they all depend on where you live and where you're accessing the Internet. For the purpose of helping you I am going to take the view that no authority is really going to do everything for you and that you are on your own.

So, let's set those regulations aside and take a closer look at what you can do. Here are the basics of the controls that you, as a parent, can put in place:

- **Time limits**
  Decide or at least agree together what you think is an acceptable amount of time your kids spend online and at what times of the day. Build in the time they will need to be doing their studies as so much of this is done online today. Gone are the days of paper and pen.
- **Filter content**
  Many companies create huge databases of websites and group them in categories of up to 60 different types, which can help you choose what you want your kids to be looking at. There are some obvious things that you do not want your kids looking at, like drugs, sex, and terrorism etc. Beyond that, there are then many categories that are subjective and that rely on some decisions about what works for you and your family. Now, with the right filtering in place, you are in control to a certain degree. There are a number of products available that can help you set this up. Look for one that has some pre-set templates or that makes recommendations based on age.
- **Blacklists and Whitelists**
  On top of filtering content by category or age, you should also look for software or settings that give you the option to exclude or include websites manually. This lets you create a blacklist of sites you don't want your kids to see, and likewise a whitelist of sites that you feel are safe and acceptable.
- **Games**
  Honestly, most kids play games on consoles so we should be filtering here too, although it can be tougher with gaming consoles. While they provide controls as to which age-related games can be played on them, parental controls don't always go into great detail with regard to the web browsing that kids can do on the latest generation of game consoles. These control settings vary from console to console, so you'll want to take a look and see what yours offers.
- **Device profile**
  As well as having a profile for your kids that states how long they can go online or what sites they can visit, you also need to look at the ability to create a report of their usage, regardless of what device they are using - whether it's the PC, the phone or tablet.
- **Reports and alerts**
  These will help you know what kind of online activity is going on, which can help you make decisions about adding or subtracting rules or when it might be time to check.
- **Keywords**
  Some parental controls allow you to block certain words from being searched. These controls are usually intelligent enough to leave the false positives alone, like "Sussex" for example, even though Sussex contains the word "sex" incidentally within it. Just so you know, Sussex is a county in New Jersey, as well as being a county in the UK.

- **Chat/IM**
  Many kids love to chat, so there should be a tool in the package to allow you to monitor their use of instant messages and the conversations your kids have. Additionally, it should have the intelligence to help you block your phone number, email addresses or any personal data from being exchanged.
- **Application installation and usage**
  This parental control will help you set what can and can't be installed on your computers and devices. This is a really essential item. There is no point blocking something if the kids can install something else that allows them to do the very thing you are blocking.

When making a decision on which product you want to go with, also consider that you should have a layered approach. No single solution will do everything you need it to. A layered approach might look like this: a whole home filter for the Internet connection in general, plus something else that will allow you to create profiles for your kids and the devices that they use. Remember that kids are smart and many will find loopholes or push a few boundaries.

Heck, you've probably been thinking that as you read this, and you're right. Parental control software should not be seen as a solution that fixes everything. It's a tool that allows you to be informed and make decisions based on having good information. However, accept the fact that this information will never be absolutely complete. You can't monitor every device they'll use or come across. The best advice is to talk to your kids. Your point of view and your values count. While you and your kids won't always exactly see eye-to-eye, you should be very clear about what the rules and consequences are when it comes to technology - just as you're clear about them in everything else. Let them know that your rules about content and usage apply to any device they use - not just the ones in your household.

Typical parental control software – an example

When you put it all together, what does a typical piece of parental control software look like? As I work for AVG, I humbly assume you will indulge me in using an AVG product as an example. There are many solutions out there, so you should certainly look at a few on your own before you decide. For the purposes of seeing what this software looks like in real life, let's explore the major features of AVG Family Safety.

- **Protect your children** when using an iPhone, iPad, iPod Touch or a Windows Phone mobile device.
- **AVG Family Safety® uses key-stroke technology to monitor your child's activities in chat-rooms and on social networking sites.** If it spots words, phrases, or language that is known to be used to victimize children online, it will notify you immediately via SMS or email.
- **Create unique logins and accounts for every child and enable Block, Warn, or Monitor modes according to their age and maturity.** Adjust them over time as your household's use

of the Internet and its understanding of Internet threats increase.

- **Take steps to protect your children from inappropriate material.** Enable 58 categories of protection spanning over 60 million websites.
- **Know what your children are looking for by monitoring searches on popular engines like Google, Yahoo! and Bing.** Help keep them from being exposed to questionable words, terms, and phrases by filtering their search terms.
- **Take steps to protect your child by filtering objectionable material from over 80 social networks** like Facebook, restricting access to chat rooms and functions, and monitoring instant messages and social network threads.
- **Make sure your children aren't spending too much time online** by setting specific time frames or limiting their Internet access.
- **Restrict questionable software** by monitoring inappropriate applications and blocking PC games with mature themes.
- **Keep aware of your children's online activity**. Organize detailed, easy-to-read text and email reports, staying informed of their searches, posts and downloads. That way you'll learn if questionable sites are being accessed intentionally or visited by mistake.
- **Protect your child remotely** by controlling group or individual content from any web-enabled device. Stay informed of their online activities by receiving detailed reports on your cell phone or work PC.

As you can see from the standard product description above, the majority of the elements you may require are right there in a parental control product. Reviewing descriptions like this and making a tick box selection is a good start. Also good to know is that many products can be tested on a trial basis prior to purchase.

Setting up a monitored network – another real-world example:

Let's look at my own household to see what's being monitored and how it's getting reported. It starts at the connection point, which in my case is an Internet connection that is provided by my cable provider. As we talked about in Chapter 3, you probably have a router of some sort.

In my case, the router is a box that provides a combined connection for my telephone, Internet, and cable TV. It's one of those "bundle" packages that many cable companies offer. Before this I had my own dedicated Internet router that I controlled. Either way, both cases are the same. I just wanted to point out there are different types of connections. My cable provider offers an option for parental control of the Internet through traditional filtering software. However, because I work for AVG, you can guess I use the AVG Family Safety product instead.

The first step for me is to enable "whole home filtering," which means that all the devices that connect to my router for Internet access will have a level of filtering on them. This applies equally to everyone, whether an adult, child, or even a guest in my home—hence the use of the phrase “whole home.”

All the devices that connect to my router for Internet access will have a level of filtering on them.

Based on this, I keep these settings pretty broad rather than getting too specific and locking too many individual things down. So, from the roughly 60 different categories of website that I can filter here, I use this whole home approach to take out the categories that no one in the house needs to see; malware, pornography, plus proxies and anonymizers. These are used to circumvent parental controls and filtering, so are good ones to block too. I think we all have different opinions on what these broad settings should look like, so here you should make this decision based on the general rules of your household.

Next, we have a general filter installed that lets us look at how we filter specific devices, like different PCs and tablets and so on. Here I’ll start with the household PCs where we can configure profiles for the different devices and different family members who use them. This is very straightforward. Using the Windows user system on my PC - typically found in Start > Control Panel > User Accounts - I start by adding user accounts for each family member. This lets me take the next step, which is to configure each one in the Family Safety system. Here I control which devices can be used by which family members, all based on those accounts I just created. Plus it lets me individually adjust the content that each person can see and how long they can spend online. You can get as detailed as you want with these settings, and you can even choose to monitor some categories rather than block them outright. Examples of this are social media sites or instant messenger applications, even search engines. You don’t want to preclude their use outright, but you will want to keep an eye on them.

Ok, that was quite a bit of information, so let’s pause a moment to recap.

So far, we’ve set some broad filtering that applies to any person who uses the network at home. Then, we created user profiles for each person in the house. After that, I applied some basic rules for each person on each device - rules around what they can look for, how long, what apps are blocked, and which ones are monitored. So, basically, we started broad and then fine-tuned it for each person as we saw fit.

Now that I have all these policies in place, it’s time to set up some reporting mechanisms. Here I determine the reports and alerts that I get sent to me, such as when someone is trying to access a certain type of site or just a general report of activity. I have to admit I do nothing with general reports, as I take an interest in handling this through conversation. Because my son is a teenager I think the boundaries are much wider, so that’s how I choose to handle it. However, with younger children I would suggest a weekly report that gives you some high level statistics.

What's great is that I can also deploy this setup to our phones as needed. This is a bit trickier, though. It requires you to install an app that controls browsing and links to your parental control software. When selecting something to monitor phones like this it's important to select a solution that works on any Wi-Fi and through the phone network. In the case of the AVG software it does. Now I can go through these steps for all of my devices . . . remembering that I have the whole home filter that works as a backstop, I can then adjust each device to enhance the monitoring and filtering as needed.

While this setup covers a lot of stuff, it doesn't cover everything. Take movies for example. The good news is that your cable or satellite service will give you the ability to switch on parental controls too. This helps restrict programs that are deemed for adults. This works for services that stream TV content over the Internet too, such as Netflix. These services offer profiles that protect your kids from age-inappropriate content and that keep the parents' movie queue hidden from view.

Then there's the human touch. As you've seen so far, I'm a big fan of that! No technology can do it all - nor should it. We have a great system in our house for movies that I think would work for most families.

One thing I've noticed is that as time goes by, so do the boundaries of what's acceptable. Take a movie that was given a "R" (Restricted) rating in the U.S. system in 1980 and you might find that if it was reviewed today it would probably get a PG-13 rating (Parental Guidance Age 13). We use the Internet Movie Database (IMDB) app or a movie review website to check out the parental advice information.

These typically go into great detail about use of language, violence, and sexual content. Give it a try. You may find that some of those older movies are acceptable. Just a funny note here, we may watch something with a few bad words in it and the IMDB app will tell you how many to expect. My family sits there and counts them when watching to see if they got them all!

Games consoles are next on my list. So what are the options there? Well, like a lot of computers, you can configure individual user profiles on the system that restrict the types of games that can be played by the user profiles that are signed in. You'll see this on systems like the Xbox or PlayStation, and you'll also see that video games follow a rating system similar to those used for movies. When combined, these add up to another great parental control that can keep things age-appropriate for your kids.

As for some of the other devices in your home, like the cameras and devices mentioned in Chapter 2, you'll want to take a look at each one and see what solutions are built in.

Many devices allow direct posting to the Internet, so my earlier advice of "get to know your device" still holds true here. Check out the parental controls, or at least understand what it can do so that you can treat it accordingly.

In a nutshell

I think that covers most of what's in my house. Now I feel like I need to get rid of some of the tech we have sitting in here - we have too much!

Hopefully this gives you a good overview of how all of this can work in the real world. Now, no matter how you decide to do this yourself, there's one thing you should bear in mind: let your kids know what's being monitored and in what way. We don't want our kids to feel like they're being stalked, we want them to feel like they're being held to a reasonable set of rules - and protected in the process.

This has to happen above the board. No secrets. You wouldn't rifle through their room and start poring over their diary, would you? Only if there's a dire emergency or horrible set of circumstances, right? The same is true for the Internet. Strike your balance of monitoring and control, temper it based on their age and behavior as needed, but always communicate beforehand what you're doing.

Chapter 7

Cyberbullying

At times we all need help. When it comes to keeping our families safe online, there should be no embarrassment whatsoever if a situation comes up where you need to turn to a professional or a trusted organization for help. These people are experts. They will not judge your uncertainty or lack of knowledge. They will simply be keen to help.

I think this is highly important to say right up front, because we're going to take a look at a very serious topic that's been getting a lot of attention: cyberbullying. This is any kind of harassment or bullying behavior that occurs online. Typically, like most bullying, you'll know it when you see it. It can take the form of malicious rumors circulating in email or on social media sites; it could be a page on a site that's designed to host hurtful messages about a person; it could be flat-out sexual harassment. It can take the form of images, text messages, or threats made in chats during an online game. In all cases, they hurt the recipient, whether directly or by encouraging scorn from others. Again, you will know it the moment you see it.

As I write this, there is an article on the BBC website detailing a survey in the UK by the National Society for the Prevention of Cruelty to Children (NSPCC) that found 1 in 5 children who use social networking sites suffered a negative experience in 2012. Their definition of the term cyberbullying included bullying, unwanted sexual messages, cyberstalking, and feeling pressure to look a certain way. Most of the experiences seemed to center on an online bullying tactic called trolling, which involves insulting or intimidating others, usually under a false identity, to provoke a reaction. This is a timely article, as I'm sure you've seen enough recent headlines about just how terrible cyberbullying can get - even to the point where the bullied child takes his or her own life in the face of such torment. It's concerning that a child can be made to feel so isolated, so helpless and so alone that they resort to this final step. I hope that this book and the advice in it makes us all more aware of all aspects of cyberbullying, in all its forms, whether it happens in passing or if it's more extreme, so that we can protect our children. That goes for their digital lives and the way their digital lives cast ripples into their personal lives as well. As I've said before, the two are now innately intertwined. We must be engaged and ever present.

Cyberbullying: This is any kind of harassment or bullying behavior that occurs online.

Bullying is not a new topic and has been around since the dawn of time, whether picking on someone because they can't kick a ball straight, because of the color of their hair, their weight, their race or just because they are less confident. Unfortunately, children can be very cruel and much of this I think is due to a lack of understanding of the consequences of their actions and how it makes the other person actually feel.

Name-calling can now be done anonymously and very publicly through an online account. It is also much harder to address because it's hard to identify a go-to person for recourse. If your child is bullied in the schoolyard and you address it with the school, then maybe someone gets suspended. It's harder online as it happens virtually and can be done while hiding behind a false identity.

Where do you turn? We're going to talk about that as part of this chapter, but right away I will add that many schools today have cyberbullying policies in effect. Schools are becoming an immediate go-to place to address cyberbullying among students, even if it does not actually happen on their premises. If you don't know where to start, you should always put your child's school right at the top of the list.

If you suspect your child is being cyberbullied, there are some practical steps to take. Right off the bat, take it seriously and act. That's the first piece of advice for anyone. We must not let it fester and become a much larger problem. Know that cyberbullying can be as simple as an email or text - it doesn't have to come from a gang of kids or have to build up over time to qualify. It can be a single, hurtful act. If your child is being bullied and feels threatened or hurt, it qualifies.

If you actually fear for your child's safety, don't hesitate to call the police. You'll know right away if it's that serious. Act on it. Take a proactive stance, have a conversation about cyberbullying. What it is, what it looks like. Let them know the signs and let them know that they should act.

Likewise, if you think your child is the one doing the bullying, take it seriously and act. Know those signs too. Is your child creating unflattering images of others? Is your child posting on a social network page that's exclusionary, hurtful, or just downright mean? Your child may not even understand it or be fully aware of it, but that's bullying - and someone out there is the victim. Put an end to it, just as if it was your child on the receiving end. It's that serious.

This all requires a tremendous amount of responsibility on our part, which is a theme you've seen many times throughout this book. It's up to you to take an active interest in their online activities, whether by being friends with them on a social media site or just by asking them about what they are doing. Because "it takes a village" to raise a child, we need to keep an eye out for other children too. In so many ways, stamping out cyberbullying is up to all of us, collectively as parents.

As for knowing some of the warning signs that your child is being cyberbullied, yes, that can get a bit tricky. What you want to do is keep an eye out on moods, any worrying signals that something is wrong.

Sure, that sounds like it could apply to most teens, but what you're specifically looking for are those moods or changes in typical behavior that simply don't feel right on a gut level. That's your cue to really step in and find out what's going on. Having an open communication line already in place so that your child can talk to you without feeling pressured for information is another great step in the right direction. When we do uncover a problem, as a parent the temptation is to find out right there and then what happened.

Resist the urge to interrogate. Sometimes a family friend or relative is in a better spot to be the go-to person, so don't feel hurt if your child talks to others before he or she talks to you. Embrace it, as your child just might feel more comfortable and give up more information to someone other than you, at least initially. From there you can step in.

If you do indeed spot a case of cyberbullying, be sure to do the following: document the bullying. This is vitally important.

Get screen captures of the bullying text, image, or site. Save the emails. Create a record of evidence. Even better, train your child to do the same in the moment when he or she feels like there's bullying going on. Have your child share it with you, or that trusted adult we just talked about. Help the child understand that one of the first steps he or she should take is making sure that others are aware of the problem, that capturing evidence can help determine just how serious the bullying is - and what needs to be done about it right away.
In the meantime, help your kid recognize that many bullies thrive on getting a rise out of their victims. They want to know that they hurt the victim. They want the child to respond so they can then take the reaction and twist it to create further hurt.

Let your children know this, and see to it that they resist the urge to respond to the attack. It can only make matters worse. Plus, depending on how your child chooses to respond, that response can paint your child in an ugly light as well - even if he or she was not the instigator.

As part of documenting the evidence, don't be afraid to seek out professional help through a teacher, doctor, school counselor, or even a police officer. There are also many external organizations that can assist you. They have professional help at hand and will give you good advice on your specific case.

This is also so important. While I can give you general advice on what to do, every case of cyberbullying is unique. There's a specific context, culture and situation at work that requires a tailored solution and counsel. They may even offer the opportunity to advise your kids directly. Sometimes that's what it takes - there are no blanket answers here.

Where to turn

Websites such as social networks give you the ability to report incorrect behavior. Get to know the tools that they have available and don't hesitate to use them if the situation demands. Additionally, there are numerous organizations in every country that can help.

Here's a brief list of organizations that I would recommend for more information, and also assistance if needed:

StopBullying.gov

www.stopbullying.gov
A website managed by the U.S. Federal Government, StopBullying.gov provides information from various government agencies on what bullying is, what cyberbullying is, who is at risk, and how you can prevent and respond to bullying.

Common Sense Media

www.commonsensemedia.org
Common Sense Media is a San Francisco-based non-profit organization that advocates on child and family issues. They also study the effects that media and technology have on young users.

ChildNet International

www.childnet.com
ChildNet's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children.

NSPCC

(National Society for the Prevention of Cruelty to Children)
www.nspcc.org.uk
The NSPCC was founded in 1884 and their vision is to end cruelty to children in the UK. Naturally, this extends to their digital lives as well.

Another way you and your child can take control – removing negative content

My wife has been looking over my shoulder from time to time as I've been writing this book and she just asked a great question: how do you remove comments or content that you don't want to appear on the Internet? You can see why she asked that because it absolutely applies to the subject, so let's take a closer look.

We've already talked about the fact that we should assume that our online content never disappears, and that we should make sure that our privacy settings are fully understood when joining and posting content on the Internet.

But what do we do about content that we don't want appearing, whether in a search engine or in a social network? What if there's an instance of clear and present cyberbullying that you'd like to see removed? There are two different solutions here, one for search engines and one for social networks.

Search engines scan websites for content through a combination of complex mathematics and code. From there, they serve snippets of content in search results based on what someone is searching for. This means that you need to address the problem of a nasty search result at the root i.e. the website where the offending content is posted.

Depending on the site, you can contact the website owner and ask them to remove the personal or identifiable information that has been posted about your child. Most responsible site owners will do this. Now, once the content is deleted or corrected, you can submit a removal request to the search engine, which means that they will scan the site or web page in question once again, which will make the offending content disappear from the search result.

So what about the procedures for removing offending content from other popular websites?

Let's take a look at a few of the major players:

- **Facebook**
  If someone has posted inappropriate content, created a group or page about your child, or you feel that you spotted some content that's generally not appropriate you can report this to Facebook using the "Report this Post/ Page or Group," which is shown as a link under each post or page. You can even report a person if you feel they are fake, and at a minimum you can block them from connecting with your account. Educate your kids on this feature!
- **Twitter**
  If someone has posted something inappropriate on Twitter, you can report it by visiting the Twitter Help Center (http://support.twitter.com/) and filing a support ticket.
- **YouTube**
  Here you can make a report to YouTube by selecting the "Flag" button under the video in question and selecting the reason. Note: you may need an account to make a report.
- **In general**
  Most websites want to comply with the wishes of users, especially in the case of content about children. Never hesitate to contact them - dig around on the site and find a button, an email, or even a phone number where you can make a report. Plus, let's not forget about the direct approach here too: contacting the person who posted it. In clear and even tones, see if they'll remove it. Sometimes, this is all it takes - but certainly don't rely on that alone. After all, you're possibly dealing with a bully and should set your expectations accordingly . . .

In a nutshell

Remember that the Internet is a fun place overall, and even while we address some of the serious issues and concerns that come along with it, we want our kids to see the Internet as a good place.

To be very candid, it's easy to get caught up in some of the headlines - those high-profile cases of cyberbullying where something absolutely tragic occurs as a result. It's important to be aware of what's happening out there, but it's also vital to keep our perspective in check. These are extreme cases of cyberbullying, hence the headlines, and we should remind ourselves that cyberbullying doesn't have to make the headlines to hurt and have lasting effects. It can take more subtle forms that are still tremendously painful for a child. We need to be vigilant, and we need to nip it in the bud when we spot it.

As with so many things we've talked about in these pages, trust your gut and act on it. Keep an even keel when it happens, and then do what's right for your child.

Conclusion

The big things to keep in mind

We've covered a lot of ground, haven't we?

I really hope you've found the information helpful, along with the look at how I manage technology in my own family life. Of course, this short book is not designed to be the end-all-be-all of advice, but rather a thought-provoking set of guidelines that you can take and build upon.

My feeling is that if parents understand the basic risks and some of the ways to address them, then the next steps should be that much simpler to take. Making sense of how to manage technology and teens all starts with a foundation of good information, and then your own internal compass will guide you from there.

For me it all boils down to a couple of important points.

The first is that we need to teach our kids to communicate online in the appropriate way, just as we teach them to communicate appropriately in general. Their ability to show empathy, understanding and to think a situation through will have a profound influence on their future.

The second is that we need to learn how to strike a balance in our lives - and this is a lesson we're all learning, parents and kids alike. The University of Michigan released a study that shows solitary use of a social network may decrease a person's feeling of wellbeing.

I'm not sure that this is news to anyone, or if it just confirms what we could have already guessed. Either way, it highlights we need balance in life, particularly in the ways we communicate. As human beings, we're wired to interact. To support each other. To befriend each other. To simply hang out. So much of that simply has to happen in person. It's in our nature.

So, if there's an absolute shortlist of the things I hope you take away from this book, it'd look something like this:

- **Keep the conversation going.**
  Talk with your kids and share in their online activity as you can. Be part of it.
- **Implement "The Basket".**
  Remember The Basket from Chapter 4? Meal time and after 9pm should be Free Family Time, which means free from phones and other mobile devices. Try it and see the difference it makes - for everyone.
- **Lead by example.**
  Yep, that means putting down your technology too, and doing other things like watching your own behavior on social networks, thinking twice before firing off that angry email, or simply getting smarter about the security settings on all your family's devices.

What's next for managing the technology in the Anscombe household? That's a good question. Right now my teenage son is mobile with his smartphone, and I'm sure some issue or other is bound to come up with that soon enough.

My prediction is that we will enter the social network scene and have to do some education around acceptable behavior. In general, I expect my son to continue enjoying the Internet under my guidance, and in doing so he'll push just about every boundary that's set out for him. If I don't see that happening, well, then I'll have reason for concern. Either it means he's not testing his parents like a teenager should or it means that he's up to something and I'm simply not seeing it. That's kids for you, right? As a parent, staying on top of that comes with the turf. Who signed us up for this job, anyway?!

The Internet is this generation's Industrial Revolution. There's no wishing it away. Embrace it and enjoy the ride. It really is pretty cool.

Glossary of terms used in SMS and texts

:-)

:-7 Smirk
:-D Grinning
:-P Sticking tongue out
:') Happy and crying
:'-(Crying
:-(Sad
:-( ) Shocked
:-(o) Shouting
:-) Smiling
:-* Kiss
:-|| Angry
:-<> Surprised
:-O Wow
:-o zz Bored
:-X Big sloppy kiss
;-) Wink (Twinkle)

#

2d4 – To die for
2g4u – Too good for you
2l8 – Too late
4e – Forever
4yeo – For your eyes only
7K – Sick

A

A3 – Any time, anywhere, any place
AFAIK – As far as I know
AFK – Away from keyboard
ASAP – As soon as possible
ATB – All the best
ATK – At the keyboard
AWHFY – Are we having fun yet?

B

B4 – Before
BBL – Be back later
BBS – Be back soon
BF – Boyfriend
BFF – Best friend(s) forever
BFN/B4N – Bye for now
BGWM – Be gentle with me
BRB – Be right back
BRT – Be right there
BTW – By the way

C

Cm – Call me
CU – See you
CUIMD – See you in my dreams
CUL8R – See you later

D – F

DK – Don't know
F2T – Free to talk
FAQ – Frequently asked questions
FYEO – For your eyes only
FYI – For your information

G

GF – Girlfriend
GR8 – Great

GSOH – Good sense of humor

H – I

H8 – Hate

IDK – I don’t know

ILU – I love you

IMBL – It must be love

IMFL – I’m falling in love

IMHO – In my honest/humble opinion

IMO – In my opinion

J – K

J4F – Just for fun

JK – Just kidding

KC – Keep cool

KIT – Keep in touch

KOTC – Kiss on the cheek

KOTL – Kiss on the lips

L

L8 – Late

L8r – Later

LMAO – Laughing my a** off

LMFAO – Laughing my f*****g a** off

LOL – Laugh out loud

M, N, O, P

M8 – Mate (UK – friend)

MYOB – Mind your own business

NC – No comment

O4U – Only for you

PRW – Parents are watching

R

R – Are

ROFL – Rolling on the floor laughing

RUOK? – Are you okay?

S – T

SK8 – Skate

SWALK – Sent/sealed with a loving kiss

T2Go – Time to go

TBC – To be continued

THX – Thank you

TMI – Too much information

TTFN – Ta-ta for now!

TTYL – Talk to you later

U

U – You

U2 – You too

UR – You are

W, X, Y

W4u – Waiting for you

W8 – Wait

WRT – With respect to

WTF – What the f***?

WUWH – Wish you were here

X – Kiss

Yt? – You there?

YOLO – You only live once

Glossary of tech terms

A

Antivirus – Software that removes or blocks malicious programs which attack your computer.

App – Short for application; commonly associated with app stores where applications can be downloaded for mobile or tablet devices.

ATM – Automated Teller Machine, provided by a bank or financial services company; called a "cash point" in some countries.

B – C

Blog – Short for "web log" where an individual or organization regularly publishes articles, typically about a specific topic. For example, I have a blog on consumer and family security here: https://blogs.avg.com/author/tony-anscombe

Bundle Packages – Groupings of computer software or services that are meant to complement each other. Examples include when a new computer comes "bundled" with an operating system and office software, or when a cable company offers to "bundle" TV, Internet, and phone service.

Chat – A one-on-one or group-based conversation that's held online in real-time; usually uses text, but applications like Snapchat offer the ability to do so using pictures.

Chat Room – A group of people engaged in an online conversation on a specific topic or area of interest.

(the) Cloud – The means of storing information or providing a service that is not saved locally on your machine. For example, email can be cloud-based - you have no idea where your email is being stored, but you can access it from any machine, via a web browser that is connected to the Internet.

Code – Put simply, a sequence of instructions written in a computer programming language. It's used to create all sorts of things like websites, smartphone apps, computer software and much more.

Console – A word used to describe video game machines like the PlayStation, Xbox etc. Remember that these are fully Internet-connected devices.

Content Filtering – A way of controlling which websites, videos, shows or software can be viewed or used. This can be done by creating rules for a device, a user or both. Good parental control software will allow you to do this.

Cyberbullying – Bullying that takes place using technology such as cell phones, computers, and tablets; can occur through social media sites, text messages, chat, websites, blogs, emails, pictures and more.

D – E

DSL – Digital Subscriber Line, a high-speed connection to the Internet over traditional phone wires.

Email – An electronic letter to someone or a group of recipients.

Encryption – A method of keeping information safe when it's being transmitted by scrambling everything up with a unique code key.

F – G

Facebook – The world's largest social network site with 1.15 billion users as of March 2013.

Firewall – Software that controls what comes in and out of your device, like having a bouncer covering every entry to your home.

Geotagging – The act of attaching or "tagging" location information, often to pictures taken with a smartphone or camera that has GPS technology built-in. This helps you accurately locate where the picture was taken.

Google, Yahoo, and Bing – Three of the most highly-used search engines on the Internet. Each offers a service that indexes all of the content stored on the Internet and displays summaries and links to that content based on your search terms.

GPS – Short for Global Positioning System which uses satellites to pinpoint your location to a device; used for navigation applications that serve up location-specific content, and by some cameras when taking pictures (see "Geotagging," above).

H

Hacking – The act of breaking into a computer or a computer network by sidestepping or removing security measures.

HotSpot – A wireless access point to a network or the Internet, typically used to describe a public Wi-Fi service such as at an airport or coffee shop; some public hotspots are free, others may charge for service. (See "Wi-Fi" for more detail).

HTTP – Short for Hypertext Transfer Protocol, which is the technical language that websites use to deliver content to your browser in a way that's pleasing to the eye.

HTTPS – Just like HTTP above, but with an "S" for security added; the data is encrypted so that no one can read it if they are between you and the service you are accessing. Think of it like a letter in an envelope instead of a letter on the back of a postcard.

I

IM – Short for Instant Message, a one-to-one message sent directly from one person to another via an application built for that purpose. It's a bit like text messaging but with an IM app you can see if the other person is online and there is no restriction on the length of the text. You can also send files through most IM systems.

IMDB – Short for Internet Movie Database, located at www.imdb.com. This is a place where movie facts and reviews are offered, along with great parental guidance.

Instagram – A photo and video-sharing service that allows users to easily filter and view content from people they follow; often combined with other social networks, such as where people use Instagram to host pictures and Facebook to share them to a broad group of friends.

Internet – A global system of connected computers - private, government, companies, and so on; allows for either public or private access to information and services. The World Wide Web (WWW) is a subset of the Internet because it uses the Internet to transport its information.

ISP – Short for Internet Service Provider, which is the company that provides you with your connection to the Internet.

M – P

Mac – A brand of Apple computer that runs its own proprietary operating system (user interface).

Malware – Short for "malicious software," a category of software including viruses that harm data or spyware that steals personal information.

Parental Controls – Software designed to allow a parent to either monitor or block access to certain content on the Internet based on a child's age or what the parent feels is appropriate.

PC – Short for Personal Computer, typically refers to a computer that runs Microsoft Windows (as opposed to a Mac, see above).

Phishing – Used to describe an attack that is designed to try to steal your information. It often involves attempts to steal your login and password to a service by tricking you into thinking that the service is requesting them for some reason. For example, you might receive an email with a link that takes you to a website which looks and feels like a bank communication but isn't, it's just a phony site created by a scammer out to steal your info. This can also occur via text messages, pop-ups, and even phone calls.

PIN – Short for Personal Identification Number, which is normally 4 digits used to unlock a phone or to make a transaction with a credit or debit card.

Pinterest – A pin-board photo-sharing service that allows you to create a board of pictures related to you or to a subject you are interested in; allows other users to re-pin your pictures too.

Post – Refers to putting something on a social network site, such as when you post a picture or quick update on your status; also refers to posting articles online.

Proxy Anonymizer – Software or a service that can hide a person's identity and activity while using the Internet. Often helpful for keeping "anonymous" when using the Internet, these can also be used by kids to work around parental controls.

R–S

Router – A device that sends and receives data on a network. A common type is the cable or DSL modem that connects a home to the Internet.

Sharenting – When a parent shares information about their children on social networks.

Skype – Software that allows you to talk, video or instant message other people using the Internet, all free of charge if it's to another Skype user. You can also Skype out to a normal phone line for a small fee.

Smartphone – A cell/mobile phone that is a fully featured, Internet-connected device; it is a bit like having a computer in your pocket.

Social Network – A network of individuals or organizations that want to share experiences or content with each other; for example, Facebook and MySpace. For younger children this can include Club Penguin, which is a moderated social network.

Spam – Unwanted digital messages that are sent in bulk, usually ads. Often associated with junk e-mail messages, it can also apply to other forms of digital communications like instant messages, texts or messages posted on Internet forums.

SSL – Short for Secure Sockets Layer (also see HTTPS, above); this is the encryption standard used to keep web pages secure.

T

Tablet – A thin device with a touch user interface that allows you to easily access information and apps; examples are the Apple iPad, Nexus (Android), Microsoft Surface.

TCP/IP – This is the method of transport the Internet uses, imagine the Internet is the highway and TCP/IP is the type of car.

Twitter – A social networking service that allows user to "micro blog" by sending messages that are 140 characters in length to followers around the world, also known as "Tweets."

Two Factor Authentication – A way of confirming your identity by using two things: one is typically "something you know" and another is "something you possess." An example of this when you use an ATM - your personal ID number (PIN) is the "something you know" and the card you use is the "something you possess."

Trolling – A slang term for posting harassing or argumentative comments meant to disrupt the conversation in an online community. Think of it as digital heckling. This can take place in a message board, a chat room, or even in a blog.

V, W, Y

Virus – A malicious piece of software designed to do damage to your computer and spread by copying itself to other places.

Wi-Fi – Wireless connection to the Internet or a network by using a radio transmission to connect devices together.

WPA/WAP – Wi-Fi networks can use encryption to make sure the information you're sending is kept safe, and these are specific standards for providing encryption on Wi-Fi.

WWW – Short for World Wide Web, which connects documents to other documents on the Internet. Think of the WWW as the content you see on the Internet and the Internet as the way that the content is transported.

YouTube – A video-sharing service, note that not all content is appropriate for everyone.

The coming of the internet is this generation's industrial revolution. It has changed everything.

However, tangled up in all the wonders that the internet provides are dangers and problematic situations that you, as a parent, will have to confront. Especially when your children are teenagers.

In this book, Tony Anscombe, father and Ambassador of Free Products for AVG Technologies, outlines his own knowledge and experiences in dealing with the myriad situations posed by the internet to parents and their teens.

Through a mix of personal anecdotes, professional experience and a caring parent's application of common sense and fairness, Tony offers a guiding hand through this moral maze.

How can parents get to grips with technology as quickly as their teens?
How is the internet affecting your teen's behavior?
How can you manage the technology in your home so that everyone is safe?
How far should a parent go in controlling what their teen can and can't do on the internet?
What do all the terms even mean?

In clear, easy-to-understand language, Tony offers parents the benefit of his expertise and experience and shows how parents can manage their teens' use of technology with security and confidence and make the most of all the web has to offer.