White Paper

# The Challenges of Digital Parenting in the Connected Home

# Contents

Author: Luana PASCU

## Summary of Top Findings

- Although 12 to 13 year-olds spend more time on tablets, smart TVs, e-book readers and smartwatches, and are more active on social media, **14 to 16 year-olds are more prone to cyberbullying and to being diagnosed with depression**.

- **57% of teenagers say looks/not conforming to society's beauty standards are a top reason for bullying**, followed by differences of opinion (44%), personality traits (30%) and fashion (27%).

- 7 out of 10 kids have **strangers** in their online friend list and **talk to about 41% on a regular basis**.

- **3 out of 10 teenagers fell victim to cyberbullying in 2017**, while 5 out 10 have friends that dealt with cyber bullying or harassment at least once.

- **Instagram (40%) is a top cyberbullying platform**, followed by Facebook (31%) and Snapchat (31%).

- If cyberbullied, **29% of teenagers wouldn't confide in their parents**, while 28% wouldn't tell anyone, 26% said talking to a friend is an option and 24% consider changing their look.

- **44%** of teenagers between 14 and 16 years of age are **concerned their data is gathered online without their consent**.

- **More than 1 million children fell victim to identity fraud in 2017, and two-thirds were under eight years old**.

## How Parents Can Live in Technical Bliss with Digital Natives

What are the **challenges of digital parenting** and how can parents live in harmony with their digital-native kids? As families grow more connected and daily life moves online, privacy and security should become top priorities in each smart home. The biggest challenge is probably faced when children are involved. They want to explore, learn new things, so they might unknowingly expose themselves, and their family, to countless risks that could be avoided simply by using parental control software. Parents can help their children explore the online world safely, not only through available software, but also by **communicating with them from an early age and building trust to educate them for a digital life**.

The online environment is constantly changing; parents have to **lead by example** when it comes to screen time. Not only do they face a number of digital challenges of their own, but they must educate themselves first before they start a dialogue with their kids. Kids born today have been labeled **"digital natives,"** users who might be oblivious to the danger and risks of online culture. They are simply absorbed by social networks and gadgets which could trigger unhealthy development that, in turn, may affect them long into adulthood.

A **Bitdefender survey** found that, compared to teenagers, **pre-teens (12 to 13 year-olds) are likely to spend far more time on tablets, smart TVs, e-book readers and smartwatches, and are more active on social networks. In spite of this, the cyberbullying incidence is higher among 14 to 16 year-olds, who are also more prone to depression if cyberbullied.**

According[1] to the American Academy of Pediatrics (AAP), parents should set some limits on media use, talk to their children about online navigation, establish clear media-free activities for **a balanced online-offline lifestyle and teach them about respectful online behavior**. The digital world can be educational and great for early learning, especially if parents take the time in advance to research the games, apps, social networks and quality of content their kids are exposed to.

Not all parents have a proper understanding of the online ecosystem or the risks their children are exposed to on a daily basis, such as **predators and cyberbullies**. This can prove a major roadblock, especially when children deal with 24/7 harassment, as some parents might not take them seriously. Many parents were bullied themselves once, but could at least feel safe in their homes. This is not the case anymore, as cyberbullying has taken the lead.

Who can get away from social media, gaming consoles or smart phones? Many people – parents and children alike – struggle with **addiction to technology,** because it has integrated with life. While the former discovered it later in life, the latter were born into it. The AAP found[2] that over **30 percent of children in the US are mobile device-savvy when still toddlers, while 75 percent of teenagers own a smartphone.** Honest, educational conversations, especially with teenagers, might help prevent risky behavior, because keeping them in the dark about the existence of tablets or Facebook, for example, will simply not help.

**As difficult as it may seem at first, parents have to accept that becoming more digital is part of natural evolution**, which makes living in tech harmony with their kids essential. Technology offers a number of benefits and opportunities for children to explore their creative side. It's also a matter of trust. Technology is addictive, this is a fact, but after an honest dialogue about how to spend their time online and how to deal with strangers online, for example, parents should trust their children can make the right decision. Teenagers are tied to computers, parents are glued to their phones, and kids often act out because they feel ignored and want attention.

Chances that children have access to inappropriate content online are high so, before they set some ground rules, they should also consider the option of enabling parental control and safety features on the gadgets they use, be friends with them on social media without invading their personal space, and oversee their activity without being aggressively intrusive.

# Online Risks and Challenges for Children

## Online Predators: Any Child Is a Target

"*People who do not believe that their children could ever become victimized online are living in an unrealistic world. Regardless of if your child makes 'As' or not, that child has the potential to become victimized through online technologies. I think it is very important for* ***parents of all socioeconomic status and with all different roles in society to take this problem very seriously***."

Melissa Morrow, Supervisory Special Agent, Child Exploitation Squad[3], FBI

The Internet's growing popularity and availability have led in recent years to **a global surge in Internet crimes against children**, according to Interpol statistics[4]. The police organization reports that "not only can offenders distribute and access child abuse material more easily, but they can also come into direct contact with children – via chatrooms and social networking sites**." Any child can become an online victim, which leaves parents wondering how to protect their children from predatory behavior without making them feel scared or stalked**.

Are parents fully aware of who their children spend time with online? As per FBI investigations[5], Internet predators are usually adults who lie about their age, pretending to be teenagers or at least close in age to their target. They spend a lot of time scanning for victims on social media, on various forums and even video game consoles. The Internet helps them stay anonymous.

By hiding behind computers and pretending they care about them, they create alter egos and give kids enough attention to lure them into meeting in person. Sometimes they request explicit information, photos and videos where kids expose themselves, which predators can later use for blackmail or to make public on social media. **Online predators can manipulate children into sharing personal information about their family, such as passwords, home address, Social Security Numbers or payment card data, for use in identity fraud.**

It's important to teach children how to recognize suspicious behavior and to always be vigilant from a young age. **In 2017, over 1 million kids fell victim to identity fraud, and two-thirds were under eight years of age**, according to Javelin Strategy & Research[6]. By stealing Social Security Numbers, or even buying them from the Dark Web for as little as $2, hackers can steal identities. They take advantage of the child's clean credit history to get new bank accounts and credit cards, sign rent contracts, get medical treatments, apply for loans, or access government social programs. The US Federal Trade Commission recommends[7] all valuable documents that contain personally identifiable information be kept in secure locations, and people should shred documents before throwing them away and check if there's a credit report in the child's name before turning 16.

### How Online Predators Operate

**Pre-teens are more vulnerable than teenagers, which makes them a top target for online predators.** Predators hiding behind computer screens will go the extra mile to draw information out of them, manipulate them into exposing themselves in photos or videos, or trick them into meeting outside the house.

**Grooming is the most pervasive technique.** Predators will stalk children for months to groom a relationship with them. Once they have gained their trust, they will act out their plan. By scanning the forums, social media or chat rooms for vulnerable kids, predators know that the perfect victim is a vulnerable, emotional victim. If the child is feeling neglected by parents, the predator will meet that need with sympathy and offer comfort, excitement or even try to buy trust with presents. Others will feel rebellious, misunderstood or depressed. No matter what they go through, a predator will manipulate their emotions to trick them.

Many young people reach out to the online community for advice or to simply talk to someone who understands their problems, and predators take advantage of this opportunity. Too many kids give away information without even being asked to and feel they are friends with people they met online, yet never in person. **"Girls aged 11 to 14 initially said they disguised their identities in chat rooms,"** found a survey conducted in Canada[8]. "They admitted, however, that it was impossible to maintain a false identity for long and eventually revealed personal information when they felt they could 'trust a person.'" This relationship-building process took between 15 minutes to a few weeks. Teenagers think they outsmart predators and detect their behavior, but they are in fact quite trusting and the online world is deceptive. While they are exploring their sexuality, for example, a predator mirroring the same emotion is waiting for the child to take risks and open up.

Predators will take their time to groom their victim and fish for valuable personal information they can later use, such as hobbies, favorite band or sport, the name of their school, information about their parents and financial situation and even Social Security number. By **fishing for information**, predators can get all the necessary details to get closer to the child and ask even more personal questions, possibly also gradually engaging in explicit conversations. In some cases, they can use the information to create other personas for future victims.

**Social network Kik has been actively used by online predators**. The app has officially been linked to over **1,100 abuse and exploitation cases investigated by 28 police forces in the UK in five years**, according[9] to the BBC. One victim in the case claims he was contacted by approximately 200 men asking for selfies and explicit photos and videos.

Surely, Twitter, Facebook, Instagram and Pinterest are well known even among adults. But where did Kik Messenger come from and what are they doing to protect the vulnerable? The company was founded in Canada in 2009, counts 300 million users and its top perks are anonymous accounts and false identities. Perfect for online predators. When the UK police reached out to the company to help identify offenders in a major case involving 90 profiles, Kik replied they would give away information about their users only in case of "imminent threat of death or serious physical injury to any person."

And Kik is not the only suspicious teen application with lurking predators. BBC writes that child predators have used Omegle as a means to share Kik usernames and move the conversation to a smartphone. A Bitdefender study found that the most dangerous online social entertainment platforms are MeetMe (41%), Omegle (37%), Yellow (31%) and Monkey (29%). These apps are used by teenagers to meet new people, arrange dates and send explicit content. Just last month, a 48-year-old man was arrested[10] for sexual exploitation of a 16 year-old girl he had been talking with on MeetMe.

**When asked what they think about dating or messaging platforms, teenagers say they are dangerous, but only 4 out of 10 understand that these websites involve risks, Bitdefender found**. The same survey found that **7 out of 10 children have strangers in their online friend list and engage in conversations with them**. On average, **teenagers chat with about 41% of strangers in their online friend list**. About **44% of teenagers between 14 and 16 years old think online networks pose a very high risk of gathering data without their consent**. 44% of teenagers fear their identity could be stolen online, while 41% fear someone could hack their smart devices to spy on them and 40% fear an intruder will take over their devices and demand ransom to release the data.

Companies developing social networks and messaging apps should be able to detect suspicious activity and not put children at risk. However, until this happens, safety awareness for pre-teens and teens is critical.

## Measures Parents Can Take to Prevent Predatory Behavior

- Parents should **take any suspicious behavior seriously** because children are more **likely to open up to strangers**, especially if they are led to believe they are speaking with someone their own age, struggling with similar life experiences.

- Ideally, children should learn how to **make smart decisions online from an early age** and learn that anything they publish will be part of their **digital footprint** forever. Because it is part of their identity, children have to understand the dangers of online predators, personal accountability and the importance of data privacy.

- Do they know that **social media profiles should be set to "private"**? If not, all of their photos, thoughts posted and simply any information shared will be public for anyone to see and use against them. **Privacy settings must be turned on** for all social networks, online gaming and chat rooms to keep predators from contacting them.

- Explain to children how sharing personal identifiable information such as birthdates, Social Security numbers online or any family-related information could make them **a target for identity theft**.

- Explain to them why they should be **suspicious of people asking them to send explicit photos or videos via email or social media**. Give examples of real-life scenarios involving sex offenders, how to detect them and teach kids that inappropriate content shared online can't be removed completely.

- Teach kids how to be **digitally savvy** and **skeptical about any offers that sound too good to be true**, suspicious emails, links or texts from people they don't know in person, social media profiles that mirror their emotions to build trust.

- Have an honest and direct **talk to kids about messaging apps** such as WhatsApp and Kik, but also research the web for other suspicious apps or social networks that may appeal to youngsters.

- Check **online store settings** and keep a close eye on **in-game purchases**.

## Cyberbullying: Warning Signs and Influence into Adulthood

A group of boys are beating each other up during recess, two girls constantly refuse to let the third sit next to them at lunch, while another kid is perpetually humiliated or insulted in the classroom or hallway. Each victim feels rejected and afraid but hopes the bullying will end once they leave school. Maybe this was the case in the past, but bullying has now made its way online. Every day, there's a child out there who deals with social exclusion, threats and humiliation online, because the bully wants to feel empowered by picking on someone they think is weaker.

**In 2016, 1.5 million teens in the UK were cyberbullied, but they were afraid and even embarrassed to open up to a parent or counselor**, according to an anti-bullying organization from the UK[11]. The situation hasn't improved. Cyberbullying is learned, incessant abuse that takes place online. This means that children who deal with physical abuse offline don't feel safe anywhere, not even in their homes, because the harassment continues online. Pre-teens and teens are digital natives, they are excited about everything that involves technology and staying connected; no wonder they are permanently on social media. But there are no rules online – anyone can post content, any adult can pretend to be a teenager looking for friends and any bully can hide behind a profile to torment someone weaker.

With internet access widely available on smartphones and computers, it's not much of an effort for an abuser to take to social media, spread death threats and hate emails, or expose a victim's private photos and videos online. Cyberbullying affects teenagers worldwide; it's not restricted to a certain region. Parents, school districts and law enforcement play a critical role in fighting cyberbullying and its devastating effects on children.

### Top Warning Signs Something Is Wrong

The trouble with most parents is that they can't figure out whether their child is really dealing with a bully or it's simply some mean argument kids might have. It's crucial for parents to constantly talk to their kids about what goes on at school and online, if there is anything or anyone bothering them. It's best to be direct and ask them bluntly. In most cases, teenagers keep to themselves and rarely open up to adults, whether they are parents, guardians or school counsellors. Children who are bullied feel ashamed and wrongly believe that they deserve it, which is why they often display certain behavioral patterns.

Here are some **common warning signs** something is wrong:

- ✓ All of a sudden, the child is covered in **bruises**, appears very **stressed** and has **anxiety** attacks when school or school-related events are mentioned.
- ✓ Sudden **weight loss or gain**, **muscle pain**, **nightmares** and **pessimism**.
- ✓ School is becoming a problem – the child is either **dropping in grades** or **refuses to leave the bedroom**.
- ✓ The child starts wearing **long sleeves**, even in extreme heat. This may be a sign of **suicidal behavior** which means measures must be taken immediately to understand what is happening and how to help overcome this coping mechanism.
- ✓ Activities that used to be fun, such as sports, hanging out with friends or video games, are no longer of interest. In fact, the child suddenly **avoids gadgets and refuses to socialize**.
- ✓ The child has become **withdrawn**, with **low self-esteem**, shows signs of **depression** and has **mood swings**.
- ✓ The child's mood suddenly changes after certain calls, texts or social media content, and shows **little interest in fun activities**.

## The Broad Impact of Cyberbullying on Psychological Health

A Bitdefender survey of US-based children aged 12 to 16 years old found **that 3 out of 10 teenagers were cyberbullied or harassed in 2017, while 5 out of 10 have friends that have dealt with cyber bullying or harassment at least once**. **The most frequent platform for cyberbullying is Instagram (40%), followed by Facebook (31%) and Snapchat (31%).**

**The United States deals with 123 suicides daily, with a suicide rate of 13.15 for 15 to 24 year olds in 2016. It has become the "tenth leading cause of death in the US,"** according to the American Foundation for Suicide Prevention[12]. Cyberbullying contributes greatly to these statistics. Another study from Swansea University Medical School[13] found that children who were threatened, humiliated or intimidated online are more prone to self-harm and suicidal behavior. YouthTruth, a nonprofit from the US, found[14] that **looks, ethnic background and sexual orientation are the most common reasons for bullying at majority-white schools**. **Religion** and **gender** are also common reasons for cyberbullying, with **girls targeted more than boys, and non-white more often than white.**

Each social network is approached differently, depending on the reasons for bullying. For example, Bitdefender found that **Instagram is more popular when criticizing one's looks**. Overall, pre-teens said that **MeetMe is the most dangerous platform, but most bullying was experienced on Facebook, Live.ly, WhatsApp and Pinterest**. Bitdefender found Snapchat is more popular with 14 to 16 year-olds, who perceive **Omegle as the most dangerous online platform**. In spite of this, they said **most cyberbullying was experienced on Kik Messenger**. When it comes to online risks, teenagers are more aware and believe smart devices pose a very high risk of data theft.

**57% of respondents complained that looks/not abiding by society's beauty standards are a top reason for bullying, followed by differences of opinion (44%), personality traits (30%) and fashion style (27%). After they were bullied, children said they felt diffident/ insecure (45%), sad (45%), depressed (40%) and strange/odd (35%**).

**Pre-teens (12 to 13 year olds) are more likely to turn to their parents and teachers if dealing with cyberbullying, while children between 14 and 16 years old would rather keep to themselves**. 29% of teenagers wouldn't speak with their parents about their problems, while 28% wouldn't tell anyone, 26% said talking to a friend is an option and 24% consider changing their appearance.

**Only 5 out of 10 teenagers spoke with their parents about online bullying**. Even before they get social network profiles, parents should talk to their children about online risks such as cyberbullying and predators.

Victims of cyberbullying who refuse to bring it to the attention of their parents, school or law enforcement develop unhealthy coping mechanisms, with destructive effects on their future development. **If neglected, cyberbullying can lead to self-harm, drug abuse, suicidal thoughts and dropping out of school**. Children who are abused are more likely to develop psychological trauma that they carry with them into adulthood. While cyberbullying victims are at a greater risk for suicide, some become bullies themselves as a coping mechanism, believing they are entitled to hurt others as revenge for what they suffered.

Nothing is more important than psychological health so, if someone is a victim or witness to cyberbullying, they should know it's important to document all abuse tactics and report it to the school district and law enforcement. Cyberbullying victims must immediately receive psychological counselling and be removed from the toxic environment that's hurting them.

**Bitdefender conducted in-depth interviews with a number of pre-teens and teens living in the US about their online experience. Below are some of their statements regarding their personal experience with cyberbullying:**

> *"**Instagram** has a lot of **offensive accounts**, but it is easy to filter them. **Facebook** has loads of funny videos, but there's also **lots of false information and political fights**. There's people on **Instagram** who will **harass girls for nudes**. **8/10 times it's a person you know**. On **Snapchat** pretty much anyone can add you and because pictures disappear. **Lots of people send nudes**."* (Girl, 15)

> *"I feel as if **Instagram is more dangerous** of a platform because you can share things about yourself or others that can **ruin someone's self-esteem or cause jealousy and bullying**."* (Girl, 15)

> *"**I am insecure because I would look at society's standards of beauty and compare myself to them realizing I can't change.** Online bullying makes me sick because being able to bully someone through a screen let alone at all should not happen. Judging someone based on their looks or views is just wrong."* (Girl, 15)

> *"At first I tried to ignore it but soon it became bothering to me and **made me go into a state of depression**."* (Girl, 16)

> *"I feel like people typically **target others with different beliefs.** This causes **sadness and loneliness.**"* (Girl, 15)

# How Bitdefender Parental Control Helps Reduce Online Risks

There is no way to get rid of smart devices. Living in a digital home is the new normal, and everyone is encouraged to be more and more connected, to have an online presence. Technology has always been attractive to youngsters. While in the past people were consumed with television, the first cell phone, game consoles and the original personal computer, it is now time for their kids to get excited about smart watches, smart fitness bracelets and social networks. Who knows what will follow? Technology is addictive, which means kids won't put down their phones any time soon. This brings up a number of concerns for parents, such as the impact these gadgets have on their children's behavior, personality and social skills. And a more pressing matter: **how will they fight back against online predators and cyberbullying?**

If parents want their children to instantly flag inappropriate content and behavior online, they have to be part of their tech experience and online adventure. By showing them what is age-appropriate and how they can make smart decisions online, they can trust them to make smarter decisions when making friends online, playing videogames or about letting strangers into their home.

Because it's natural for parents to be wary of the unknown, especially of completely new worlds, they can reach out to a number of **software tools** to ease their mind. They can, for example, **activate parental control features on the gadgets their children use**. In that way, they are informed where the children are, about their internet activity, predatory behavior and cyberbullying-related content.

**Bitdefender Parental Control is a breakthrough detection filter that helps parents manage their children's online experience without making them feel under surveillance.** Parents receive a detailed report about their children's browsing history, how much time the child spends surfing the web and on each smart device, and who they speak with on the phone or via text. The tool detects verbal attacks, and inappropriate content requests for photos or videos or attempts to lure the child into meeting outside the house, give away credit card or Social Security numbers, or engage in inappropriate activities. Interaction with sexual predators should always be a top concern, and both parents and children should be vigilant.

**Bitdefender Parental Control also detects repeated, aggressive behavior and language with intent to harm a child that results in an imbalance of power in cyberbullying cases.** It analyzes conversations that take place on messaging platforms and social media interactions, but also addresses bystanders. Bitdefender Parental Control doesn't in any way expose the child's or parents' privacy, as it doesn't expose conversation excerpts or snapshots. The tool sends clear warnings to make digital parenting easier, making room for more heart-to-heart conversations and family time.

# References

1. American Academy of Pediatrics. *Growing Up Digital: Media Research Symposium.* October 1, 2015 PDF

2. Ceder, Jill LMSW, JD. *AAP's Guidelines for Screentime for Kids*. Verywellfamily.com. May 30, 2017 Web

3. Internet Safety 101, Web

4. INTERPOL, Web

5. FBI. *About Protecting Your Kids.* Web

6. Weisbaum, Herb. *More than 1 million children were victims of ID theft last year.* NBC News. June 21, 2018 Web

7. Federal Trade Commission. Consumer Information. *Child Identity Theft* Web

8. Sexual Assault Support Centre of Waterloo Region. Internet Safety-Tips for Parents Web / Originally published at http://www.bewebaware.ca/english/OnlinePredators.aspx

9. Crawford, Angus. *Kik chat app 'involved in 1,100 child abuse cases'*. BBC. September 21, 2018 Web

10. Gebregiorgis, Senait. Parents with teenagers warned of risks involved with 'MeetMe' mobile app. FOX Illinois. November 20, 2018 Web

11. DitchtheLabel.org. *The Annual Bullying Survey 2017*. Registered charity number 1156329. July 2017 PDF

12. American Foundation for Suicide Prevention. *Suicide Statistics*. Web

13. Ann, John, FFPH et al. Swansea University Medical School. *Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review*. JMIR Publications. Published on 19.04.18 in Vol 20, No 4 (2018): April Web

14. McClellan, Jennifer. One third of middle- and high-schoolers were bullied last year, study shows. USA Today. September 24, 2018 Web

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

All Rights Reserved. © 2018 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners. FOR MORE INFORMATION VISIT: enterprise.bitdefender.com.