11 DIGITAL DANGERS HIDING IN PLAIN SIGHT

HOW SOME OF YOUR CHILD'S FAVORITE SITES COULD BE THE MOST DANGEROUS ON THE INTERNET

A publication by uKnow.com

TABLE OF CONTENTS

INTRODUCTION

INTERNET DANGERS

The world of the Internet can be a scary one for parents, particularly if you're not an avid Internet user or don't own all of the latest tech devices. Internet-savvy kids can easily undermine the monitoring efforts of their parents, and the web gives kids access to a host of information that was previously unavailable. It also gives them a broad variety of opportunities to share information about themselves and to gain information about others. While this can enable kids to learn, to keep in touch with friends, and to find new hobbies, it can also expose them to dangers such as cyberbullying, damage to their reputations, and exposure to Internet predators.

Because new sites are developed each day, it's impossible to keep an exhaustive list of every potential danger. Rather than focus on specific sites, it's wise for parents to take a holistic approach that includes open communication and regularly checking up on your child. Commonsense safety measures can also help keep your child safe. Some key steps to take to protect your child when she's using the Internet include:

- Putting the computer in a public location so that you can easily see what your child's doing online.
- Becoming Internet-savvy yourself, and keeping track of popular new websites.
- Fostering open communication and teaching your child basic Internet safety skills such as never giving personal information to a stranger.
- Using tried and true parenting tactics such as taking away privileges when your child breaks the rules.

- Soliciting your child's input and asking her about her opinions on the sites she uses.
- Networking with other parents who may be able to tell you about your child's activities and struggles they've had with their own children.
- Regularly checking your Internet browser history and cache, and forbidding your child from deleting web history.
- Keeping credit cards and other tools for easy online purchases out of your child's reach.
- Regularly searching online for both your child's real name and screen names she frequently uses.

This book is designed to give parents a brief overview of some emerging cyber threats that are increasingly popular with kids.

The Internet is a rapidly-changing environment, however, and no single source can list all of the dangers children face. Rather than focusing on a narrow list of websites, it's best to maintain open communication and stay up-to-date on emerging technologies. The sites and applications in this book give parents a rough overview of what's out there, but it's ultimately up to you to remain vigilant and keep up-to-date on Internet dangers. uKnowKids can be a part of that equation, providing parents with helpful information about emerging digital dangers and monitoring kids' Internet and mobile activity.

CHAPTER ONE

BURN NOTE

WWW.BURNNOTE.COM

WHAT IS BURN NOTE?

Most parents have warned their children that the things they say and do online will stay around forever, possibly creating an embarrassing digital permanent record. Burn Note attempts to buck this system by destroying messages after they are read. Users can post messages on the site and send them to a specific e-mail address. After the recipient logs in to see the message, she has 60 seconds to read it, at which point the message is permanently deleted from Burn Note's servers and cannot be accessed again.

WHAT ARE THE DANGERS OF BURN NOTE?

Burn Note creates an ideal environment for cyberbullying, and makes it nearly impossible to keep a record of such bullying. A teen can send another teen a mean or threatening note, but there will be no record of it and no way to trace who sent it.

On the flip side, the promised anonymity of Burn Note can also land your child in trouble. There's no stopping a recipient of a Burn Note from taking a screen shot or photo of a note, and this can create a permanent record of the note. A child who sends a threatening message to a teacher or who participates in online pranking might think there's no way to track it. But a savvy Internet user who wants to hang on to a copy of the note can still do so.

WHAT CAN PARENTS DO?

Because Burn Note promises anonymity and destruction of messages, kids can end up with a false sense of security when using the site. Talk to your child about the potential unintended consequences of using such a site, and explain that there is never a foolproof guarantee that anything will be anonymous or that your child's message won't be memorialized via screen shots or photos.

Because Burn Note can also be used for cyberbullying, blocking the website from your home computer may be the only option for preventing your child from becoming either a victim or a bully. The site now has a mobile app, and you may also want to consider blocking this app from your child's smart phone.

Of course, a child can always use someone else's computer or phone to send or receive a Burn Note, so regular communication with your child about her Internet use can make a world of difference. Burn Note, like most websites, does not allow children under 13 to use the service and states on its website that it takes precautions to prevent young users from sending notes. If your child is under the age of 13 and has sent or received a Burn Note, report the use to the website.

CHAPTER TWO

INSTAGRAM

WWW.INSTAGRAM.COM

WHAT IS INSTAGRAM?

Instagram is a photo-sharing service that allows users to quickly post photos from their smart phones to the web. Instagram apps were originally only available on iPhones, but newer versions of Android phones are now compatible with the service. Instagram capitalizes on the vintage trend by producing photos in a square shape similar to old Polaroid photos. Users can also apply filters to their photos to change color schemes, create an aged look, or make photos black and white. Some Instagram users feel that the photo filters make the photos more flattering.

WHAT ARE THE DANGERS OF INSTAGRAM?

Like most photo-sharing sites, the primary danger of Instagram is that kids will post photos that they later regret such as sexually explicit images, images of drinking or drug use, or photos of illegal or unethical activity such as bullying. Instagram users can set up accounts, follow complete strangers, comment on and receive comments on photos.

The rapid-fire posting offered by Instagram is also a concern. Like many other photo sites, users can upload photos from their phones directly to the site in a few seconds. Consequently, your child could snap an inappropriate photo and display it to the world in a few seconds and, even if your child later regrets the photo, the fact that it is displayed online means that millions of people have had the opportunity to view it, copy it, and repost it to other sites.

WHAT CAN PARENTS DO?

If your child uses Instagram, set up an Instagram account for yourself and require that your child allow you to “follow” her on the site. This enables you to see what she’s posting and to talk to her if you have any concerns about her photos. Even if your child’s photos are entirely innocent, however, privacy can be a real issue. Require that your child keep her Instagram account private, and mandate that she only allow people she knows in real life to follow her.

The commenting feature of Instagram means that bullying can be an issue, particularly when people make mean-spirited comments about others’ photos. Talk to your child about the risks of cyberbullying, and set rules as well as consequences if those rules are broken. While getting your own Instagram account and following your child is a good first step, it is not enough. Get a Parental Intelligence system like uKnowKids, one of the only ones that monitor Instagram, to understand how your child uses the site and make sure she is safe online, even when she wants to keep her activities secret.

Share this eBook!
www.uKnowKids.com

CHAPTER THREE

SPILLIT

WWW.SPILLIT.ME

WHAT IS SPILLIT?

Everyone, particularly self-conscious teens and preteens, craves the opportunity to learn what people truly think of them, and Spillit capitalizes on this desire. Users can set up a profile, then post a few questions and ask family, friends, and strangers to answer these questions. People can answer the questions anonymously or as themselves. The site has a Facebook application, making it easier for users to post their Spillit profile to Facebook and to expand the network of people from whom they seek input. Spillit also has a smart phone app.

WHAT ARE THE DANGERS OF SPILLIT?

Spillit is rife with cyberbullying, and the anonymous commenting feature means that anyone can say virtually anything to your child. Your child can also engage in bullying, and because her comments won't be posted to her own profile, you won't be able to track what she's saying. Spillit will not reveal the identities of anonymous posters, but your child might inadvertently give away her own identity in her posts, creating an environment in which bullying is rampant and children may make comments they eventually regret.

WHAT CAN PARENTS DO?

Because Spillit creates an environment where bullying can easily occur, it may be best to block the website and tell your child you don't want her to use it. Because it can be nearly impossible to keep your child from using a site, however, this website may require that you regularly check your child's Internet history as well as her smart phone usage. If you notice that your child has been using this site, talk to her – in a non-confrontational way – about why she wanted to use the site and what she sees as the benefits. This can provide an opportunity for an open dialogue about safety, online reputation, and the importance of avoiding cyberbullying.

CHAPTER FOUR

SNAPCHAT

WHAT IS SNAPCHAT?

Most parents are concerned about the effects of sexting – the practice of sending sexually explicit, photos, videos, or messages to web users. Snapchat, a mobile app, aims to ease some of these fears. Users can upload photos and videos to chat partners, but the images are deleted in about 10 seconds, meaning there's no permanent record of them and users don't have to worry that their images will one day end up on a website or result in public humiliation.

WHAT ARE THE DANGERS OF SNAPCHAT?

The primary danger of Snapchat is that it encourages users to send photos that they don't want other people to see since there is a self-destruction aspect. While there are other users for Snapchat, many users are using the site specifically to send explicit messages and images. While the photos are deleted from the server, the site poses the same dangers as Burn Note. Users can take photos or screen shots, permanently capturing images, even though Snapchat deletes them.

WHAT CAN PARENTS DO?

I would be wise to check your child's smart phone to see if she's been using the service. Talk to your child about the risks of sending explicit pictures and explain that there's no guaranteed method that ensures that there won't be a permanent record of the photo created. Carefully monitor her mobile phone use and, if Snapchat becomes a problem, you might want to replace your child's smart phone with a traditional phone that does not allow access to Snapchat.

CHAPTER FIVE

VINE

WWW.VINE.COM

WHAT IS VINE?

Vine is an app for mobile phones that allows users to take short videos of up to six seconds. These videos can then be uploaded directly to social networking sites. The app is commonly used with Twitter, but other websites can also accept Vine videos. Vine poses many of the same dangers as YouTube, and parents can take similar measures to make using both sites safer.

WHAT ARE THE DANGERS OF VINE?

Shortly after its release, Vine users began posting pornography, which some social networking websites – notably Twitter – do not ban. Children can also use Vine to capture inappropriate or illegal behavior such as bullying, drinking, drug use, and sexually explicit behavior. Because the videos are short, Vine can also be used while driving, increasing the risk to teen drivers.

WHAT CAN PARENTS DO?

Vine isn't always dangerous, and has been used for art projects, for social commentary, and even in advertising. Children who use it have access to a creative outlet, so banning its use entirely is probably not necessary. Instead, require that your child regularly show you her Vine account, as well as her social networking pages. Talk to your child about the potential risks of posting videos online, and ensure that she understands that the Internet makes it very easy for a "private" video to quickly go viral.

CHAPTER SIX

ASK.FM

(WWW.ASK.FM)

WHAT IS ASK.FM?

Ask.fm is the latest in a series of popular question and answer sites that also includes sites such as Yahoo answers. Users can post questions of nearly every variety to the website. Questions might be of a personal nature, such as, “How can I get along better with my sister?” or could be general knowledge questions about schoolwork, science, the news, and numerous other topics.

WHAT ARE THE RISKS OF ASK.FM?

Like other question and answer sites, kids can post personal information. The site has also gained a reputation for cyberbullying because some kids post questions asking about their relative attractiveness or use their friends’ names in their posts. The site also poses some privacy concerns. Users can post under their real names. A child who asks a question about illegal or immoral activity – such as, “How can I make a fake ID?” -- might see her Internet reputation haunted by the post for years to come.

WHAT CAN PARENTS DO?

Ask.fm and similar websites can provide easy access to information and opinions, so banning the site outright could be counterproductive. Instead, talk to your child about the importance of Internet privacy and ensure she’s not using her real name or a screen name that makes her identity easy to uncover. Explain that, even if she’s anonymous, she can still be tracked, so it’s wise to avoid cyberbullying and posting about illegal activity. Check your child’s Ask.fm account regularly to see what she’s been posting. Set rules for using the site, and consequences for breaking those rule. Sites such as Ask.fm can become the most dangerous when parents don’t know what their children are posting.

CHAPTER SEVEN

TUMBLR

WWW.TUMBLR.COM

WHAT IS TUMBLR?

Tumblr is a recent take on blogs and uses an approach known as "microblogging" that thrives on short posts. Users can post media to their own Tumblr site, and can also start Tumblr sites dedicated to information-gathering or specific causes. For example, your child might start a Tumblr dedicated to her favorite celebrities.

WHAT ARE THE DANGERS OF TUMBLR?

Tumblr, like social networking sites and blogs, allows kids to post private information, including photos and videos, for the entire world to see. Because Tumblr pages are often topic-specific, the site can be a recipe for cyberbullying. A child could easily create a Tumblr account dedicated to making fun of another child, for example. Further, some Tumblr sites promote questionable values by, for example, posting "thinspiration" photos for anorexics. Tumblr is open to all ages, and makes impulsive, questionable posts much easier to make than traditional websites.

WHAT CAN PARENTS DO?

Tumblr doesn't allow users to make their entire blog private. Instead, your child will have to select the option to lock individual posts, and you should require that she keep each post locked if she wants to use the site. Check in with her frequently and ask to review what she's posting on Tumblr. You should also require that she add you to the list of users who are permitted to see her Tumblr postings. Talk to her about the importance of privacy; don't allow her to use her full name, address, or phone number on her blog, and don't allow her to post photos of herself, her friends, or her home. Posting photos of clothes, animals, or events is usually ok.

CHAPTER EIGHT

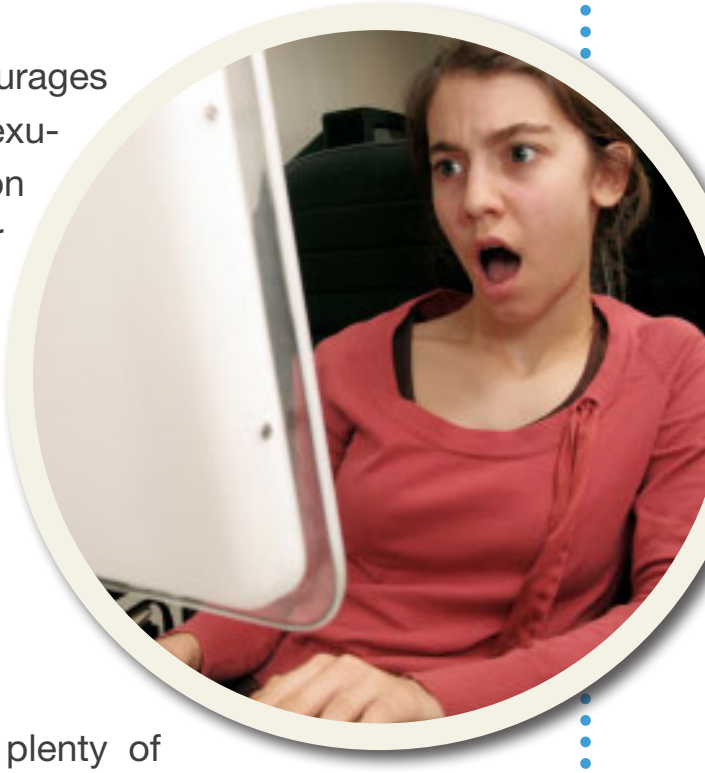
KEEK

WWW.KEEK.COM

WHAT IS KEEK?

Keek, like Vine, is a video-posting application that allows users to post brief videos online. The videos are advertised as status updates similar to the brief posts users can make on sites such as Twitter and Facebook. Users have to have a Twitter or Facebook account to access Keek.

WHAT ARE THE DANGERS OF KEEK?



Because the videos are short, Keek encourages impulsive posting, including the posting of sexually explicit content, which is not banned on Twitter. Even when kids have private Twitter or Facebook accounts, others can re-post or re-tweet their videos, making privacy a mere illusion on Keek. Keek can also be used to network with unfamiliar people across the world, giving cyber predators and bullies an opportunity to target your child.

WHAT CAN PARENTS DO?

Because Keek provides little reward and plenty of opportunities for trouble, it's best to block the site and ensure your child does not have the app on her smart phone. Because the site posts through social networking, monitoring your child social networking pages can help you investigate whether she's been using the site, and a Parental Intelligence service like uKnowKids can keep track of your child's social networking pages for you.

CHAPTER NINE

TEXTFREE

SMART PHONE APP

WHAT IS TEXTFREE?

TextFree is an app that allows kids to text one another within the application itself rather than through their phone. Texts are free and don't show up in a user's normal texting records. TextFree is one of many such applications, and there are dozens of free texting applications on tablets and smart phones.

WHAT ARE THE DANGERS OF TEXTFREE AND OTHER MESSAGING APPS?

Unless your child's cell phone plan charges for each text, there's no good that can come from TextFree. The service hides texts, so if you've forbidden your child from texting or regularly go through her phone, you won't be able to see what she's been up to. This lack of parental supervision invites sexting, inappropriate text conversations, texting during school, and texting about breaking parental rules.

WHAT CAN PARENTS DO?

If you want your child to be able to text but don't want to pay for a data plan, TextFree could be a good application. You'll simply need to require that your child show you her text messages when asked. If, by contrast, your phone plan already allows unlimited texting, TextFree has little use, and you're probably better off banning the app. However, kids are sneaky and can easily download apps even without your permission. Use uKnowKids to monitor your child's phone for new apps to make sure they are following the house rules.

CHAPTER TEN

DATING WEBSITES

WHAT ARE DATING WEBSITES?

The Internet has opened up the world of online dating, and about 40% of people meet their significant others online. Teens are increasingly using online dating sites, even when those sites specifically forbid people under 18 from accessing the site. There are a wide variety of dating sites, including Match.com, OkCupid, Plenty of Fish, Adult Friend Finder, and numerous others.

WHAT ARE THE DANGERS OF DATING WEBSITES?

Dating websites are specifically designed to move online relationships to the real world. Not only can your teen meet people who aren't who they appear to be; your teen can also present inaccurate or misleading information about herself. Further, these sites can be a breeding ground for people who want to prey on naive and unsuspecting minors.

WHAT CAN PARENTS DO?

Blocking dating websites is a step in the right direction, and carefully monitoring your child's Internet use can help keep you aware of any new dating sites that spring up. Additionally, use the same rules you'd use for offline dating. Require that you have to meet anyone your child goes on a date with and forbid her from meeting people from the Internet. If you notice that your child is suddenly talking to a new person quite a bit, don't overreact, as this can increase secrecy. Instead, talk to your child about her dating life and encourage her to come to you with questions and to rely on you as a source of information.

CHAPTER ELEVEN

ONLINE GAMING

WHAT IS ONLINE GAMING?

The world of online gaming is a diverse one, with thousands of games available. Simple applications, such as Pathwords and Typing Maniac, are built into Facebook and mobile phones. More complex games include massive online multi-player role-playing games such as Second Life and Internet-based gambling websites. Many online games require a membership or credit card, but others are available for free.

WHAT ARE THE DANGERS OF ONLINE GAMING?

Because the online gaming world is so diverse, the dangers vary from game to game. One of the most serious concerns is that online gaming can be addictive. Additionally, online games give users an opportunity to interact with a wide variety of people. While this can build social skills and help kids make friends, it can also lead to bullying, inappropriate sexual behavior, and encountering dangerous people who want to meet offline. Second Life in particular has received significant media attention because it encourages users to create a second identity that can blur the boundaries between fantasy and reality.

Internet-based gambling poses unique dangers. While children aren't allowed to gamble and gambling is illegal in many states, all your child needs is access to someone's credit card. He can then quickly run up large gambling debts, potentially interacting with dangerous people in the process. Gambling is also highly addictive.

WHAT CAN PARENTS DO?

Don't allow your child to have a credit card, and keep your credit cards inaccessible. This ensures that your child can only play membership-based online games with permission. It's also wise to ask your child about her gaming habits and talk about the dangers of addictive gaming as well as the risks of meeting people who aren't who they claim to be. If you notice your child spending an inordinate amount of time on her phone or computer or see that she's neglecting other responsibilities, try limiting her daily gaming time.

Share this eBook!

www.uKnowKids.com

CONTRIBUTORS:

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

Zawn Villines - Zawn is a professional writer who specializes in parenting and mental health. A former nanny, she educated numerous parents about digital dangers and has written hundreds of articles and dozens of eBooks on child safety.

Edited by **Callie Harris**

Layout & Design by **Julie Csizmadia**