COX®

your friends in the digital age®

INTERNET SAFETY

On behalf of our 2,000 employees dedicated to providing the very best, fastest and safest Internet experience available, Cox Communications has created this special section for you as part of our ongoing commitment to San Diego families.

Cyberbullying and Sexting Growing Dangers

Cyberbullying and sexting are becoming more common among teens ages 13 to 18. Many parents don't even know whether their child has been a victim or been involved in cyberbullying or sexting. So, what can parents or guardians do to combat these growing dangers?

Cyberbullying occurs when a person is being harassed online, whether through a text message, email, or social networking website. Some forms of cyberbullying include receiving an anonymous email with a hateful or threatening message, or a rumor that is started through a social media website. Cyberbullying can even occur while your child is playing a video game with others online. In all of these instances, an online "bully" can remain anonymous if he or she chooses.

Cyberbullying can be as emotionally painful for a child or teen as being bullied on the playground. However, with cyberbullying, you can't see the perpetrator, so it's especially important for children to tell their parents when they experience or are witness to cyberbullying.

A survey conducted by Cox Communications and the National Center for Missing and Exploited Children indicates that:

• More than one-third of teens surveyed have been cyberbullied, have perpetrated cyberbullying, or know friends who have experienced or perpetrated it;

• 66% think cyberbullying is a serious problem;

• About four in five teens (81%) think that bullying online is easier to get away with or to hide from their parents than bullying in person.

Parents can help keep their children safe from cyberbullying.

• Remind your child that he or she can come to you when feeling threatened or scared by a comment or image. Many times, they are hesitant to tell their parents for fear that they will be blamed, are embarrassed, or will be banned from using their technology or social networking sites.

• Do not respond to the message. It's important that your child not engage the cyberbully.

• Save the message or image in case you need to share it with your child's school or local law enforcement if the harassment continues.

• Report the cyberbullying to the social media outlet where it was seen – whether it was an Instant Message on Facebook or a text message on your child's cell phone. And, don't forget to remove the bully from your child's online friends list.

• Monitor your child's online pages and text messages to make sure they are not receiving harassing or threatening messages.

Sexting – sending, receiving or forwarding sexually suggestive nude or nearly nude photos through a cell phone – is another growing problem among teens. The survey conducted by Cox Communications and the National Center for Missing and Exploited Children indicates that 81% of teen "sexters" are under 18. The survey also indicates:

• 19% of teens surveyed have engaged in sexting;

• 60% of teens who sent sexts say they send photos to their boyfriend or girlfriend;

• 11% say they've sent sexts to someone they don't even know;

In addition to talking to your kids about the dangers of sexting and how it can negatively impact online reputations, there are some other things parents can do to reinforce the message that sexting is inappropriate behavior.

• Inform your child that it is illegal to send or forward sexually explicit photos, messages or videos from a cell phone and that they could be breaking the law and face legal consequences if they participate in sexting.

• Remind them that saving this type of message is also illegal, so they need to delete a sext immediately if one is sent to them.

• Encourage your teen to tell you if he or she recognizes an individual in a sext. The person in the photo may be a victim and not aware that a sexually explicit photo or video of him or her is being circulated.

• Monitor your child's text messages to make sure they aren't sending, receiving or saving sexts.

Experts and teens say the best advice they can give to parents and guardians about how to talk to their kids and how to protect them from harm is – don't overreact. Children need to feel they can tell their parents or guardian when they receive an unsolicited message, or if someone makes them feel uncomfortable while online.

Teens who don't tell their parents about cyberbullying or sexting have stated they won't tell because they're embarrassed by the content or photos they received and they're afraid their parents will blame them for receiving the message. When talking to teens about cyberbullying or sexting, hold them accountable for using appropriate behavior online, but stay calm to keep the lines of communication open.

Also, remember that teens don't just access the Internet through computers. Nineteen percent of teens surveyed go online via their cell phone, and their parents are often unaware. That can change if parents take action, like talking to their kids and visiting websites such as **www.Cox.com/TakeCharge** that provide online safety tools and tips.

TAKE CHARGE: Navigating safely through the digital age

Q&A with digital media expert James Andrews

"The act of social networking – the verb – is just something we do," says James Andrews, Digital Media expert and co-founder of Everywhere. "As author Charlene Li (Groundswell) describes it, it's like air. Social networking is becoming a course of action we all engage in, without even realizing we're doing it."

A contributor to CNN and a frequent blogger on FastCompany.com, Andrews and his wife are active participants of social networking. The couple's 15-year-old son writes a food critic blog for a local Atlanta newspaper, and their 8-year-old daughter is making her mark as an online DJ.

As part of its Take Charge initiative (www.cox.com/takecharge) to keep kids safe online, Cox Communications spoke to Andrews about his tried and true rules for social media; steps that parents can take to establish their own social networks; and how he governs his own children's use of social media.

Cox: How should parents start a dialogue with their children about their online behavior?

James Andrews: It starts with a parent's own interaction with social technologies which is critical. The technology is moving so fast that it's a game you can't play from the sidelines. You must be a real user of the tools. It's not enough to read about it in the New York Times or some other publication. Join a social network; it's the only way you'll gain the basic fundamentals of interacting with complete strangers. It's really hard to have these conversations with someone who's not using social media.

COX: In addition to test driving the technologies, what other resources do you rely on to stay abreast of where the technology is headed?

JA: Parents could start www.mashable.com, but there are several bloggers and authors I follow on Twitter, such as author Charlene Li and blogger Jeremiah Owyang who are with The Altimeter Group. That's really how I use Twitter and Facebook; it's my newsstand.

COX: Despite five years of disturbing research about teens' online behavior and the dangers they face online, parents still have to be convinced of the difference their involvement can make. What's your best pitch?

JA: Parental involvement is critical because, whether you like it or not, kids are learning the skill of social networking. So, the question becomes how much you as a parent are going to inject yourself into the equation. Those parents waiting for a declaration that 'Social networking is happening now!' will be left behind. You must start discussing online issues now which includes privacy concerns, digital reputation management and how information kids post leaves a digital trail. Parents who are involved with social media have a much better understanding and can talk to their kids more candidly than parents who aren't.

Coincidentally, social networking also allows for a different level of parenting; whereby parents can not only watch their children, but they can watch your children as well. In about the same way that if you saw your neighbor's kid in a liquor store you would alert them, social networks allow you to parent a kid within your community. So, if you're friends with one of your friends' kids, and they're acting out of line, it's critical for us who are engaged in social media to keep disconnected parents in the loop.

COX: You raise an interesting point about being online friends with kids who aren't yours. Are there guidelines for navigating the "Do's" and "Don'ts" of being online friends with other people's kids?

JA: I'm a little concerned about parents who are friends with kids in social networks, especially if they're not in your community or circle of friends. It becomes part of the privacy conversation that needs to happen in the home, and parents should be very clear about who of their friends their child is allowed to "friend" online. This is one of those areas that could go very wrong. That's why I will outline for my daughter who of my male friends she's okay to "friend" online – because I will want to be a friend of his and see the dialogue between them…which is a prime example of why I can't govern from the sidelines. There's also the issue of teachers being friends with students online, as well as parents being friends with teachers.

COX: In your expert opinion, where do you think the conversation is headed?

JA: Connecting with people while you're driving is definitely a big one, but there are also privacy concerns that come with location-based technologies such as foursquare. Facebook will launch something similar in the next few days – and the same with Twitter. Social technologies, combined with mobile, GPS-type technologies, will become the norm, but users will need to set privacy settings around online tools with 'check-in' features. It's not the future, it's now. There are positives to location-based technologies, but they don't come without privacy concerns.

COX: What five-step process can you offer to parents interested in joining a social network?

JA: Step #1 – Get involved. Facebook is a beginner site. Start to engage and build a community there, but be sure to learn how to set your privacy settings. Control what information you'd like to share and what you'd like to receive.

Step #2 - Manage your online persona. The other aspect of social media is managing your online reputation so, if you're a parent, set up Google Alerts for your name and your child's name to manage your online reputation. Another search term of interest might be "Internet safety" and "kids."

Step #3 - Become familiar with mobile technologies. Personally, our house rule is no mobile technologies or laptops in the bedroom. Since Apple came out with the iPhone, the house rule now includes phones. But we may have overlooked that if we didn't have an understanding of the capabilities of today's smart phones. Today's phones are really a computer in your kid's hand.

Step #4 – Set some ground rules. For instance, know the functions of IM or the chat function. We used to love that our son used AOL chat because they provide you with a back-end parental guide to track your child's IM habits; how frequent they chat; what time of the day; who they chat with, etc. But now, Facebook has a chat function … which gives you nothing. So, you may need to tell your kid which chat function they can use; however, be aware that they'll want to chat where everyone else is. As a parent, use instant messenger, use Facebook chat and learn the loopholes for communication.

Step #5 – Beware of video chat. There are several iterations to consider: Tinychat, Chatroulette, Skype and Apple's iChat. There's also Ustream which is a streaming video site where kids can chat with their favorite celebrities. It used to be that kids would read about their favorite celebrities in magazines, but now they're communicating with them online and there's a level of intimacy that wasn't there five years ago.

COX: How do you govern your own children's usage of social media?

JA: Outside of the "creepy people" factor, there's the issue of social media being a "time suck." As parents, we must govern usage by establishing set hours for when children can log into their social networking sites. It used to be that parents would set their kids in front of the TV for a few free minutes. Now, they give them a computer or smart phone to keep them busy and that can be dangerous. Additionally, at a bare minimum, you need to have passwords to your kid's accounts. Yes, your child will probably adjust the privacy settings so you can't see everything, but talk about that. And, obviously, social networking should not be happening at 3 a.m. in your child's bedroom or bathroom. Designate a family room in the house for use of social technologies. Social media is fun to play with, but it can have a damaging effect on time which is something we can't get back.

ONLINE SAFETY FOR SENIORS

Nine ways to be Internet savvy

By Claire Yezbak Fadden

For many San Diegans, the Internet is a cyber path to convenience. With just a click, they can stay connected to friends and family, pay bills, check bank statements, make vacation plans, share photos and shop for hard-to-find treasures. For some older adults, though, the Internet is a passage to a world of unknown threats, scammers and hackers.

Although seniors are computer savvy, many are reluctant to take advantage of this amazing tool sitting on their desktop. Studies show that many mature adults worry that they might break something, lose irreplaceable information or fall prey to online predators.

By exchanging misgivings, worry and doubt for planning, preparation and alertness, seniors can go online with ease, confidence and peace of mind. Here are nine ways to get started.

1) Protect your computer. Take steps to ensure your computer is properly secured. After installing security software, be sure you are receiving automatic updates. Double check to make certain your firewall is turned on. If you're not sure how to do this, hire a computer technician from a reputable company to review your settings for security and fix any problems you may have.

2) Make your passwords strong. "I'm really careful with my passwords," said baby boomer Carol Schoenherr of Chula Vista. "To keep them from being deciphered, I use a mnemonic device — like taking the first letter from each of the words of a song lyric." Schoenherr doesn't use the same password for every site and never shares them. "Don't keep your list of passwords on your computer," she advises, "unless you have a foolproof way to keep others from of accessing it."
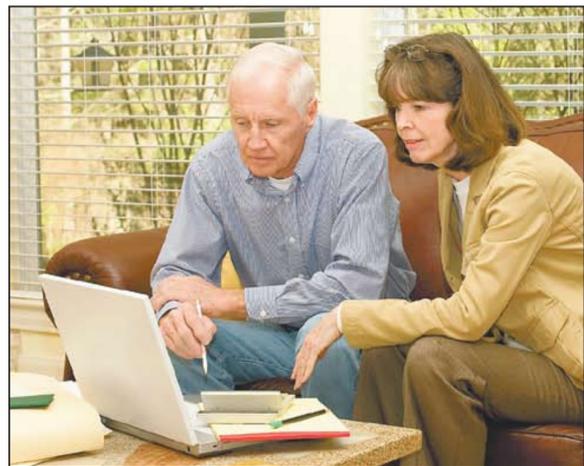
3) Protect your information. Just because a site asks for your personal or financial data doesn't mean you have to provide it. Whether you're on a social networking site, using e-mail or doing a bit of online shopping, always stay leery of sharing any personal data. If it's not a site you trust, don't be afraid of being rude. Decline to continue. That's a much better option to being ripped off.

4) Deal with trusted sites. It's easy to judge a brick-and-mortar store or folks you meet in person. It's tougher to judge a company you meet online. No matter what your age, fake sites are difficult to identify. Scammers build sites to look official and legitimate. If the site seems suspicious to you, or they're asking for information they should already have, leave the site before any providing information.

5) Be aware of e-mail scams. A common way online criminals get access to personal information is through e-mail. They call this phishing and their goal is to steal your identity. Reputable banks and companies don't contact you through e-mail to verify your information, validate your identity or re-enter your password.

6) Don't open e-mail attachments. Clicking on the little paperclip might lead to photos from friends, but if you don't know the sender, don't open any attachments. "Attached files may contain malware (malicious software), which can damage your computer — or it may install code that can track your activities," said Nancy C. Muir and Linda Criddle, authors of "Using the Internet Safely for Seniors For Dummies."

7) Bookmark verified sites. One thing a criminal can't fake is the actual web site address of a company or bank. Instead of clicking an e-mail link, search for the real online address using a search engine, like Google or Yahoo. Use that site's information or call the phone number listed on your statement to investigate the message you received. Mark the real site as a favorite in your browser so you can find it easily in the future.

8) Targeting seniors. Criminals use age, interests and hobbies as a way to get your information. Crooks trying to target 20-somethings may offer tickets to a popular concert. For mature adults, the scam may come in the form of discounts for prescriptions or insurance. Their goal is to get you to take action before you've really had a chance to think. If the deal seems too good to be true, pass it by.

9) Update Your Internet skills. The more we do something, the better we get at it. You'll learn a lot about "surfing the web" by just spending more time online. You can also read or take a course to brush up a bit. Many computer classes are offered at low cost through local colleges and libraries. Check out the San Diego Eldercare Guide's computer class listing at **http://eldercare.signonsandiego.com/?q=node/1090** for classes in your area.

Decoding Internet, texting lingo
What kids are really saying online

Parents may know their child's frequent hangouts, closest friends, and favorite kind of music. But unless they know the difference between the P in PM, PU, and POS, they're clueless about their teen's life online. With 75% of teens today using Instant Messenger, odds are your teen is fluent in chat lingo. While these abbreviations and acronyms make Internet chatting easier, they also can be used to hide information from their parents.

A survey by Cox Communications and the National Center for Missing & Exploited Children revealed that 95% of parents don't know the common chat lingo teenagers use to warn those they're chatting with that a parent is watching.

Knowing the difference between PM (private message), PU (that stinks), and POS (parent over shoulder) is a simple precaution for parents to take against online predators. With startling statistics, such as nearly 30% of teens are considering meeting a person they have only talked to online and 14% of teens have had F2F (face-to-face) meetings with people they've met through the Internet, parents need to crack the code.

Translations for common phrases include suggestive acronyms like WTGP (want to go private) and NIFOC (naked in front of the computer) along with signals like P911 (my parents are coming!) and PA (parent alert). Other popular acronyms include:

A/S/L – age, sex, location
BF – boyfriend
DIKU – do I know you?
GF – girlfriend
H&K – hug and kiss
ILU or ILY – I love you
IPN – I'm posting naked
IWALU – I will always love you
KOC – kiss on cheek
KOL – kiss on lips
LTR – long term relationship
NP – nosy parents
OLL – online love
PAL – parents are listening
PANB – parents are nearby
RBTL – read between the lines
TAW – teachers are watching
WTGP – want to go private
WTMIRL – want to meet in real life

While learning the chat lingo won't earn you any cool points with your teens, it can help you protect them from online danger. For a complete list of chat terms, go to **www.cox.com/takecharge**.

Survey reveals teens not as safe online as they think
84% now have social networking profile

Since 2006, Cox Communications has partnered with The National Center for Missing & Exploited Children (MCMEC) to conduct a nationwide survey each year among teens ages 13-17 to gauge teen online behavior and give parents a window into their children's online world – a world that many parents rely on their kids to help them navigate through.

This year, the survey revealed that although confident that they are being safe online, teens continue to take risks and remain vulnerable. Teens claim to carefully manage the image they project online, yet they continue to post personal information and photos online that can be seen by people they've never met. In fact, 42% of the survey respondents admitted to having a public profile on a social networking site such as Facebook or MySpace that anyone could see, and they're posting information such as their age, school and city where they live.

And, the number of teens who are interacting online is increasing.

In 2006, 51% of teens surveyed had a profile on a social networking site such as MySpace. That number jumped to 84% in 2010 (a 33% increase in the past five years). Today, 84% of teens have cell phones that they use for text messaging. That's an increase of 21% since 2006, when only 63% of teens surveyed texted on their cell phone. And, the number of teens who play video games online with people they've never met in person increased from 33% to 45%. Children of all ages have ways to access the Internet beyond their home computer. They are going online via their cell phone, gaming systems, and even handheld video games, so parents have even more to consider when monitoring their children's online activity.

So, whether they're playing a game online, sending text messages, or posting information on their Facebook page, make sure your teens remember the following:

• Once they post or send something online, they can't take it back. Even an inappropriate photo meant to be seen by someone they trust can be forwarded without their knowledge, or posted on another person's social networking page for the world to see.

• Don't use inappropriate language. Other adults such as their friends' parents, teachers, college admissions officers, or potential employers may be able to view their posts.

• Teens that use sex talk online are more likely to come in contact with online predators, so the need to refrain from using any sexually explicit language in their posts.

• Do not post telephone numbers or street addresses – either their own or another's personal information. Posting someone else's personal information, whether a friend or not, can compromise that individual's safety.

• Do not open or forward chain emails or texts. Just delete them. They can carry viruses or spyware, which can then be used to access personal information.

Take our survey to test your Internet security knowledge

1) "Pharming" is:
a) An e-mail that tries to persuade you to give up personal information
b) A web site imitating a legitimate brand you know and trust
c) The new, hip way to grow crops

2) A good way to judge whether a web site is secure is to:
a) Access the web site by clicking on a link in the e-mail
b) Look for the company logo and corporate color-scheme
c) Look for "https://" at the beginning of the URL

3) A "Phishing" scam is:
a) Calling into work sick, and then going fishing
b) An e-mail that contains false urgency to validate personal information immediately - with the intentions of stealing your personal information
c) People selling counterfeit concert tickets to see a Grateful Dead-like band

4) The best way to avoid phishing and pharming online is to:
a) Never shop online – always go to the brick and mortar store to make purchases
b) Cut up your credit cards and only use cash
c) Continue to pay bills and shop online – but be aware of when and where you give out personal information

5) If you come across a phishing or pharming scam, you should:
a) Notify the FBI, FTC, the Anti-Phishing Group and the company that is being imitated
b) Forward it to all your friends
c) Do nothing

6) Security software is:
a) Nice to have, but not really important.
b) A waste of time and/or money.
c) Important to have installed on every computer.

Answers: 1) b 2) c 3) b 4) c 5) a 6) c

A TEEN'S PERSPECTIVE

Managing your reputation online

By Michelle Wintersteen

Think for a second. What does your Facebook page or online presence reveal about you? If someone you don't know looks at your profile page, how do your pictures, posts, and comments reflect who you are as a person?

This past summer, I was invited to participate in Cox Communications' Teen Summit on Internet and Wireless Safety in Washington D.C. moderated by John Walsh from America's Most Wanted in partnership with The National Center for Missing and Exploited Children. There, I met with teens across the nation to discuss important topics regarding our use of social media. The topics included: cyberbullying, texting, sexting, and, what is becoming more and more important, reputation management.

But what is reputation management, and what does Facebook or other forms of social networking have to do with it? Reputation management refers to how a person presents himself or herself to others online. A 2008 Kaplan University study presented the effects of social media on students applying for college. The reality is that Facebook and other social media pages are not just for your own social circle anymore. It reported that, "of 320 admissions officers from top colleges … roughly 10% visit social networking sites." Today, what teens post on the Internet can be viewed by college admissions officers, teachers, and potential employers.

San Diego teen Michelle Wintersteen discussed online safety with "America's Most Wanted" host and child advocate John Walsh during the 5th annual Cox Teen Summit on Internet and Wireless Safety in Washington D.C. in June.

Most teens seem to know that what they post can have an effect on their reputations, but many are still posting inappropriate comments or sexually explicit images of themselves online. Cox Communications' Teen Online Safety & Digital Reputation Survey in 2009 reported 82% of teens believe their reputation can be affected by what they post online. Now that college application deadlines for Fall 2011 are fast approaching, teens must reconsider what we post online. Personally, I want my actions online to reflect my character. I want a college admissions officer to recognize that I am thoughtful and conscious of what I do and do not post.

Social Media is a powerful form of communication that can be a great benefit to us all if used appropriately. It allows us to stay in touch with cherished family and friends who are far away and share photos and videos of milestones or important moments in our lives. When used inappropriately, such as posting risqué photos of yourself or others, there can be life-changing consequences. Among the college admissions officers surveyed by Kaplan who visit social networking sites, they were more likely to get a negative impression of the applicant than a positive one. An applicant's web information made a positive impression about 25% of the time and a negative impression 38% of the time, according to the Kaplan survey. Regarding students' Facebook accounts, Kaplan goes on to list that what students do on the web could do more potential harm than good.

Kaplan suggests that college applicants remove from their social networking pages any pictures of themselves or others involving alcohol or anyone who appears to be under the influence. Also on the list: sexually explicit photos, groups suggesting illegal activities or bigotry of any kind, and anything that exhibits poor judgment. With all of the dangers that come along with the Internet, posting personal information, especially phone numbers and addresses, is considered poor judgment. All of these factors play into how a potential employer or future college may view you.

I am a hard-working student. I am currently witnessing firsthand how competitive it is to get into college. Today, everything done during high school is taken into consideration, from grades and test scores to extra-curricular activities and athletics. As students, we are counseled to show colleges something that gives us an edge over all of the other students applying with similar applications. We must answer the question: "How do I stand out?" We must remember that what we do on the web is a factor. I know that I think twice when I post. I learned at the Teen Summit that what I post on the Internet is on the Internet permanently. One bad decision can have lasting consequences. Knowing this, I want to create the best possible reflection of who I am. When college admissions officials compare my application to those of the hundreds of similar 3.9 GPA applicants, I invite them to look at my Facebook page. I want them to see that I am the responsible, smart, focused, confident and conscientious student that they are looking for.