The BROWARD COUNTY CRIME COMMISSION

Presents

2017 PSYCHOLOGY of CYBERCRIME Conference

"Internet Child Crimes, Cyberstalking, Computer Hacking, Ransomware Extortion"

An Ongoing Concern

As Part of the Crime Commission's *Building Bridges* Mental Health Conference Series

DATE:

Wednesday, October 4th, 2017

ADDRESS:

Deerfield Beach Doubletree by Hilton Hotel

100 Fairway Drive

Deerfield Beach, Florida 33441

SIGN-IN SERVED WITH CONTINENTAL BREAKFAST

7:15 a.m. – 7:45 a.m.

AGENDA SERVED WITH SIT-DOWN LUNCH

8:00 a.m. – 3:45 p.m. (Lunch 12:00 p.m. to 1:00 p.m.)

www.BrowardCrime.org

"Evil Triumphs When Good People Stand Idly By"

10640 Northwest 32nd Street, Sunrise, FL 33351; TEL: (954) 746-3117; FAX: (954) 572-7988;
EMAIL: info@browardcrime.org

ABOUT THE CRIME COMMISSION:

Purpose:

The Broward County Crime Commission is a 39 year old independent, state chartered office, acting judiciously on behalf of law – abiding citizens, in overseeing local, state, and federal Criminal Justice System protocols, processes, methodologies, and approaches, to better protect and assist the citizens of Broward County.

Mission:

The Crime Commission assesses and evaluates crime in Broward County (and south Florida), and works in concert with Law Enforcement, the General Public, and the Criminal Justice System, to derive solutions against crime, as well as social issues that can transpire into crime, in order to enhance public safety.

Role:

As an independent, fact – finding agency, the Crime Commission has distinguished itself as a laureate governing body, which works diligently to improve the integrity of the Criminal Justice System, as well as strengthen and preserve the key components of Public Safety in Broward County, on behalf of the Broward County citizenry.

Operations:

The Crime Commission executes its operations through a cadre of meritorious program's involving perspective, education, research, white paper studies, technology, analytics, advocacy, certifications, outreach rehabilitative and counseling programs, and facilitation of findings to both the Criminal Justice System and the residents of Broward County.

Programs:

The Crime Commission embodies innovative, preemptive, and proactive protocols (versus reactive programs), especially with guiding and mentoring children, so that they do not succumb to a life of crime, or suffer the ill fate of a heinous crime.

Programs for 2017 include:

1. The Building Bridges Mental Health Conference Series, as It Relates to Psychosis, Psychopathology, and Crime Reduction
2. Broward County Crime Commission Center for Research and Technology
3. CSI: STEM Leadership Summer Camp
4. High School Criminal Justice Curriculums

INTERNET CRIMES AGAINST CHILDREN:

The Problem:

Research conducted relative to Internet crimes against children can be grouped into several subtopics: unwanted solicitation for sexual contact or pictures; pornography (children as the subject); harassment and bullying; and unwanted exposure to sexually explicit material. Many of the studies described in this document have been conducted by researchers affiliated with the Crimes Against Children Research Center at the University of New Hampshire who extrapolated data from the First (2000) and Second (2005) Youth Internet Safety Survey. These surveys canvassed a nationally representative sample of 1,500 youth ages 10 to 17 to determine the incidence and risk factors of youth exposure to sexual material on the Internet. Researchers also extrapolated data from the National Juvenile Online Victimization Study, which was intended to estimate the incidence of Internet sex crimes against minors occurring during a one year period (2000–2001) that were known to law enforcement officials. This bibliography reviews the findings of the studies conducted using these surveys, as well as other surveys conducted for the purpose of identifying the patterns and frequency of criminal use of the Internet involving children. The bibliography also reviews the results of focus-group studies, literature reviews, and reports commissioned by the U.S. Congress.

Scope of the Problem:

Communication technologies, such as computers and cell phones, and social-networking sites as Facebook enable the rapid creation and dissemination of harassing and pornographic text, pictures, and video. Paris S. and Robert D. Strom note that whereas adults generally use technology only as a tool, adolescents consider technology, including text messaging and chat rooms, to be an essential part of their social life. The results of a 2007 online survey of more than 40,000 students ranging from kindergarten through twelfth grade (Samuel C. McQuade and Neel Sampat) indicate that children begin using the Internet at kindergarten age or younger and that online activities of children in the grades covered by this study include inappropriate behavior and exposure to inappropriate content. Wolak, Mitchell, and Finkelhor note that Internet use by youth age 12 to 17 increased from 73 percent in 2000 to 87 percent in 2005. Cyberbullying (bullying by means of electronic communication, such as instant messaging, e-mail, chat rooms, and cell phones) and victimization begin as early as second grade for some children, and by middle school, students as a group experience or engage in all known forms of cyber abuse and this document is a research report submitted to the U.S. Department of Justice.

Researchers (Wilson Huang, Matthew Earl Leopard, and Andrea Brockman) have concluded that the rapid growth of online sexual exploitation of children can be linked to increased Internet accessibility and anonymity, commercialization of exploitative media, and digitization in the production and dissemination of images. These researchers found that, despite legislative initiatives intended to keep pace with the incidence of this type of crime against children, the nature and distribution of child pornography, as well as the characteristics of offenders and victims alike, have remained similar over time and across a wide sample of studies. A 2007 staff report of the U.S.

House Energy and Commerce Committee placed the issue of Internet crimes against children in perspective. The committee found that the number of sexually explicit images of children on the Internet was increasing, and that victims were typically younger and the images more violent than in previous years. At the time the report was written, it was estimated that Web sites hosted in the United States accounted for more than half of the child pornography on the Internet, and that commercially available child pornography on the Internet comprised a multibillion-dollar per year industry.

Incidence of Internet Activity:

Researchers studied the frequency of exposure to sexually explicit material by boys and girls, how often the youths posted this material, and the frequency of online bullying and harassment activity. Kenzie A. Cameron and Laura F. Salazar found in their study of adolescents ages 14 to 17 that among the participants who reported incidences of exposure to sexually explicit Web sites, most occurred accidentally or unintentionally, via unsolicited e-mails (10 to 20 per day) containing explicit content or links to explicit material. Chiara Sabina, Wolak, and Finkelhor, using data compiled from an online survey of more than 500 college students, found that 72.8 percent (93.2 percent of the male students and 62.1 percent of the female students) of the sample group reported that they had viewed online pornography before the age of 18. Males were found to be more likely to view pornography frequently and to view a variety of images, while females were more likely to be involuntarily exposed to pornography. Wolak, Mitchell, and Finkelhor, in "Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users" reported findings of data taken from the Second (2005) Youth Internet Safety Survey regarding exposure to online pornography. They found that 42 percent of a sample of 10- to 17-year-old Internet users had viewed online pornography during the previous year. Of that 42 percent, 66 percent reported that they had not sought or desired the exposure to pornography.

A survey of more than 1,000 teens and young adults conducted in 2008 and reported by the National Campaign to Prevent Teen and Unplanned Pregnancy revealed that 20 percent of the teens had sent or posted nude or seminude pictures or video of themselves, and 11 percent of young adolescent girls (ages 13 to 16) had done so. Thirty-nine percent of teens reported sending sexually suggestive text messages ("sexting"), and 48 percent of teens reported having received such messages. Mitchell, Finkelhor, and Wolak, in "Online Requests for Sexual Pictures from Youth," used data from the 2005 youth survey to assess the incidence of soliciting youth to produce sexually explicit images and post or transmit them online. The authors found that 13 percent of the youth in the study population had received unwanted sexual solicitations over the Internet, and although 4 percent of the youth had received an online request to send a sexual picture of themselves, only one complied. Thirteen percent of the overall survey group received unwanted sexual solicitations that included requests for pictures.

Social-networking Web sites, such as Facebook, My Space, and You Tube, are often used by young persons to harass their peers. Michele L. Ybarra and Mitchell, in "Prevalence and Frequency of Internet Harassment Instigation," extrapolated data from the 2005 youth survey to identify the frequency with which youth ages 10 to 17 engaged in online harassment activity. They found that almost 30 percent of youth had harassed others online during the previous year: 6 percent had frequently harassed others via the Internet; 6 percent had occasionally harassed others online; and 17 percent had

harassed others a limited number of times. Amanda Lenhart reports the results of a Parents and Teens 2006 Survey tabulating the incidence of cyberbullying. Researchers found that 32 percent of more than 900 youth (ages 12 to 17) Internet users surveyed had been harassed online. Of this group, 38 percent of the girls and 41 percent of the girls ages 15 to 17 had experienced online harassment, as compared with 26 percent of the boys. Thirtynine percent of teenagers who provided personal information on a social networking site were the target of harassment. Robin M. Kowalski and Susan P. Limber studied the prevalence of electronic bullying (defined as bullying that takes place through Internet chat rooms, e-mail, instant messaging, or Web sites) among middle school students. Their research found that 11 percent of the students reported being electronically bullied one or more times in the previous two months; 7 percent stated that they had bullied others electronically and had been the victims of electronic bullying; and 4 percent reported that they had bullied others electronically but had not been victims. Chris Moessner reported the results of a national survey of more than 800 children ages 13 to 17 measuring adolescent reaction to cyberbullying, which is defined as the use of the Internet, cell phones, or other technology to send or post text or images intended to hurt or embarrass another person. More than 43 percent of the teenagers in the survey reported that they had experienced cyberbullying in the previous year, with the most common occurrence among those 15 and 16 years old.

Role of the Family and Other Caregivers

Researchers looked at the role parents and other caregivers can play in preventing children from becoming victims of Internet crime, emphasizing that better education programs are needed and that strong communication between adults and children is critical. The study by Chang-Hoan Cho and Hongsik John Cheon found that parents generally underestimate their children's exposure to negative material on the Internet, when in fact children encounter negative content frequently. McQuade and Sampat found that 66 percent of high school students reported that their parents provided no supervision of Internet activities. Cho and Cheon confirm the findings of earlier studies that parents of families exhibiting high levels of cohesion perceive greater control and understanding of their children's Internet use. Similarly, Greenfield found that a warm, communicative parent–child relationship, appropriate sex education, and parental participation in children's Internet activities are critical factors in protecting children from adverse effects of exposure to explicit sexual material. Moessner, in his study of a national survey of cyberbullying by those 13 to 17 years old, suggests that parents can help their children avoid cyberbullies by setting expectations for online behavior and monitoring children's Internet activities. Stefan C. Dombrowski, Karen L. Gischlar, and Theo Durst note that caregivers can access various software tools such as firewall security barriers to monitor a child's online activity and help protect him or her from accessing unsafe Web sites. In addition, they recommend that parents discuss Internet dangers, monitor Internet usage, supervise Internet friendships, and establish an Internet-use contract with their child. Whitney Roban, reporting a 2001 study of more than 1,000 girls ages 13 to 18, concluded that not all girls are receiving pertinent Internet safety information from their parents, and that half the girls in the study reported breaking Internet rules set by their parents. The study concludes that parents should try to be more proactive in their relationship with their daughters; if they develop a greater understanding of their daughters' online lives, they can better help them navigate

negative Internet experiences. The Internet Safety Technical Task Force, in its final report, concludes that in order to address the problem of online safety for minors, adults must use the numerous technologies intended to enhance Internet safety, together with parental oversight, education, social services, and law enforcement.

Demographics and Social Characteristics:

Some researchers categorized the incidence of sexual solicitation, unwanted exposure to pornography, and bullying/harassment according to demographic and gender indicators. According to Mitchell, Finkelhor and Wolak, in their evaluation of the second youth survey ("Online Requests for Sexual Pictures from Youth"), youth who are female, black, have close online relationships, or engage in online sexual behavior are more likely than others to receive solicitations for sexual pictures. In another study ("Trends in Youth Reports"), these same authors, extrapolating survey data, found that black youth and low-income families had experienced an increased incidence of sexual solicitation. Unwanted exposure to pornography had increased among those 10 to 12 years old and 16 to 17 years old, boys, and white, nonHispanic youth. These authors found in another study ("Victimization of Youths on the Internet") that predators had targeted girls for sexual solicitation at almost twice the rate of boys, and youth who were at least 15 years old accounted for nearly two-thirds of incidents of unwanted exposure. They also found that young people at risk for unwanted sexual solicitation, harassment, and exposure to sexual content on the Internet tend to be troubled, older adolescents who use the Internet frequently and engage in high-risk online behavior, although those youth not falling into these categories are at risk as well.

`Ybarra and Mitchell studied the social characteristics of offline and online aggressors. Analyzing the results of the first youth survey (2000), they found that although boys commit most incidents of offline harassment, the number of boys and girls who use the Internet to harass their peers is almost equal. Both offline bullies and youth who harass others online often have multiple psychosocial issues: 51 percent of all bullies had been victims of traditional bullying, 44 percent had a poor relationship with their caregiver, 37 percent showed a pattern of delinquency, and 32 percent were frequent substance abusers. These same authors, in "Exposure to Internet Pornography among Children and Adolescents," found that the majority of youth who reported seeking pornography online and offline were male; only 5 percent of females reported having looked for pornography. The majority (87 percent) of those who reported having sought sexual images were older than 14.

Law Enforcement:

Researchers studied the role that law enforcement can play in prosecuting online predators and evaluated the effectiveness of their investigations. Brown, in his guide for prosecutors seeking to prosecute online predators, recommends that law enforcement officers acquire probative evidence against the perpetrator, collecting and preserving all evidence of grooming (preparing children for sexual exploitation), such as pornography, Web cameras, and other electronic equipment, in order that prosecutors can present the evidence at trial to show the perpetrator's motivation. Mitchell, Wolak, and Finkelhor, in

"Police Posing as Juveniles Online to Catch Sex Offenders," used data from the National Juvenile Online Victimization (NJOV) Study to evaluate the effectiveness of proactive online investigations, in which police investigators use the Internet—posing as minors and often assuming a different gender—to communicate via chat rooms, e-mail, and instant messaging, to interdict youth enticement and child pornography. These investigations were used in 25 percent of all arrests for Internet crimes against children, and resulted in offenders entering pleas in 91 percent of cases. Melissa Wells, along with Finkelhor, Wolak, and Mitchell, used the results of the NJOV Study to highlight two problems faced by law enforcement agencies in making arrests for child pornography: the nature of the child pornography portrayed in the confiscated images may not fit the definitions of existing statutes, and investigators may not be able to determine the age of the children in the images with certainty.

Other problems in law enforcement are discussed in the U.S. House Energy and Commerce Committee staff report. Researchers found that although law enforcement agencies at the state level prosecute 70 percent of all cases involving sexual exploitation of children over the Internet, there is a wide discrepancy among state criminal codes in their treatment of these offenses and in their sentencing practices. Encryption methods, such as anonymizers, significantly interfere with law enforcement's ability to investigate and bring charges against offenders.

Impact of Internet Crimes

Most of the research on Internet crimes against children has focused on quantifying the prevalence of illegal activities and identifying ways of preventing future activities. However, a few researchers have attempted to assess the psychological impact these activities have on young persons, as well the implications for other criminal activity. For example, Cameron and Salazar, in their study of adolescents ages 14 to 17 who regularly use the Internet, determined that both boys and girls reported their perception that exposure to sexually explicit material had no effect on their personal views of either gender or of relationships. Similarly, Sabina, Wolak, and Finkelhor found in their study of college students that only a minority reported that viewing online pornography before the age of 18 had strongly affected their attitudes or emotions about sexuality. On the other hand, Greenfield, who studied the unintended exposure of young people to pornography through peer-to-peer file-sharing networks, concludes that evidence supports the thesis that pornography and sexualized material can influence the moral values, sexual activity, and sexual attitudes of children and youth, including their attitudes toward sexual violence. Neil Malamuth and Mark Huppin studied the relationship between pornography and child molestation. They found that although child molesters (individuals who commit sexual acts against children) use pornography to groom potential victims, pedophiles (individuals who are sexually aroused by children) are less likely to molest a child after viewing pornography. The researchers conclude that whether exposure to a real or virtual child affects a person's behavior depends on a number of risk factors, and that, therefore, no strong cause and effect exists between viewing child pornography and committing sexual molestation of a child. Michael Bourke and Andres Hernandez, in a very recent study on the relationship between the viewing and collection of child pornography and the commission of a sexual contact crime against a child, reach a different conclusion. The results of their research indicated that following participation in a treatment program, child pornography offenders admitted to a significantly greater number of sexual abuse crimes than before they were sentenced.

Persons in this study group who had used the Internet to access child pornography were also significantly more likely to have committed a sexual contact crime. The authors conclude that persons using the Internet to commit child pornography offenses may also be undetected child molesters.

Sources for Annotated Bibliography Executive Summary

Berson, Ilene R. "Grooming Cybervictims: The Psychological Effects of Online Exploitation for Youth." Journal of School Violence 2, no. 1 (2003): 9–18. http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf (accessed March 20, 2009).

Bourke, Michael L., and Andres E. Hernandez. "The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders." Journal of Family Violence 24, no. 3 (April 2009): 183–93.

Brown, Duncan. "Developing Strategies for Collecting and Presenting Grooming Evidence in a High Tech World." Update (National Center for Prosecution of Child Abuse), 2001, 1. http:www.ndaa.org/publications/newsletters/update_volume_14_number_11_2001.html (accessed March 24, 2009).

Cameron, Kenzie A., and Laura F. Salazar. "Adolescents' Experience with Sex on the Web: Results from Online Focus Groups." Journal of Adolescence 28, no. 4 (2005): 535–40.

Cho, Chang-Hoan, and Hongsik John Cheon. "Children's Exposure to Negative Internet Content: Effects of Family Context." Journal of Broadcasting and Electronic Media 49, no. 4 (December 2005). http://findarticles.com/p/articles/mi_m6836/is_4_49/ai_n25120984/ (accessed May 2009).

Dombrowski, Stefan C., Karen L. Gischlar, and Theo Durst. "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet." Child Abuse Review 16, no. 3 (2007): 153–70.

Greenfield, Patricia M. "Inadvertent Exposure to Pornography on the Internet: Implications of Peer-to-Peer File-Sharing Networks for Child Development and Families." Applied Developmental Psychology 25 (2004): 741–50.

Huang, Wilson, Mathew Earl Leopard, and Andrea Brockman. "Internet Child Sexual Exploitation: Offenses, Offenders, and Victims." In Crimes of the Internet, edited by Frank Schmalleger and Michael Pittaro, 43–65. Upper Saddle River, NJ: Pearson Education, 2009.

Internet Safety Technical Task Force. "Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States." Report, Internet Safety Technical Task Force, Berkman Center for Internet and Society, Harvard University, Cambridge, MA, December 31, 2008. http://cyber.law.harvard.edu/pubrelease/isttf/ (accessed January 5, 2009).

Kowalski, Robin M., and Susan P. Limber. “Electronic Bullying Among Middle School Students.” Journal of Adolescent Health 41, no. 6 (2007): S22–S30. http://www.wctlaw.com/CM/Custom/Electronic%20Bullying%20Among%20Middle%20School% 20Students.pdf (accessed March 24, 2009).

Lenhart, Amanda. “Cyberbullying and Online Teens.” Research Memo, Pew/Internet and American Life Project, Pew Research Center, Washington, DC, June 27, 2007. http://www.pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying% 20Memo.pdf.pdf (accessed March 23, 2009).

Malamuth, Neil, and Mark Huppin. “Drawing the Line on Virtual Child Pornography: Bringing the Law in Line with the Research Evidence.” New York University Review of Law and Social Change 31 (2006–2007): 773–827.

McQuade, Samuel C., III, and Neel Sampat. “Survey of Internet and At-Risk Behaviors: Undertaken by School Districts of Monroe County, New York, May 2007 to June 2008 and October 2007 to January 2008.” Report, Center for Multidisciplinary Studies, Rochester Institute of Technology, Rochester, New York, June 18, 2008.

Moessner, Chris. “Cyberbullying.” Trends and Tudes, April 2007, 1–4. http://www.harrisinteractive.com/news/newsletters/k12news/HI_TrendsTudes_2007_v06_i04.pdf (accessed March 23, 2009).

Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?” Sexual Abuse: A Journal of Research and Treatment 17, no. 3 (July 2005): 241–67. http://www.unh.edu/ccrc/pdf/CV82.pdf (accessed March 28, 2009).

Roban, Whitney. “The Net Effect: Girls and New Media.” Executive Summary, Girl Scout Research Institute, Girl Scouts of the United States of America, New York, 2002. http://www.girlscouts.org/research/pdf/net_effect.pdf (accessed March 20, 2009).

Sabina, Chiara, Janis Wolak, and David Finkelhor. “Rapid Communication: The Nature and Dynamics of Internet Pornography Exposure for Youth.” CyberPsychology and Behavior 11, no. 6 (2008): 691–93.

Strom, Paris S., and Robert D. Strom. “Cyberbullying by Adolescents: A Preliminary Assessment.” Educational Forum 70, no. 1 (Fall 2005): 21–36.

Wells, Melissa, David Finkelhor, Janis Wolak, and Kimberly J. Mitchell. “Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession.” Police Practice and Research 8, no. 3 (July 2007): 269–82.

Wolak, Janis, David Finkelhor, and Kimberly J. Mitchell. “Internet-Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study.” Journal of Adolescent Health 35, no. 5 (2004): 11–20. http://www.unh.edu/ccrc/pdf/CV71.pdf (accessed March 23, 2009).

CYBER HARASSMENT:

Cyber Harassment is the use of electronic communications to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm. Unlike physical harassment involving face-to-face contact, cyber harassment uses electronic devices, which entails verbal, sexual, emotional or social abuse of a person, group or organization. The cyber harasser's objective is to exert power and control over the targeted victim(s).

Cyber Harassment is normally executed via harassing emails, instant or text messages, or social media posts, or even creating websites for the sole purpose of tormenting the victim.

When minors are involved, Cyberbullying is the term describing Cyber Harassment and when direct or implied physical harm to the targeted victim(s) is involved, Cyber Harassment becomes Cyberstalking. Albeit, whether Bullying, Harassment, or Stalking, one thing is for certain: the repeated behavior demonstrates a definitive intent to harm, and should be treated very seriously.

CYBER BULLYING:

Cyberbullying has become increasingly common, especially among teenagers. Harmful bullying behavior can include posting rumors about a person, threats, sexual remarks, disclose victims' personal information, or pejorative labels (i.e., hate speech). Awareness in the United States has risen in the 2010s, due in part to high-profile cases.[6][7] Several states in the US and in other countries have laws specific to regulating cyberbullying.[8] These laws can be designed to specifically target teen cyberbullying, while others use laws extending from the scope of physical harassment.

CYBERSTALKING:

Cyberstalking is the next phase of Cyber Harassment and Cyber Bullying, which involves incessant and constant taunting of implied or actual physical threats. Cyberstalking is a criminal act in many states and continues to grow as a national problem.

Cyberstalking Statistics

As people begin to rely more and more on technology, the incidences of cyberstalking increase. Law enforcement and government agencies continue to study the crime in order to learn how to better deter criminals from engaging in this crime of control, fear, and intimidation. The national advocacy group Survivors in Action admit that cyberstalking statistics are often difficult to come by, as a great deal of this activity goes unreported. However, noteworthy data worth observing is as follows:

1. The majority of cyberstalking victims are between 18 and 29 years of age.

2. Roughly 56 percent of cyberstalkers are male

3. Women make up 60 percent of victims

4. In over 70 percent of cyberstalking cases, the victim and perpetrator live in different states

5. Nearly 50 percent of cyberstalkers are the victim's ex, and 15 percent are an online acquaintance of the victim

6. More than 30 percent of cyberstalking attacks begin on Facebook, or through email

7. Over half of cyberstalking victims are single, and 31 percent are married

8. Caucasian people are 10 times more likely to be targeted for cyberstalking than people of other ethnicities

Cyberstalking Laws

Laws governing stalking, harassment, and slander, as well as specific "cyberstalking" laws, vary by state, and might include a series of acts that might not be considered illegal under other circumstances. Stalking is a form of emotional assault, and cyberstalking, also referred to as "cyberbullying," is a high-tech method of inflicting more pain.

The Violence Against Women Act of 2000 placed cyberstalking under the prevue of federal law in the U.S. While many people find cyberstalking laws to be inadequate, state and federal legislatures point out that cyberstalking laws are fairly new and, as technology continues to grow and improve, so do the laws. Although specific laws vary, cyberstalking laws make it clear that this type of harassment is a criminal offense. A conviction for cyberstalking may result in a restraining order being issued, imprisonment, probation, fines, and restitution.

Forms of Cyberstalking:

Cyberstalking cases differ from regular stalking in that it is technologically based, though some cyberstalkers escalate their harassment to include physical stalking as well. A cyberstalker acts of out of anger, or a need to control, or gain revenge over another person through threats, fear, and intimidation. There are several forms of cyberstalking, including:

1. Harassing the victim

2. Embarrassing and humiliating the victim

3. Exerting financial control by emptying the victim's bank accounts, or by ruining his credit

4. Isolating the victim by harassing his family, friends, and employer

5. Frightening the victim by using scare tactics and threats

Identifying Cyberstalking

It is sometimes difficult for a person who is being harassed or stalked to realize the situation is a criminal act that should be reported to the authorities. In deciding whether a situation is truly stalking, the victim should consider whether the perpetrator is acting with malice and premeditation. Stalking activities are often a repetitive, obsession-based vendetta, directed personally at the victim. This behavior continues even when the victim has personally warned the perpetrator to stop.

Key factors to identifying cyberstalking cases include:

1. False accusations. A cyberstalker often tries to damage the reputation of his victim by posting false information on social media websites or blogs. A perpetrator may even create fictitious websites or other accounts for the purpose of spreading false rumors and allegations about the victim.

2. Gathering information about the victim. A cyberstalker may try to gather as much information as possible about the victim by interacting with the victim's friends, family, and colleagues. In serious cases, a cyberstalker may hire a private investigator.

3. Monitoring victim's activities. A cyberstalker may attempt to trace his victim's IP address, or hack into the victim's social media accounts and emails to learn about his online activities.

4. Encouraging others to harass the victim. The offender may encourage the involvement of third parties to harass the victim.

5. False victimization. It is not uncommon for a cyberstalker to claim the victim is harassing him, taking the position of victim in his own mind.

Protecting Yourself Against Cyberstalking

The U.S. Department of Justice has issued recommendations for people who believe they are victims of cyberstalking. The first step should be to demand the stalker to stop all contact, and stop the harassing actions. Additionally, in order to facilitate prosecution of the perpetrator, the victim should:

1. Save all emails, messages, and other communications for evidence. It is vital that these are not altered in any way, and that the electronic copies are kept, rather than only printouts.

2. Save all records of threats against the victim's safety or life. This includes any written or recorded threats, and logs of the date, time, and circumstances of verbal threats.

3. Contact the perpetrator's internet service provider. Internet service providers (ISP) prohibit their users from using their service to harass others. Contacting the ISP may result in discontinuation of the harasser's internet service, and will put the ISP on notice to maintain record of the harasser's internet use.

4. Keep detailed records of contact with ISP and law enforcement officials. It is important to keep a log of all reports made to any agency or provider, and to obtain copies of the official reports when available.

Examples of Cyberstalking

A woman contacted police in 2003, claiming someone had given her private information, including her location and her description, to men through a dating service. The woman discovered the act when she was contacted by two different men, each of whom stated they had previously talked with her, and arranged a personal encounter.

Claire began being harassed by strangers after someone made a post on the Internet offering sexual services in her name. The post included private information, including her phone number and home address.

After John and his girlfriend broke up, he began stalking her by planting a prepaid GPS-enabled cell phone under her car. John tracked his ex-girlfriend's movements, and followed her by logging into the cell phone account online. John also called his ex upwards of 200 times a day.

SOURCE: Legal Dictionary: https://legaldictionary.net/cyberstalking/

RANSOMWARE EXTORTION:

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Ransom Prices and Payment

Ransom prices vary depending on the ransomware variant and the price or exchange rates of digital currencies. Thanks to the perceived anonymity offered by cryptocurrencies, ransomware operators commonly specify ransom payments in bitcoins. Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards. It should be noted, however, that paying the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or hostaged files.

Ransomware Infection and Behavior

Users may encounter this threat through a variety of means. Ransomware can be downloaded onto systems when unwitting users visit malicious or compromised websites. It can also arrive as a payload either dropped or downloaded by other malware. Some ransomware are known to be delivered as attachments from spammed email, downloaded from malicious pages through malvertisements, or dropped by exploit kits onto vulnerable systems.

Once executed in the system, ransomware can either lock the computer screen, or, in the case of crypto-ransomware, encrypt predetermined files. In the first scenario, a full-screen image or notification is displayed on the infected system's screen, which prevents victims from using their system. This also shows the instructions on how users can pay for the ransom. The second type of ransomware prevents access to files to potentially critical or valuable files like documents and spreadsheets.

Ransomware is considered "scareware" as it forces users to pay a fee (or ransom) by scaring or intimidating them. In this sense, it is similar to FAKEAV malware, but instead of capturing the infected system or encrypting files, FAKEAV shows fake antimalware scanning results to coax users into purchasing bogus antimalware software.

How Ransomware Attacks Occur

The majority of malware comes in via emails. Many attacks are delivered by mass unsolicited spam with malicious attachments or web links. They are usually delivered opportunistically but over the past year we have seen these emails being localised for New Zealand and designed to look more legitimate.

The second most common way is when you browse the web. Your computer could be infected while surfing compromised websites, malicious websites or downloading infected files. When users unknowingly save malware on the network, more systems are infected.

Protecting yourself from attacks

Obviously the best defense is to stop ransomware from ever being installed. Now would be a great time to ensure that your security is up-to-scratch, with an end-to-end approach including these steps.

1. Ensure you've got email filtering to block emails with ransomware attachments or links to malicious websites. Choose an email provider that provides spam filtering and anti-malware scanning.

2. You also want to have web filtering on your computer or gateway (if you have a network) to protect users when they are browsing the internet by identifying and blocking malicious websites and scanning downloads for malware when browsing the web.

3. Update managed and monitored firewalls with the latest security patches to protect the border between your network and the internet.

4. Anti-virus software on computers and mobile devices are considered your last "line of defense" and will attempt to stop malicious software from being opened or installed. Install supported security software for your device or computer operating system. Always keep it active and current.

5. Educate personnel so that they don't click links or download files from suspicious emails - even if they think they know the person who sent it. Even the websites of reputable companies can be compromised and people should be careful about downloading files and installing software.

6. Keep a backup of the critical data you need for your business so you can quickly recover much of the data encrypted by the attackers. You need a backup program that does versioning - saving older versions of your files. But even those older versions will be useless if the ransomware succeeds in encrypting all the files on your backup drive.

7. Create a response plan and test your restore process so you know what to do if disaster strikes. Think about what other things you might need, like spare computers or on-demand computing for your servers.

Source:

https://www.trendmicro.com/vinfo/us/security/definition/ransomware

http://www.sparklab.co.nz/articles/7-steps-to-prepare-for-a-ransomware-attack

AGENDA:

7:15 a.m. to 7:45 a.m. - **SIGN IN/CONTINENTAL BREAKFAST**

7:45 a.m. to 8:00 a.m. - **Opening Comments by Broward County Crime Commission**

8:00 a.m. to 8:20 a.m. – **BRIDGE Talk Presentation 1: Dennis Nicewander, Assistant State Attorney, Office of the State Attorney, 17th Judicial Circuit Broward County: *Cyberbullying and Internet Crimes Against Children***

8:20 a.m. to 8:50 a.m. - **Presentation 2: Special Agent Matt Fowler, FBI, *Violent Crimes Against Children***

8:50 a.m. to 9:20 a.m. **– Roundtable Discussion One: Pembroke Pines Police Department: *Cutting Edge Digital Forensics***

9:20 a.m. to 9:30 a.m. – **BREAK**

9:30 a.m. to 10:30 a.m. **– Panel Discussion I: *Internet Crimes Against Children***

10:30 a.m. to 11:00 a.m. – **Roundtable Discussion Two: Child Rescue Coalition, *Protecting Innocence through Technology***

11:00 a.m. to 11:10 a.m. – **BREAK**

11:10 a.m. to 12:00 p.m. - **Presentation 3: Kevin O'brien, National Center for Missing and Exploited Children (NCMEC)**

LUNCH – Noon to 1:00 p.m. –

Luncheon Keynote Speaker: 12:20 p.m. to 1:00 p.m. -

Charles 'Brad' Leopard, United States Secret Service

1:00 p.m. to 1:15 p.m. – **BREAK**

1:15 p.m. to 2:00 p.m**. – Presentation 4*:* Dr. Asia Eaton, Florida International University (FIU): *Adult and Workplace Cyber Harassment, Cyber Bullying, Cyber Stalking, & Sextortion***

2:00 p.m. to 2:10 p.m. – **BREAK**

2:10 p.m. to 3:00 p.m**. – Presentation 5: Florin Lazurca, Technical Security Analyst, Citrix Systems: *Ransomware Extortion***

3:00 p.m. to 3:45 p.m. **– Panel Discussion II*:* Identity Theft, Economic Crimes and Electronic Fraud**

Event Finishes NLT 3:45 p.m.

PANEL AND ROUNDTABLE PARTICIPANTS:

Roundtable Discussion One: ***Cutting Edge Digital Forensics***

Mike Silver, *Detective, Pembroke Pines Police Department*

Gordon Angus, *Senior Police Digital Forensics Examiner, Pembroke Pines Police Department*

MODERATOR: **Dr. Michael Brannon**, *Institute for Behavioral Sciences and the Law (IBSL)*

Roundtable Discussion Two: ***Protecting Innocence through Technology***

Caroline Asher Yoost, *Founder and CEO, Child Rescue Coaltion*

E. Desiree Asher, *Managing Director, Child Rescue Coalition*

MODERATOR: **Dr. Lori Butts**, *Clinical & Forensic Institute, Inc.*

Panel Discussion I: ***Internet Crimes Against Children***

Giuseppe Weller, *Detective, Broward Sheriff's Office, South Florida Internet Crimes Against Children Task Force*

Donald Cannon, *Special Agent, Computer Crime Center, Florida Department of Law Enforcement (FDLE)*

Dr. Jill Levenson, *Associate Professor of Social Work, Barry University School of Social Work*

Nancy Mcbride, *Executive Director, Florida Outreach National Center for Missing & Exploited Children (NCMEC)*

Heath E. Graves, *Special Agent, Federal Bureau of Investigation (FBI)*

Adam Granit, *Detective, Davie Police Department*

Neva Rainford Smith, *Assistant State Attorney in Charge (ASAIC), Sexual Battery Unit, Office of the State Attorney, 17th Judicial Circuit, Broward County Florida*

MODERATOR; **Senior Judge Joel Lazarus,** *Advisory Board Member, Broward County Crime Commission*

Panel Discussion II: ***Identity Theft, Economic Crimes and Electronic Fraud***

Scott Mosely, *Detective, Fort Lauderdale Police Department, Economic Crimes*

Scott Hoffer, *Detective, Fort Lauderdale Police Department, Economic Crimes*

Anthony Arena, *Postal Inspector, United States Postal Service*

Kevin Tyrrell, *Assistant Special Agent in Charge (ASAIC), Homeland Security Investigations*

Mark Moretti, *Detective, Miramar Police Department, Economic Crimes*

Jon Garon, *Dean and Professor of Law, Office of the Dean, Shepard Broad School College of Law, Nova Southeastern University*

MODERATOR; Danielle Dudai, *Assistant Statewide Prosecutor, Office of Statewide Prosecution, Office of the Attorney General*

DISTINGUISHED SPEAKERS & PANELISTS

1. **Gordon Angus, Senior Police Digital Forensics Examiner, Pembroke Pines Police Department – Roundtable Discussion One**

   Mr. Angus was retained to implement and administer the Digital Forensics Laboratory for the Pembroke Pines Police Department. In this regard, he mentors detectives involved with technology based, complex investigations. Due to Mr. Angus' efforts, the Pembroke Pines Police Department has also been exceptionally supportive and invaluable in assisting other police departments requiring digital forensic laboratory assistance.

2. **Anthony Arena, Postal Inspector, United State Postal Service – Panel Discussion II**

   The mission of the U.S. Postal Inspection Service is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the U.S. Postal Inspection Service has a proud and successful history of fighting criminals who attack the nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public.

3. **E. Desiree Asher, Managing Director, Child Rescue Coalition – Roundtable Discussion Two**

   Desiree Asher is the Managing Director of Child Rescue Coalition, and she also serves on the Board of Directors. She is a member of Child Rescue Coalition's Champions Club. Desiree is responsible for executing the strategic plan in the areas of marketing and branding, donor relations, corporate partnerships, and fundraising. In 2015 Desiree was honored as a winner of the 40 Under 40 Dealmaker of the Year M&A Advisors award. She is on the Board of Directors for City Harvest in New York City, and she is a member of the Federal Club Council of the Human Rights Campaign. Desiree served with Carly as Co-CEO of TLO, LLC, a technology company that specialized in investigative and child protection tools. Desiree has been with Child Rescue Coalition since inception.

4. **Dr. Michael P. Brannon, Founder, the Institute of Behavioral Sciences and the Law – MODERATOR – Roundtable Discussion One**

   Dr. Michael P. Brannon holds a Bachelor of Science degree in Psychology, a Master of Science degree in Psychology, and a Doctorate degree in Clinical Psychology from Nova University. He was the Clinical Director of The Starting Place, a program for teenagers with substance abuse problems, from 1980 to 1990. He has been licensed as a psychologist in the state of Florida since 1990. He has specialized in the area of forensic psychology since 1994. He is currently the

co-director of the Institute for Behavioral Sciences and the Law in Coral Springs, Florida. He has conducted over 20,000 forensic evaluations and testified as an expert over 1500 times in Federal Court and State Court. He has been featured on numerous television shows including CNN, The Today Show, Erin Burnett OutFront, Forensic Files, Chris Matthews Hardball, The O'Reilly Factor, and Headline News Network.

5. **Lori J. Butts, J.D., Ph.D., President and Director of the Clinical & Forensic Institute – MODERATOR – Roundtable Discussion Two**

Dr. Lori J. Butts is currently the President of Florida Psychological Association. She is also the President and Director of the Clinical and Forensic Institute, with offices in Fort Lauderdale and Lake Worth, Florida. She is a Florida licensed psychologist, with specializations in clinical and forensic psychology; she is also a member of the Florida Bar Association. After graduating from Clemson University with Honors, Dr. Butts received her law and doctoral psychology degrees from the innovative jointly sponsored program by Villanova School of Law and Drexel University Department of Clinical Psychology. She completed her internship in clinical and forensic psychology at New York University School of Medicine, Bellevue Hospital, and Kirby Forensic Psychiatric Hospital.

6. **Donald Cannon, Special Agent, Computer Crime Center, Florida Department of Law Enforcement (FDLE) - Panel Discussion II**

The Florida Department of Law Enforcement (FDLE) promotes public safety and strengthens domestic security by providing services in partnership with local, state, and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE is composed of five areas: Executive Direction and Business Support, Criminal Investigations and Forensic Science, Criminal Justice Information, Criminal Justice Professionalism and Florida Capitol Police. In addition, the department formally coordinates boards, councils, and commissions. FDLE employs about 1,700 members statewide

7. **Danielle Dudai, Assistant Statewide Prosecutor, Office of Statewide Prosecution, Office of the State Attorney General – MODERATOR - Panel Discussion II**

Danielle Dudai is an Assistant Statewide Prosecutor for the Office of the Attorney General. She has been a prosecutor since 2010, previously serving at the Office of the State Attorney in Broward County. As a prosecutor, she founded the Human Trafficking prosecution unit at the Broward State Attorney's Office, acting as the sole dedicated prosecutor to the prosecution of Human Trafficking Offenses falling in Broward County's jurisdiction. Currently, Ms. Dudai works on large-scale organized crime cases, spanning large jurisdictions across the state of Florida.

8. **Dr. Asia Eaton, Florida International University (FIU): Adult and Workplace Cyber Harassment, Cyber Bullying, Cyber Stalking, & Sextortion – Presentation 5**

Dr. Asia Eaton received a Ph.D. in Social Psychology with a minor in Statistics from the University of Chicago, and is currently an Assistant Professor in Psychology at Florida International University (FIU). She is a core faculty member in both the Developmental Psychology Program and the I-O Psychology Program at FIU, and supervises Ph.D. students in both programs. Her research examines how gender and social power interact and support one another in intimate partner relationships and in the workplace, and how gender intersects with race, sexuality, and age. Dr. Eaton is the recipient of the 2016 Michele Alexander Early Career Award for Scholarship and Service from the Society for the Psychological Study of Social Issues, has won FIU's most prestigious faculty award for undergraduate advising and mentorship, and has received teaching awards from FIU and the University of Chicago. She also serves as Head of Research for Cyber Civil Rights Initiative (CCRI), which is working to understand and end the emerging epidemic of non-consensual porn in the U.S., and is working with leadership at Lotus House to better understand the needs of women experiencing homelessness.

9. **Matt Fowler, Federal Bureau of Investigation (FBI), Violent Crimes Against Children – Presentation 2**

Special Agent Matthew Fowler is currently assigned to the Crimes Against Children Squad for the Federal Bureau of Investigation (FBI) in the Miami Division. In this capacity, Special Agent Fowler works to investigate those who prey on children online. In addition, Special Agent Fowler is a member of the FBI's National Child Abduction Rapid Deployment Team, which responds to incidents of missing children nationwide. Special Agent Fowler also regularly conducts internet safety presentations for the community. Prior to joining the FBI in 2009, Special Agent Fowler served as a Police Officer and Detective with the Independence, Missouri Police Department. In total, Special Agent Fowler has more than 14 years of law enforcement experience.

10. **Carol Fredrick, Resident Special Agent in Charge, Florida Department of Law Enforcement (FDLE) – Panel Discussion II**

The Florida Department of Law Enforcement (FDLE) promotes public safety and strengthens domestic security by providing services in partnership with local, state, and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE is composed of five areas: Executive Direction and Business Support, Criminal Investigations and Forensic Science, Criminal Justice Information, Criminal Justice Professionalism and Florida Capitol Police. In addition, the department formally coordinates boards, councils, and commissions. FDLE employs about 1,700 members statewide

11. Jon Garon, Dean and Professor of Law, Office of the Dean, Shepard Broad School College of Law, Nova Southeastern University – Panel Discussion II

Jon M. Garon is dean of Nova Southeastern University Shepard Broad College of Law. Dean Garon serves as chief academic officer for the law school, providing strategic leadership on programming, curriculum, enrollment management, marketing, and finance. He is a nationally recognized authority on technology law and intellectual property, particularly copyright law, entertainment and information privacy. A Minnesota native, he received his bachelor's degree from the University of Minnesota in 1985 and his juris doctor degree from Columbia University School of Law in 1988. Prior to joining Nova Southeastern University in 2014, Garon was the inaugural director of the Northern Kentucky University Salmon P. Chase College of Law, Law + Informatics Institute from 2011-2014. The Law + Informatics Institute serves to integrate the specialized programming on technology and information systems as they apply across legal disciplines. A tenured member of the law faculty, Garon taught Information Privacy Law, Cyberspace Law, Copyright Law, Entertainment Law, and related courses. Garon served as dean and professor of law at Hamline University School of Law in St. Paul, Minnesota. He was professor of law from 2003 to 2011, dean of the Law School from 2003 to 2008 and Interim Dean of the Graduate School of Management from 2005 to 2006. Before Hamline, Garon taught Entertainment Law and Copyright at Franklin Pierce Law Center in Concord, New Hampshire and Western State University College of Law in Orange County, California. Among his numerous accomplishments, Garon has held key leadership positions as past chair of both the American Bar Association's Law School Administration Committee and the Association of American Law Schools Section on Part-Time Legal Education. His teaching and scholarship often focus on business innovation and structural change to media, education and content-based industries. He is the author of three books and numerous book chapters and articles, including The Independent Filmmaker's Law & Business Guide to Financing, Shooting, and Distributing Independent and Digital Films (A Cappella Books, 2d Ed. 2009); Own It – The Law & Business Guide to Launching a New Business Through Innovation, Exclusivity and Relevance (Carolina Academic Press 2007); and Entertainment Law & Practice (2d Ed. 2014 Carolina Academic Press). Additionally, he has presented at more than 60 forums across the U.S.

12. Adam Granit, Detective, Davie Police Department – Panel Discussion I

Detective Adam Granit is a veteran investigator with the Criminal Investigations Unit of the Davie Police Department. The Davie Police Department Investigations Bureau is comprised of the Person Crimes Division, Property Crimes Division, Special Investigations Division, Victim Advocate, Crime Analysis, Crime Scene Unit and the Missing Persons Unit. The Person Crimes Division handles a variety of criminal investigations, including: homicide, sexual assault, robbery, etc. They are also responsible for identifying and tracking sexual predators and sexual offenders.

13. Heath E. Graves, Special Agent, Federal Bureau of Investigation (FBI) – Panel Discussion I

The mission of the FBI's Violent Crimes Against Children program is threefold: first, to decrease the vulnerability of children to sexual exploitation; second, to develop a nationwide capacity to provide a rapid, effective, and measured investigative response to crimes against children; and third, to enhance the capabilities of state and local law enforcement investigators through programs, investigative assistance, and task force operations.

14. Scott Hoffer, Detective, Fort Lauderdale Police Department, Economic Crimes – Panel Discussion II

Detective Scott Hoffer is part of the Fort Lauderdale Police Department's Economic Crimes Unit. The Economic Crimes Unit is responsible for investigating the offenses of fraud, embezzlement, identity theft and arson. Members of the unit are also assigned to a federal fraud task force sponsored by the US Secret Service. Detectives work closely with the State Attorney's Office to determine if an offense is criminal or civil in nature. Investigators also work with members of the business community to assist other detectives in cases where financial data has been taken during another offense and used fraudulently. Since many of these offenses cross multiple jurisdictions, members of this unit work cooperatively with other municipal, state and federal law enforcement investigators.

15. Senior Judge Joel Lazarus, 17th Judicial Circuit Court of Florida (Broward County) – MODERATOR - Panel Discussion I

Senior Judge Joel Lazarus, a graduate with High Honors from the Charter Class of Nova Law in 1977 spent the next sixteen years as an Assistant State Attorney. In 1993, Lazarus was appointed to the County Court Bench by the late Lawton Chiles. Until 2010, he served as a County Court Judge and Acting Circuit Court Judge, where he presided over in excess of 900 criminal jury trials. He retired on June 30, 2010 and returned the next day as a Senior Judge, He continued to try criminal cases until assigned four years ago to the Foreclosure Division. He also holds a B.S. degree from Babson College and an M.B.A. from Columbia University Graduate School of Business. He lives in Davie, is married with three sons, a daughter, has five grandchildren, and an adorable Maltese named after Dustin Pedroia, the Red Sox second baseman. In 2010, he was awarded the Outstanding Judge in Florida by his peers, an award from Florida Law Related Education Association for his leadership in education. He is on the faculty of the Florida Prosecutor-Public Defender Trial Advocacy Training Program (for over 22 years) at the University of Florida Law School. Lazarus is Chairman of the Advisory Board, Broward County Crime Commission.

16. Florin Lazurca, Citrix Systems: Ransomware Extortion - Presentation 4

Florin Lazurca is a Technical Security Strategist at Citrix. Florin drives technical direction for solutions that enhance user experience, flexibility, and security. His background includes being an Information Technology

Architect in network optimization, virtualization, and security. He was most recently responsible for managing a team of network and security systems engineers to protect networks, applications, and data for diverse companies and organizations. He is passionate about Information Systems security, and has amassed a wide range of knowledge in security tools, technologies, and best practices based on his experience.

17. **Charles "Brad" Leopard, Supervisor; Miami Electronic Crimes – Task Force Forensic Laboratory, United States Secret Service – LUNCHEON KEYNOTE SPEAKER**

Brad Leopard supervises the United States Secret Service Miami Electronic Crimes Task Force. Brad has more than fifteen years of experience working cyber investigations and conducting digital forensic examinations. Brad previously instructed computer forensic classes for federal and state law enforcement agencies and managed incident response for large data breach investigations. Brad received a Master's Degree in Cyber Systems and Operations from Naval Postgraduate School.

18. **Dr. Jill Levenson, Associate Professor of Social Work, Barry University School of Social Work – Panel Discussion I**

Dr. Jill Levenson, PhD, LCSW, Professor of Social Work, is a SAMHSA-trained internationally recognized expert in trauma-informed care. She has published over 100 articles about policies and clinical interventions designed to prevent repeat sexual offending, including projects funded by the National Institutes of Justice and the National Sexual Violence Resource Center. Her groundbreaking research on the link between childhood adversity and sexually abusive behavior has paved the way for innovations in treatment programs that now utilize a trauma-informed approach. She has also been a clinician for over 30 years, using a scientist-practitioner model to inform both her research and her work with survivors, offenders, and families impacted by sexual abuse. She has been invited to present as a keynote speaker about trauma-informed care in clinical, correctional, and forensic settings in Wisconsin, Virginia, Pennsylvania, New Jersey, Florida, Idaho, Oregon, Michigan, Massachusetts, Vermont, Maryland, Colorado, New York, Minnesota, Canada, New Zealand, and Australia. Dr. Levenson has co-authored four books about the treatment of sexual abuse, including the recently released book: Trauma Informed Care: Transforming treatment for people who have sexually abused, co-authored with Gwenda Willis and David Prescott, and published by Safer Society Press.

19. **Nancy McBride, Executive Director, Florida Outreach National Center for Missing & Exploited Children (NCMEC) – Panel Discussion I**

Nancy A, McBride is the Executive Director, Florida Outreach, for the National Center for Missing & Exploited Children (NCMEC). Since 1984, NCMEC has served as the national clearinghouse and resource center for families, victims, private organizations, law enforcement and the public on issues relating to missing and sexually exploited children. The NCMEC mission is to

help find missing children, reduce child sexual exploitation, and prevent child victimization.

20. Mark Moretti, Detective, Miramar Police Department, Economic Crimes – Panel Discussion II

Detective Moretti is a former Detective of the Year recipient of the Broward County Crime Commission. His core competency of Economic Crime and the nuances associated with it are unparalleled. The Miramar Police Department considers itself to be an industry leader in professionalism. Miramar has repeatedly been recognized with accreditation by CFA – The Commission for Florida Law Enforcement Accreditation and CALEA – The Commission on Accreditation for Law Enforcement Agencies. In 2017, Miramar Police Department was awarded "Meritorious" accreditation which is the highest level of international accreditation possible, given only to those agencies that have shown an excellence in professionalism and quality assurance for more than 15 years.

21. Scott Mosely, Detective, Fort Lauderdale Police Department, Economic Crimes – Panel Discussion II

Detective Scott Moseley is part of the Fort Lauderdale Police Department's Economic Crimes Unit. The Economic Crimes Unit is responsible for investigating the offenses of fraud, embezzlement, identity theft and arson. Members of the unit are also assigned to a federal fraud task force sponsored by the US Secret Service. Detectives work closely with the State Attorney's Office to determine if an offense is criminal or civil in nature. Investigators also work with members of the business community to assist other detectives in cases where financial data has been taken during another offense and used fraudulently. Since many of these offenses cross multiple jurisdictions, members of this unit work cooperatively with other municipal, state and federal law enforcement investigators.

22. Dennis Nicewander, Broward State Attorney's Office: Cyberbullying and Internet Crimes Against Children - BRIDGE Talk Presentation 1

Dennis Nicewander graduated from Wake Forest University Law School in 1987. He has been an Assistant State Attorney for the 17th Judicial Circuit in Broward County, Florida since 1987. After prosecuting a variety of criminal cases for three years, he was assigned to the Sex Crimes/Child Abuse Unit in 1990, where he successfully prosecuted numerous high profile cases. In 1998, Broward County was awarded one of the initial Internet Crimes Against Children grants where Dennis got involved immediately. Since that time, he has been the prosecutor assigned to the ICAC Task Force and provides legal guidance to law enforcement throughout the Task Force's jurisdiction of over 5 million people. He has participated in hundreds of technology-facilitated investigations and successfully prosecuted over 400 ICAC cases. Dennis has lectured on various cybercrime issues for organizations throughout the United States. He publishes his own website, www.locatethelaw.org , which provides legal resources related to sex crimes and cybercrime issues. He is married and is the father of two children.

23. Kevin O'brien, National Center for Missing and Exploited Children (NCMEC) - Presentation 3

Kevin O'Brien is a Supervisor in the Exploited Children Division (ECD) at the National Center for Missing and Exploited Children (NCMEC). In this capacity, he is responsible for managing a staff of approximately 37 analysts and support personnel. Mr. O'Brien has handled over 70,000 CyberTipline reports, resulting in numerous arrests of child sexual offenders. He has participated in various law enforcement investigative training programs on high technology crimes, online child sexual exploitation, and investigative and analytical skills development. He has provided extensive technical assistance to law enforcement in the United States, as well as abroad, on cases of child sexual exploitation, especially Internet crimes against children.

24. Mike Silver, Detective, Pembroke Pines Police Department – Roundtable Discussion One

Detective Silver is a member of the South Florida Internet Crimes Against Children task force. The South Florida Internet Crimes Against Children (SFLICAC) Task Force, formerly known as the LEACH (Law Enforcement Against Child Harm) Task Force, is a multi agency and multi jurisdictional effort to combat the on-line enticement of children and teenagers. The SFLICAC is comprised of law enforcement and judicial officials that encompass the Federal, State and Local Law Enforcement agencies. It is this robust partnership that affords a succinct and comprehensive strategy required to enforce and suppress the illegal use of the Internet.

25. Neva Rainford Smith, Assistant State Attorney in Charge (ASAIC), Sexual Battery Unit, Office of the State Attorney, 17th Judicial Circuit, Broward County Florida - Panel Discussion I

Neva Rainford-Smith, is a 12-year veteran of the Broward State Attorney's Office and is the newly appointed Assistant State Attorney-in-Charge of SAO's Sexual Battery Unit. Rainford-Smith is a graduate of Nova University and Nova's Shepard Broad Law Center. She joined the State Attorney's Office in 2001 and has held a series of key positions. Ms.Rainford-Smith worked in the Misdemeanor Trial Unit for a year before beginning athree-year stint in the Felony Trial Unit. In the mid-2000s, she prosecuted cases in theSexual Battery Unit, then became a supervisor in the Felony Trial Unit handling fourfelony divisions and specializing in DUI manslaughters and vehicular homicides.In 2011, she worked in the Career Criminal Unit, then spent a year in Homicide before being appointed head of SAO's Sexual Battery Unit this past summer. She also has served on SAO's Office Hiring Committee and has been an Attorney Mentor for both misdemeanor and felony trial attorneys. Ms. Smith is the recipient of the Broward County Crime Commission's 2013 Prosecutor of the Year Award.

26. Kevin Tyrrell, Assistant Special Agent in Charge (ASAIC), Homeland Security Investigations – Panel Discussion II

Mr. Tyrrell is a U.S. Immigration and Customs Enforcement (ICE) Supervisory Special Agent, and an Assistant Special Agent in Charge for the Miami Division of Homeland Security Investigation. HSI has broad legal authority to enforce a diverse array of federal statutes. It uses this authority to investigate all types of cross-border criminal activity, including: Financial crimes, money laundering and bulk cash smuggling; Commercial fraud and intellectual property theft; Cybercrimes; Human rights violations; Human smuggling and trafficking; Immigration, document and benefit fraud; Narcotics and weapons smuggling/ trafficking; Transnational gang activity; Export enforcement; and, International art and antiquity theft. The threats presented by criminals in these areas have far-reaching consequences. In response, HSI uses a versatile approach in its operations so that it can achieve the best results for the nation and its citizens.

27. Giuseppe Weller, Sergeant, Broward Sheriff's Office, South Florida Internet Crimes Against Children Task Force – Panel Discussion II

Sergeant Weller is a member of the South Florida Internet Crimes Against Children task force. The South Florida Internet Crimes Against Children (SFLICAC) Task Force, formerly known as the LEACH (Law Enforcement Against Child Harm) Task Force, is a multi agency and multi jurisdictional effort to combat the on-line enticement of children and teenagers. The SFLICAC is comprised of law enforcement and judicial officials that encompass the Federal, State and Local Law Enforcement agencies. It is this robust partnership that affords a succinct and comprehensive strategy required to enforce and suppress the illegal use of the Internet.

28. Caroline Asher Yoost, Founder and CEO, Child Rescue Coalition – Roundtable Discussion Two

Carly is a former Co-CEO of TLO, LLC, a data solutions provider founded by her father, Hank Asher, and specializing in custom, scalable investigative and risk management tools for due diligence, threat assessment, identity verification, fraud prevention and debt recovery. TLO enhanced and supported the child protection technology and systems used currently by Child Rescue Coalition, Inc. In late 2013 when TLO was acquired by TransUnion Risk and Alternative Data Solutions, Inc., Carly and her sister, Desiree Asher, acquired the protection technology and founded Child Rescue Coalition, Inc. to continue the work of protecting children. Carly now supports our mission by managing and directing our entire operations. After spending her younger days in Florida and North Carolina, Carly graduated with a bachelor's degree in psychology magna cum laude from Florida Atlantic University. She is a philanthropist who enjoys helping others and supports numerous charities. Recreation for her includes arts and crafts and traveling with her husband.

The Broward County Crime Commission would like to render special thanks to its Community Partners

DoubleTree by Hilton, Deerfield Beach

Mark Graphics

Terry Duffy Audio Visual and Disc Jockey (DJ) Services

THANK YOU!

www.BrowardCrime.org

"Evil Triumphs When Good People Stand Idly By"

10640 Northwest 32nd Street, Sunrise, FL 33351; TEL: (954) 746-3117; FAX: (954) 572-7988; EMAIL: info@browardcrime.org