

Abstract:

Throughout the world, public and private entities have been challenged to quickly develop new techniques to address cybercrime. The Washington State Attorney General's Office is known as a national leader in efforts to fight high-tech crimes. Washington was one of the first states to adopt a law explicitly prohibiting spyware activities and imposing serious penalties on violators. Success depends on well-crafted legislation, adequate resources, partnerships, support for law enforcement, and consumer and business education.

Bio:

Rob McKenna was elected Washington state's 17th attorney general and assumed office in 2005. As the state's chief legal officer, he directs 500 attorneys and nearly 700 professional staff who provide legal services to state agencies, boards and commissions. He began his law career in 1988 at Perkins Coie, one of the nation's top 50 law firms. McKenna was elected to the Metropolitan King County Council in 1995 then re-elected twice without opposition. He received his law degree from the University of Chicago Law School and earned bachelor's degrees in economics and international studies, both with honors, from the University of Washington, where he was student body president and graduated Phi Beta Kappa. He is a member of the second class of Aspen-Rodel Fellowships in Public Leadership, designed to bring together the best of the nation's emerging leaders to discuss broad issues of democratic governance and effective public service.

Fighting Cybercrime – A Perspective from the Washington State Attorney General

Rob McKenna

Washington State Attorney General

<http://www.atg.wa.gov>

While the Internet has revolutionized the way much of the world communicates and conducts business, it has also enabled a dramatic rise in crimes that exploit this technology.

Throughout the world, public and private entities have been challenged to quickly develop new techniques to address cybercrime including financial fraud, child exploitation, harassment, trade secret theft and the spread of destructive malware.

RISE OF CYBERCRIME

An estimated 75 percent of adults and 90 percent of teenagers in the United States use the Internet¹. With so many families, government entities and businesses online, the corresponding rise in cybercrime poses a serious threat to public safety, our economy and national security.

The true impact of cybercrime in the U.S. is unknown because incidents are not always reported or detected. Available industry studies reveal a substantial increase in illegal activity, including:

- Spam - Postini collected more than 60 billion pieces of spam between September 2006 and March 2007, totaling 537.7 terabytes of data. The company reported a 65 percent increase in spam since January 2002.²
- Bot-infected computers – Symantec observed 63,912 infected computers per day over five months in 2005, up 11 percent from the previous reporting period.³
- Trojan horse attacks – 2 million of the 4 million computers cleaned by Microsoft's malicious software removal tool between January and June 2006 were infected by at least one backdoor Trojan horse. In the same timeframe, 43,000 new variants of malware were found. The financial services industry suffered almost 40 percent of all Trojan attacks last year, according to Counterpane.⁴
- Keyloggers: The Anti-Phishing Working Group (APWG), an industry association, reported that the number of sites hosting keylogging crimeware rose to 3,362 in January

¹ Pew Internet and American Life Project, February 2008, www.pewinternet.org

² "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," GAO-07-705, U.S. Government Accountability Office, June 2007, www.gao.gov

³ "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," GAO-07-705, U.S. Government Accountability Office, June 2007, www.gao.gov

⁴ "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," GAO-07-705, U.S. Government Accountability Office, June 2007, www.gao.gov

2008, while the number of unique keylogger crimeware variants reached a new high of 364.⁵

- Phishing – APWG detected 299,307 unique URLs during 2007 and noted the U.S. remains the top country hosting phishing sites with 37 percent of all such sites. More than 55 percent of the world’s phishing attacks fabricate company Web sites hosted in the U.S., IBM reported.⁶
- Viruses - 38 percent of individuals included in a survey by Consumer Reports reported a computer-virus infection in the past two years, and 34 percent reported a spyware infection in the past six months. Virus infections prompted 1.8 million households to replace their PCs in the past two years and 850,000 replaced their PCs in the past six months because of spyware infections.⁷

Both businesses and consumers bear the sting of these crimes:

- The Internet Crime Complaint Center referred more than 90,000 complaints to law enforcement in 2007, amounting to nearly \$239.09 million in losses⁸.
- U.S. consumers lost an estimated \$7.2 billion due to viruses, spyware and phishing in 2006.⁹
- U.S. organizations lost an estimated \$67.2 billion because of computer crime in 2005.¹⁰
- A survey of U.S. businesses found that the average annual loss from cybercrime more than doubled from \$168,000 in 2006 to \$350,424 in 2007.¹¹

Computer connectivity has also opened the door to crimes that threaten public safety including harassment and child exploitation.

- A recent survey¹² found that 1 in 7 children between the ages of 10 and 17 received a sexual solicitation on-line; 1 in 3 had unwanted exposure to pictures of naked people or sexual activity; and 1 in 11 was threatened or harassed.
- Other research found that 7 percent of online teens say they have felt scared or uncomfortable as a result of contact by an online stranger.¹³
- State officials announced in July 2007 that MySpace.com found more than 29,000 registered sex offenders with profiles on its popular social networking Web site.

PATROLLING CYBERSPACE

⁵ “Phishing Activity Trends – January 2008,” Antiphishing Working Group, www.antiphishing.org

⁶ “Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,” GAO-07-705, U.S. Government Accountability Office, June 2007, www.gao.gov

⁷ “2007 State of the Net report,” Consumers Reports, , <http://www.consumerreports.org>

⁸ “2007 Internet Crime Report,” Internet Crime Complaint Center, www.ic3.gov. The Internet Crime Complaint Center is a partnership between the Federal Bureau of Investigation, the nonprofit National White Collar Crime Center and the Bureau of Justice Assistance.

⁹ “2007 State of the Net report,” Consumers Reports, , <http://www.consumerreports.org>

¹⁰ “2005 Computer Crime Survey,” FBI

¹¹ “2007 Computer Crime and Security Survey,” Computer Security Institute, www.gocsi.com

¹² “Online Victimization: A Report on the Nation's Youth”, 2006, National Center for Missing and Exploited Children, www.missingkids.com

¹³ “Teens and Online Stranger Contact,” October 2007, Pew Internet and American Life Project, www.pewinternet.org

Numerous agencies in the United States have responsibilities to detect, investigate and prosecute cybercrime. Key players at the federal government level include the U.S. departments of Justice, Homeland Security and Defense and the Federal Trade Commission. Local and state law enforcement also fill an important role in protecting the people.

As the chief legal officers of the states, commonwealths and territories of the United States, attorneys general serve as counselors to their legislatures and state agencies, and also as the "People's Lawyer" for all citizens. While varying from one jurisdiction to the next due to statutory and constitutional mandates, typical powers include the authority to enforce state laws; act as public advocates in areas such as child welfare, consumer protection, antitrust and utility regulation; propose legislation; and represent state government in court.

The Washington State Attorney General's Office is known as a national leader in efforts to fight high-tech crimes. In 2000, we became the second attorney general's office in the nation to develop a unit specifically focused on high-tech consumer protection cases.¹⁴ Our office also proposes legislation to assist police and prosecutors in their work, provides education to prevent Washington residents from become victims of cybercrime and builds effective partnerships among agencies working to tackle the issue.

Shortly after I was elected attorney general in 2005, I sought additional support from our state Legislature to address the dramatic rise in high-tech fraud and identity theft cases in our state. The Legislature approved an additional \$1.6 million for our Consumer Protection Division, a portion of which paid for two new attorneys, a computer forensics investigator and a state-of-the-art computer lab where sophisticated tools are used to detect hackers, spyware purveyors and other Internet mischief.

SHUTTING DOWN SPYWARE

Spyware has arguably become the biggest online threat to consumers and businesses since the advent of the Internet. Washington became one of the first states to adopt a law explicitly prohibiting spyware activities and imposing serious penalties on violators.

The Washington Computer Spyware Act¹⁵ became effective in July 2005 and gives the Attorney General's Office a strong tool to discourage and prosecute spyware purveyors. The Attorney General's Office has obtained judgments that benefit consumers in all of the six lawsuits we've brought under the law.

¹⁴ The Washington Attorney General's fight against cybercrime occurs primarily in the arena of civil law where weapons include fines for offenders and injunctive provisions that mandate changes in business practices. While some states attorneys general have authority to prosecute criminal cases that can result in imprisonment, Washington laws limit the office's authority to investigate and criminally prosecute such cases. The office does not launch criminal investigations without a request from a county prosecutor or the Governor.

¹⁵ Revised Code of Washington (RCW) 19.270, www.leg.wa.gov

Broadly speaking, spyware is deceptive software that is installed on a computer, often without the user's knowledge or informed consent. Such software can collect and transmit personal information, change important privacy and security settings, and even take over the user's computer.

Thirteen states now have laws that specifically address spyware. The need for such legislation is evidenced by staggering statistics, including industry reports that estimate spyware and other unwanted software reside on up to 80 percent of consumers' computers.¹⁶ One study by software providers found an average of 25 spyware, adware or other potentially unwanted programs per PC.¹⁷ Microsoft has said that 50 percent of its customer-support calls related to computer crashes can be blamed on spyware.

Most computer users are unclear how spyware ended up on their computers, but it can happen by simply downloading a program offered for free, such as a screensaver or mp3 music file. Because spyware is frequently installed surreptitiously, frustrated consumers may not immediately attribute computer malfunctions to spyware. Some assume that hardware or software glitches are the "cost of doing business" and never seek to clean their computers of the harmful software.

Businesses also become victims of spyware installation, finding themselves plagued with compromised company security, overloaded networks, and significant user downtime. Dealing with spyware becomes an expensive and time-consuming problem for these businesses.

As concerns about computer safety grow, consumer confidence in e-commerce and online financial transactions may be undermined. The only way to keep the Internet market thriving is for the Attorney General's Office to approach high-tech cases as we do the "brick-and-mortar world" and bring our law enforcement powers to bear when appropriate.

A major problem states face in combating spyware is the widespread confusion and controversy over the definitions of spyware versus adware. Some think that software which gathers any information about a user's computer use should be called spyware. Others consider bundled software that displays targeted advertising to be spyware. Another group believes the definition should be limited to software that steals personal information

Washington's Spyware Act defines spyware by the effects the software has on a user's computer, as well as the method by which it is installed. The law prohibits collecting personally identifiable information through keystroke logging; collecting Web browsing histories; taking control of a user's computer to send unauthorized e-mail or viruses; creating bogus financial charges; orchestrating group attacks on other computers; opening aggressive pop-up advertisements; modifying security settings; and interfering with a user's ability to identify and remove the spyware.

Washington's Spyware Act doesn't stop at outlawing software programs that meet the more narrow definition of "spyware," but also punishes those who make false representations to

¹⁶ Separate 2004 studies by market researcher IDC and the National Cyber Security Alliance.

¹⁷ Earthlink and Webroot Software's [SpyAudit](#) report released February 2005.

induce users to install software, including misrepresenting the extent that a program is necessary for security.

The Attorney General's Office – or any owner of a Web site or trademark who is adversely affected by spyware violations – may bring an action under our law. Microsoft has done so successfully. Defendants can be fined up to \$100,000 per violation or actual damages, whichever is greater, and a court may increase damages threefold for repeat offenders up to a maximum of \$2 million. A violation of the spyware act is also a violation of Washington's Consumer Protection Act¹⁸, under which offenders may be subject to a civil penalty of up to \$2,000 per violation.

The Attorney General's Office has filed six lawsuits using our Spyware Act. Those lawsuits have attacked a variety of iterations of spyware, and have all resulted in resolutions including monetary judgments, injunctive relief and restitution for consumer victims. They include the following:

- In January of 2006, we filed our first case against Secure Computer, a New York-based seller of a so-called anti-spyware product that was advertised through pop-ups which misrepresented the user's risk of spyware infection. The pop-up, which resembled a Microsoft official security alert, encouraged the user to implement a free scan of the computer. The scan always showed the presence of spyware, even if none was present. The pop-ups could not be closed by clicking on conventional closure spots. The lawsuit was ultimately settled with all defendants, with provisions for a \$1 million payment and full restitution for consumers.
- In August 2006, the Washington Attorney General's Office sued Digital Enterprises d/b/a/ Movieland.com, for offering free trial subscriptions to adult-content movies, then billing consumers by sending incessant pop-up video payment reminders after the free trial had expired. Recipients were unable to close or minimize the pop-ups. The state alleged Movieland installed spyware on users' computers that caused the video to be displayed and automatically reinstalled it even when consumer tried to uninstall it. The case was settled with an injunction preventing the defendants from advertising using this method, fees, and restitution for consumers.
- In October 2006, we sued High Falls Media and ROC Telecommunications for their Spyware Slayer software that improperly induced users to install it by making false claims that users' computers were purportedly already infected. The case was settled for injunctive relief restricting future advertising practices, fees and restitution.
- In November 2006, we sued a New York man for his QuickShield software which induced consumers to install it by making false statements of security vulnerabilities. The case was settled for injunctive relief, fees and restitution to consumers.
- In February 2007, the state sued California-based Securelink Networks, LLC, and several other defendants for using Net Send messages and deceptive free scans to market each other's products, including Registry Sweeper Pro, Registry Rinse, Registry Doc, Registry

¹⁸ RCW 19.86, www.leg.wa.gov

Cleaner 32 and Registry Cleaner Pro. The messages misrepresented that consumers' computers were infected with critical registry errors and that they needed to buy the defendants' product in order to delete the errors. The court granted the state's requests for summary judgment, ordering the defendants and their owners to provide refunds to hundreds of Washington consumers.

- In March 2008, we accused a Scottsdale, Arizona, man of coercing consumers to buy software to block computer pop-ups by first bombarding them with ads for pornography and Viagra. Our suit alleged that consumers who downloaded the advertised products, which included Messenger Blocker, WinAntiVirus Pro 2007, System Doctor and WinAntiSpyware, were further victimized when the software caused their computers to stealthily blast messages to other PCs at a rate of one every two seconds. The case was settled in May 2008 for injunctive relief, fees and restitution.

On the federal front, unauthorized access to a computer is illegal under the Computer Fraud and Abuse Act¹⁹. U.S. lawmakers have tried unsuccessfully, beginning in 2004 and most recently in 2007, to pass a bill to further penalize makers of spyware by increasing prison time. The Federal Trade Commission Act (FTCA), which provides remedies under civil enforcement provisions, has been used by the Federal Trade Commission as a vehicle of enforcement against spyware purveyors. While the FTCA is not as specific as Washington's Computer Spyware Act in defining unlawful practices, it has proven effective in numerous federal actions.

REDUCING SPAM

The Washington Attorney General's Office has actually been fighting high-tech crime for more than a decade and made history in October 1998 by filing the nation's first state lawsuit against a spammer.

Washington's Unsolicited Commercial Email Act²⁰, which went into effect earlier that year, was one of the first laws in the country to regulate the sending of spam. It prohibits the sending of unsolicited commercial e-mail that contains misleading information in its subject line, uses a third party's domain name without permission, or misrepresents the message's point of origin. The law imposes penalties of up to \$500 per e-mail message.

Our suit accused Oregon resident Jason Heckel of spamming millions of Internet users to sell his online booklet entitled, "How to Profit From the Internet." The Washington Supreme Court unanimously upheld the constitutionality of our state spam law in 2001 and the U.S. Supreme Court refused to reconsider the case, exhausting Heckel's appeal options.

Legislators amended our state spam law in 2005 to specifically prohibit "phishing" scams, in which identity thieves try to trick consumers out of personal information by sending e-mails that appear to come from a business, such as a bank or online auction site. The law makes it illegal for a person to misrepresent his or her identity in order to solicit personal information online.

¹⁹ 18 U.S.C. § 1030, <http://www.gpoaccess.gov/USCODE/index.html>

²⁰ RCW 19.190, www.leg.wa.gov

The U.S. Congress passed the federal Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act²¹ in 2003, prohibiting unsolicited email with false or misleading subject lines and requiring that advertisers enable recipients to opt out of receiving future solicitations.

The Washington Attorney General's Office brought its first lawsuit under the statute shortly after it went into effect in 2004. The suit filed in U.S. District Court alleged that AvTech Direct, a now-defunct California marketing firm, and MD&I, a California-based corporation that sells computers, used deceptive subject lines and made it appear that messages came from other sources.

STOPPING DECEPTIVE INTERNET ADVERTISING

The Washington Attorney General's Office has brought more than a dozen cases involving Internet advertising since 2005 alone. In addition to our spyware and spam statutes, the state's Unfair Business Practices-Consumer Protection Act²² gives us broad regulatory authority. The statute prohibits unfair or deceptive practices in trade or commerce and allows the office to seek civil penalties of up to \$2,000 per violation.

Most recently, we have taken enforcement action against Internet affiliate advertisers who used Net Send or Windows Messenger pop-ups to deceptively market software. Windows Messenger Service, not to be confused with the instant-messaging program Windows Live Messenger, is primarily designed for use on a network and allows administrators to send notices to users. Our investigations uncovered a growing number of individuals who inundated consumers with Net Send messages and traditional pop-up advertisements that frequently resembled system alerts. Their intent was to pressure consumers to buy a product that would supposedly protect a computer from pop-ups, viruses or spyware. Many consumers wound up paying for a program that was essentially worthless or left the computer more vulnerable to malware. Our lawsuits resulted in shutting down a number of these operations and obtaining refunds for consumers.

We have also recently taken action against online companies who promoted "free" big-ticket items such as high-definition televisions, digital cameras and laptops. Consumers had to pay more than the items were worth in order to receive them. Moreover, we alleged the businesses really were after consumers' personal information that they could sell to marketers. These lawsuits have also resulted in injunctions prohibiting the companies' practices and providing restitution for consumers.

Our cases have also involved deceptive billing practices and failure to fulfill merchandise orders, among other issues.

PROMOTING DATA SECURITY

Data security and protecting personal information have become among the biggest business and legal challenges for both private and public entities. It is estimated that companies spend an

²¹ U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037, <http://www.gpoaccess.gov/USCODE/index.html>

²² RCW 19.86, www.leg.wa.gov

average of \$5 million each to recover from a data breach incident. Understandably, these breaches are taking a significant toll on consumer confidence. As a result, the public is demanding more protections. Financial security is of paramount importance and our responsibility is to protect the public from business practices that put that security at risk.

Washington has joined nearly half of the states in the country enacting security breach laws to require businesses and local and state government agencies to disclose breaches of their unencrypted security systems that contain personal information of their customers. No enforcement arm is specifically listed under our data breach notification statutes²³, although the Attorney General may be assumed to be the enforcer by default.

The purpose of our laws is to assure that in the event of a data breach, prompt notice is made to consumers in order to allow them to assure their personal information is not compromised. Our laws require that disclosure of a data breach must be made without “unreasonable delay, consistent with the legitimate needs of law enforcement”. That includes written notice, electronic notice or, in certain case, substitute forms including news media.

The statutes encourage both agencies and businesses to be responsible with consumer data and enable consumers to quickly work to ensure the safety of their personal information.

Another Washington state law²⁴ requires businesses and public agencies to dispose of personal information responsibly. Violators may be subject to civil liability if an individual is harmed as a result of the breach.

The Attorney General’s Office has made it our mission to focus on education so that businesses and agencies can develop systems that protect the vital information entrusted to them by their clients, customers and the public.

PROTECTING CHILDREN ONLINE

As the top legal officer for the state of Washington, I have the unique opportunity to work with law enforcement, prosecutors, lawmakers and advocacy groups to help improve community safety.

As part of our office’s SafetyNet campaign, our office staff visited communities across Washington to share what we’ve learned from the experts about the dangers of the Internet and to talk about ways kids can avoid those dangers. We visited schools, met with law enforcement and talked with PTAs and parent groups to spread the message about safety.

In 2006, the Attorney General’s Office teamed up with the National Center for Missing & Exploited Children to provide free train-the-trainer seminars to prepare up to 400 educators and law enforcement officers to teach Internet safety using curriculum created by an organization called NetSmartz. Also in 2006, I joined the National Center for Missing & Exploited Children with leaders across the state in encouraging 10,000 Washington parents and guardians to become

²³ RCW 19.255.010 and RCW 42.56.590, www.leg.wa.gov

²⁴ RCW 19.215.010, www.leg.wa.gov

informed about online safety issues and prevention tips through the Connected Family Online Classroom, developed by telecommunications company Qwest.

In 2007, I formed the Youth Internet Safety Task Force to increase Internet safety awareness in Washington state. This broad coalition includes law enforcement, child advocacy groups, academic experts, state and local government representatives, technology firms and associations, as well as concerned citizens. Members are divided into three subcommittees, each focusing on a particular issue related to youth Internet safety. Among others, the task force is reviewing current law in related areas such as child pornography and unlawful communications with minors.

In January of this year, attorneys general nationwide signed an agreement with MySpace that created an industry-wide task force²⁵ to develop technology to verify the age and identity of users of social networking sites. MySpace and the attorneys general agreed on a joint statement of key principles in which we emphasize our shared goal of protecting children from inappropriate content and unwanted contact by adults. Due to our agreement, MySpace has made many safety improvements including reviewing images and videos for harmful content, making the default setting “private” for new users under 18 and creating a closed “high school” section for users under 18 and other changes that make it harder for adults to contact minors. The company has also deleting profiles created by registered sex offenders.

MySpace is working to set profiles of existing 16- and 17-year-old members to private and is expected to implement “age locking” this year, whereby users who indicate they are under 18 will not be able to change their indicated age. The agreement also requires the company compile a registry of e-mail addresses provided by parents who want to restrict their child’s access to the site. The company has created educational materials for parents, established a 24-hour hotline to respond to law enforcement inquiries and trained more than 3,500 law enforcement officers.

We reached a similar agreement with Facebook in May and that company, too, has joined the task force. The task force will report back to the attorneys general every three months and issue a formal report with findings and recommendations at the end of 2008.

CONTINUED CHALLENGES

Despite tremendous strides in patrolling cyberspace, public and private entities continue to face challenges. In a June 2007 report to Congress, the U.S. Government Accountability Office described several impediments to cybercrime enforcement, including a lack of accurate reporting of crimes to law enforcement; difficulty obtaining and retaining investigators, prosecutors and forensics examiners; trouble keeping up to date with current technology and criminal techniques; and working in a borderless environment.

Unlike their traditional counterparts, crimes that use computer networks can be committed from afar, carried out automatically and attack a vast number of victims simultaneously. Perpetrators can more easily remain anonymous. Investigations are further

²⁵ The task force is led by the Berkman Center for Internet and Society at Harvard University, <http://cyber.law.harvard.edu/>

complicated by the need to deal with multiple jurisdictions, each with its own laws and legal procedures.

Despite significant and frequent outreach initiatives, studies²⁶ suggest that up to 17 percent of Americans still don't have antivirus software installed on their computers and about a third don't use software to block or remove spyware. Researchers also found that half of Americans with home wireless connections have not taken basic precautions such as enabling encryption. An estimated 3.7 million U.S. households with broadband connections still lack a firewall.

Some research suggests that unless something bad has happened to them, Americans tend to neither worry about their personal information nor to take steps to limit the amount of information that can be found about them online.²⁷

IMPORTANCE OF PARTNERSHIPS

Partnerships are a key part of our success in fighting cybercrime. Early on, the rapid changes in the nature of crime and technology created almost unwitting partnerships between citizens, business, government and law enforcement as everyone floundered to find effective ways to combat these new threats.

For example, in the past, a law enforcement agency working to build a case might have needed to rely solely on friendly cooperation from Internet service providers willing to reveal information necessary to prosecute a cybercrime case. Even police with sufficient resources to blaze the trail on this new crime-fighting frontier still found it difficult to manage the vast and ever-changing landscape of Internet crime.

Fortunately, today we are on much firmer ground against high-tech criminals. Now there are mechanisms in place to assure coordination between law enforcement, service providers and others. For example, our office has worked in cooperation with Microsoft and AOL in amassing the information necessary to prosecute cases against spyware purveyors and spammers.

Additionally, as citizens seek more protections from online crimes, the role of government is evolving to address these issues. The National Association of Attorneys General hosts an annual cybercrime conference to provide training relate to investigations, legislation, case law and public education campaigns. More than 415 prosecutors from attorneys general offices have attended special training related to computer-based crimes as a result of a cooperative effort formed in 2003 between the association and the National Center for Justice and the Rule of Law at the University of Mississippi. I have personally led two technology seminars for attorneys general and their staff at our national meetings.

Raising public awareness about criminal behavior and the importance of protecting information is also critical to reducing victimization. The Washington Attorney General's Office teamed up

²⁶ Consumers Reports, 2007 State of the Net report, www.consumerreports.org and McAfee-National Cyber Safety Alliance Online Safety Study, October 2007, www.staysafeonline.org

²⁷ "Privacy Implications of Fast, Mobile Internet Access," Pew Internet and American Life Project, February 2008, www.pewinternet.org

with AARP, Microsoft and the Federal Trade Commission in 2006 to present a Cyber Safety Campaign to educate the public about online hazards such as phishing scams, viruses and spyware. Computer safety is also covered as part our identity theft prevention education.

Law enforcement agencies are arming themselves with new weapons to conduct high tech investigations as criminal evidence is increasingly being stored on computers, cell-phones, digital cameras, in e-mails, text messages and tech imagery. Businesses are stepping up data security. Most importantly, all the players now recognize partnerships are not just helpful – they are necessary and critical to fighting and preventing high-tech crimes.

CONCLUSION

Fighting cybercrime requires the participation of all of us – government, private sector and the public. The Washington Attorney General's Office is working hard to provide statewide leadership, support law enforcement, educate consumers, assist businesses and protect children. Partnerships are key to our continued success.