Department of Homeland Security and NCSA's 2006 Emerging Internet Threat List:
Helping Consumers Prepare to Avoid Potential Threats

The Internet continues to offer many new opportunities for increased commerce, community interaction and learning, but Internet crime is maturing as an ever-evolving threat. Hackers and thieves adapt quickly to foil enhanced security mechanisms, finding new ways to steal personal and financial information. As a result of these ever-changing threats, the Department of Homeland Security and the National Cyber Security Alliance (NCSA) have joined together to identify and help consumers prepare for potential emerging Internet threats in the upcoming year. We have also developed five online preparedness practices that, when implemented, could help consumers avoid becoming Internet crime victims in 2006.

Emerging Internet Threats for 2006

- **Hackers Use Instant Messaging To Spread Viruses and Worms:** In 2005, use of Instant Messaging and text messaging services in the home and at the workplace continued to increase. Hackers and criminals have taken note, and are starting to exploit IM services, in conjunction with social engineering tactics, to infect computers with viruses and worms. Even though IM and text messaging attacks are not yet commonplace, a few new IM viruses like the "Virkel Instant Message Virus" were unleashed in 2005. The Virkel virus opened a backdoor in consumers' security software, giving hackers access to files and personal information and disabling parts of anti-virus and other security software. Since consumers are largely unaware of the fact that IM and text message services can be used to spread viruses, they are extremely vulnerable to these types of attacks.

- **Phishing Fraud Becomes More Prevalent and Sophisticated:** By the end of 2005, phishers had started to shift their tactics from large scale e-mail blitzes to more targeted and concentrated attempts. One example of such a targeted approach is called "spear phishing," which is a phishing email that targets a group of people within a specific company or organization, often appearing to be sent from an internal employee in the human relations department, IT department or even a former colleague. This tactic can be more effective than a generic phishing attempt, because "spear phishing" emails may look and feel just like emails employees are used to getting regularly from their company or organization. Spear phishing banks on the fact that recipients won't question the legitimacy of the emails.

- **Viruses Attack Cell Phones and PDAs:** Mobile wireless devices, like cell phones and PDAs, are becoming increasingly vulnerable to hackers and viruses. Last year, the number of viruses and worms that affected cell phones and PDAs increased substantially. Mobile device viruses like "Cabir" and "CommWarrior.A," could read addresses and phone numbers and spread from mobile phones and BlackBerrys through Bluetooth connections and mobile messaging services without the user's knowledge. While these types of attacks have not become pervasive, they have the potential to infect and spread from

devices consumers least expect, and target devices that probably lack security protections.

- **Hackers Target Online Brokerage Accounts:** In 2005, there were increased reports of hackers using malicious code to crack consumers' online brokerage accounts. Hackers exploited vulnerabilities in consumers' computer security to steal passwords and brokerage account information. They used the stolen information to sell the unsuspecting consumer's stock and then transfer the proceeds to an online bank account, where it was withdrawn. Since the nature of online brokerage accounts makes it easy to transfer funds from various accounts outside the firm, online brokerage accounts are attractive targets for hackers and thieves.

- **Internet Crimes Go Unreported:** Although the number of Internet crime victims rose in 2005, those victims rarely filed a report with the FTC or notified a police department of the crime. According to the Federal Trade Commission's "2005 Consumer Fraud and Identity Theft Complaint Data," 61% of Internet fraud victims did not notify law enforcement when victimized by Internet crime. Moreover, the FBI's "2005 Small Business Computer Crime Survey" indicated that only 9% of those businesses that experienced a computer security incident reported it to a law enforcement agency. Not reporting crimes to law enforcement makes it more difficult to catch and prosecute online criminals, allowing them to operate with impunity.

Combat Internet Threats with these Online Preparedness Practices

As threats change, you can take some simple precautions to stay a step ahead. See www.US-CERT.gov and www.StaySafeOnline.org for additional information to protect your computer or wireless device.

- **Practice the following three core protections to secure your computer:** To better secure and protect your personal and financial information while surfing or shopping on the Internet, you should always practice the following "Three Core Protections:"
    - Install a firewall and keep it properly configured
    - Install Anti-Virus and Anti-Spyware software, and keep it up to date
    - Regularly install updates for your computer's operating system

  Incorporating these three core protections will better ensure hackers and thieves cannot break into your computer and steal your personal and financial information.
- **Do not open unexpected emails, or provide personal or financial data over email:** Even if you know the sender, do not trust unexpected emails. Phishers regularly send spam or pop-up messages purporting to be from a business or organization that you might deal with, such as an Internet service provider (ISP), bank, online payment service, or even a government agency. These phishing emails usually urge you to "update" or "validate" your account information and might threaten dire consequences if you don't respond. The message then directs

you to a website that looks just like a legitimate organization's, but is in fact a fraudulent site. If you're unsure whether or not an unsolicited email asking for personal information is from a company you normally conduct business with, simply type in the companies URL in your web browser, and contact a customer representative directly, either through a phone call or email, to verify any issues you may have with your account.

- **Don't download attachments or click on links in unsolicited emails or Instant Messages:** Never download an attachment or click on website links in unsolicited emails or Instant Messages, unless you're expecting it. Hackers use attachments and links as a way to trick you into downloading malicious software onto your computer.
- **Take precautions to secure your mobile devices:** To prevent inadvertently downloading a mobile device virus through a Bluetooth connection, check the access permissions on your Bluetooth settings and turn off your device's Bluetooth connection when you are not using it. Moreover, you can use anti-virus software on some mobile platforms to protect yourself from viruses. In addition, you should encrypt personal information on your mobile device to help ensure no one but you can access it.
- **Report Internet Crimes to the Proper Authorities:** If you witness or become a victim of Internet crime or fraud, report the incident to a local law enforcement agency immediately. You can also report Internet crimes to the Internet Crime Complaint Center (www.icw.gov), a joint initiative run by the Federal Bureau of Investigation and the White Collar Crime Center, the Federal Trade Commission (www.ftc.gov), or your state Attorney General's Office.

  You can report phishing incidents by forwarding phishing emails to spam@uce.gov and to the bank, organization, or company impersonated in the email. You should also inform your Internet Service Provider. Your ISP can use the information to filter future phishing emails and to warn other customers of the recent phishing incident. Lastly, you can also report phishing to consumer protection organizations like the National Consumers League by going to www.fraud.org, or emailing the Anti-Phishing Working Group (APWG), a consortium of Internet companies that fight phishing, at reportphishing@antiphishing.org .