February 2013

Combating Online Fraud

Key Points

- Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted dollar loss of nearly half a billion dollars.
- Microsoft's four-part approach to combating online fraud includes dedicated internal teams, technology tools, education and guidance, and relationships with government, industry, law enforcement, and others.
- Microsoft supports government efforts to fight online fraud through international cooperation, public and private relationships, and strong enforcement of anti-fraud laws.

BACKGROUND

The Internet has transformed commerce around the world, allowing people to enrich their lives, build new companies and services, and engage in a wide variety of economic activities. Total global e-commerce sales are projected to exceed $1.2 trillion in 2013.

However, as economic activity moves increasingly online, so has the problem of fraud, which threatens to undermine the public trust in the benefits of e-commerce.

Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted loss of nearly half a billion dollars. Organized groups of cyber criminals go to great lengths to perpetrate their schemes to steal identities or commit financial fraud.

Online fraud schemes lure their victims using such devious tactics as social engineering, malicious software, and other attacks that victimize millions of individuals every year.

Social engineering takes advantage of people's trust by tricking them into such actions as installing malicious software disguised as a legitimate app or entering sensitive personal information on a convincing but fake website—actions that can compromise their computer or data.

Scams that use email, text, or social network messages that appear to come from a reputable organization and entice victims to disclose information such as account numbers or passwords are known as *phishing*. Research shows that they pose a threat to consumers. In 2011, the Anti-Phishing Working Group reported nearly 200,000 unique phishing attacks worldwide, and its recent data shows that the number of brands being exploited by phishers is at an all-time high.

To combat online fraud successfully, businesses, government, non-governmental organizations, and consumers worldwide can work together to fight it.

MICROSOFT APPROACH

Microsoft's four-part approach to combating online fraud includes dedicated internal teams, technology tools, education and guidance, and relationships with government, industry, law enforcement, and others.

- **Dedicated internal teams.** The Microsoft Digital Crimes Unit (DCU) is a worldwide team of attorneys, investigators, technical analysts, and other specialists. The team fights digital crime through relationships and legal and technical breakthroughs that destroy the way cyber criminals operate. DCU is a unique team in the tech industry, focused on disrupting some of the most difficult cyber crime threats facing society today—including the sexual exploitation of children facilitated by technology.
- **Technology tools.** Microsoft offers many online safety tools to help consumers fight online fraud, including Microsoft Security Essentials, a free antimalware program, as well as SmartScreen technologies and services.
  - » The SmartScreen service helps protect consumers against downloading malware from social engineering tactics such as phishing in Windows Internet Explorer 9 and 10.
  - » The SmartScreen Application Reputation service helps Internet Explorer 9 and 10 customers make better decisions about the trustworthiness of programs they download. When a user downloads an app from the Internet, SmartScreen uses reputation data to remove unnecessary warnings for well-known files and to show warnings when the download is at a higher risk of being malicious.
  - » SmartScreen antispam technologies and services help to protect Microsoft customers from email that may contain fraudulent solicitations.
- **Education and guidance.** The Microsoft Safety & Security Center provides guidance for safer Internet use, including tips on how consumers can secure their computers and avoid online scams.
- **Partnerships.** Microsoft works with many organizations dedicated to fighting online fraud, including the Anti-Phishing Working Group and the National Cyber Security Alliance.

POLICY CONSIDERATIONS

- **International cooperation.** Microsoft has joined with industry to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address online crime.
- **Public and private relationships.** Microsoft believes public and private relationships are essential to addressing the increasing complexities of cyber crime. Microsoft gives technical training to law enforcement agencies worldwide and develops new technologies to combat cyber crime. Microsoft has also helped protect consumers through legal action.
- **Strong enforcement and balanced regulation.** Microsoft strongly supports the enactment and enforcement of laws against online fraud, and the prosecution of cyber criminals. At the same time, it is important that legislation be carefully crafted so as not to discourage innovation and technology adoption in the process.

Helpful Resources

The Microsoft Safety & Security Center with guidance for consumers
www.microsoft.com/security

Online Fraud: Your Guide to Prevention, Detection, and Recovery
aka.ms/OnlineFraudBooklet

The Microsoft Digital Crimes Unit
www.microsoft.com/dcu