Homeland Security
BAE SYSTEMS
STAYSAFEONLINE.org
National Cyber Security Alliance
USA TODAY Education

Lesson 6

Cybercriminals can't get away with what they used to

By Jon Swartz
USA TODAY
November 17, 2008

In what is shaping up as a breakthrough year, federal authorities have quietly cracked down on some of the biggest Internet crime rings.

Secret Service and FBI operations since January have broken up a huge forum for stolen credit cards and shut down the world's largest spam ring. Investigations have led to indictments of other high-profile spammers and 11 people allegedly behind the computer break-in at TJX and other major retailers.

The FBI and Secret Service do not provide annual cybercrime statistics, but high-profile arrests are significantly up this year, says Shawn Henry, assistant director of the FBI Cyber Division.

Dozens of such actions reflect better-trained agents and prosecutors, stronger laws and more cooperation from crime fighters overseas. Strides in cybercrime fighting are particularly important now because most security experts point out that fraud soars during economic downturns. Cybercrime is an estimated $200 billion market.

For the first time, "It's not a question of whether you will be caught, but when," says Hemanshu Nigam, chief security officer of MySpace who, as a Microsoft executive, crafted a $250,000 bounty in late 2003 that led to the arrest of infamous German hacker Sven Jaschan.

Aiding the crime fighting:

- **More resources.** Federal agencies have a better understanding of technology and how to infiltrate organized crime groups, especially in Eastern Europe. "The threat is not going away. But our ability to impact the threat has become much better," says Henry.

The Secret Service has ramped up training for its agents, prosecutors and federal judges. About 1,000 agents are trained, significantly more than a year ago. "These investigations take time and expertise," says John Large, special agent in charge of the Secret Service Criminal Investigative Division.

- **International help.** The feds are partnering closely with peers in Romania, Turkey, Germany and elsewhere. "Romania is the gold standard," says Henry, who laid the groundwork with the country's national police. Working with them, the FBI has arrested 90 people, primarily phishers, this year.

Romanian Prosecutor General Laura Codruta Kovesi has led the effort to prosecute individuals with ties to international organized crime involved in computer and credit card fraud schemes. "The U.S. and their Romanian counterpart agencies are working as partners and colleagues," she says.

Henry says he met with cyberofficials in Moscow in January and that Russian agents are being trained in the U.S. "We think the relationship can be as fruitful as the one in Romania," he says.

- **Stiffer cyberlaws.** Sentencing guidelines have gotten tougher. “It’s easier to get someone locked up,” says Keith Schwalm, president of DNK Consulting and a former Secret Service agent who worked on cybersecurity issues. One law in particular has given prosecutors a crime-fighting tool. The Identity Theft Enforcement and Restitution Act of 2008 makes it a felony to damage 10 or more PCs used by or for the federal government or a financial institution.

Tech companies also are more aggressively pursuing criminals with existing laws. MySpace has filed five lawsuits this year against spammers, one of which resulted in a record $230 million judgment for violation of the federal anti-spam law.

Lesson
6

Introduction

While many stories focus on cybercriminals and their misdeeds, this article looks at how law enforcement is quietly gaining ground with the help of additional resources, international cooperation and tougher laws.

Discussion

1. How much money does cybercrime bring in each year?
2. Why were the Federal Bureau of Investigation (FBI) and the Secret Service able to track down and arrest more cybercriminals in 2008?
3. What types of activities are cybercriminals involved in?
4. How have stiffer cyberlaws helped law enforcement in cybersecurity?
5. Do we, as citizens, have any part to play in bringing cybercriminals to justice? If so, what?

Activity

Divide students into pairs and assign each group one of the following letters: I, P, E or S. Each pair must have access to the Internet.
The I teams will go to: http://www.onguardonline.gov/topics/identity-theft.aspx
The P teams will go to: http://www.onguardonline.gov/topics/phishing.aspx
The E teams will go to: http://www.onguardonline.gov/topics/email-scams.aspx
The S teams will go to: http://www.onguardonline.gov/topics/spyware.aspx

With your partner, fill out the following grid:

Describe your cybercrime:	
How can people recognize this cybercrime?	
What are ways to protect yourself from this cybercrime?	
If you are a victim of this cybercrime, what steps do you need to take?	
How do you report a suspected cybercrime?	

Lesson 6

TEACHER'S GUIDE

Overview:

In this lesson, students will:

- Read the article, "Cybercriminals can't get away with what they used to."
- Summarize why law enforcement is having more success in pursuing cybercriminals.
- Research one type of cybercrime.
- Do a teachback on one type of cybercrime.
- Describe one way to avoid becoming a cybercrime victim or one way to help law enforcement catch a cybercriminal.

Grade level:

6-12

Subject areas:

career and technical education, language arts, social studies, advisory classes

Time requirements:

Step 1: Read the article (15 minutes).

Step 2: Discuss the articles using the questions provided (10 minutes).

Step 3: Pair up and prepare a teachback on your assigned cybercrime based on the FTC website (20 minutes).

Step 4: Have pairs partner up with another team that researched a different cybercrime (for example, have the "I" and "S" teams pair up, etc.). Have one pair give a two-minute report on their topic; then have the other team give a two-minute report on their topic. If there is time, have the teams swap so the "I" and "E" teams can get together. Repeat the process (10 minutes).

Step 5: As a group, have students debrief some of their key findings: What surprised them? What were some of the best tips they learned? How can they help prevent cybercrime? (5 minutes)

Total: 60 minutes in class (Times may vary according to students' grade and ability levels.)

Notes:

1. You may want to preteach the following concepts and vocabulary words: indictment, gold standard, phishers and felony.
2. Each pair of students must either have access to the Internet or a printout of one of the websites listed in the activity. The letter assigned to each group relates to a cybercrime topic. Those who are in the "I" teams will be looking at identity theft. The "P" teams will look at phishing. The "E" teams will research email scams. The "S" teams will learn about spyware. The email scam information is lengthy. You may choose to assign this to fast readers or summarize it yourself instead of assigning students to it.

Links:

- National Cyber Security Alliance: www.staysafeonline.org
- Department of Homeland Security: www.DHS.gov/cyber
- United States Computer Emergency Readiness Team: www.us-cert.gov
- i-SAFE: www.isafe.org
- Wired Safety Organization: www.wiredsafety.org
- Federal Trade Commission: www.onguardonline.gov
- Multi-State Information Sharing and Analysis Center: www.msisac.org/awareness
- ConnectSafely: www.connectsafely.org/safety-tips-and-advice.html
- iKeepSafe: http://tools.ikeepsafe.org/older-students
- FBI's Internet Crime Complaint Center: www.IC3.gov
- Identity Theft Resource Center: www.idtheftcenter.org