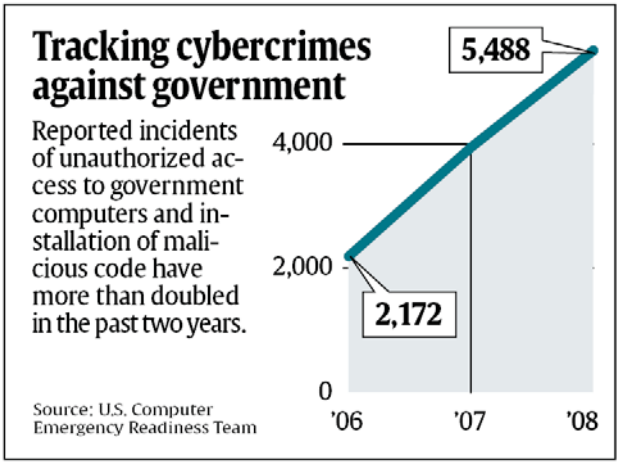
Lesson 4

Raids on federal computer data soar

By Peter Eisler
USA TODAY
February 17, 2009

Reported cyberattacks on U.S. government computer networks climbed 40% last year, federal records show, and more infiltrators are trying to plant malicious software they could use to control or steal sensitive data.

Federally tracked accounts of unauthorized access to government computers and installations of hostile programs rose from a combined 3,928 incidents in 2007 to 5,488 in 2008, based on data provided to USA TODAY by the U.S. Computer Emergency Readiness Team (US-CERT).



By Julie Snider, USA TODAY

"Government systems are under constant attack," says Joel Brenner, counterintelligence chief in the Office of the Director of National Intelligence. "We're seeing ... a dramatic, consistent increase in cybercrime (and) intelligence activities."

The government does not publicly detail the number or types of attacks that succeed. A commission of government officials and private experts reported in December that the departments of Defense, State, Homeland Security and Commerce all have suffered "major intrusions" in which sensitive data were stolen or compromised.

"The damage from cyberattack is real," says the report, issued by the Center for Strategic and International Studies with Reps. Jim Langevin, D-R.I., and Michael McCaul, R-Texas.

The new data on attacks represent a small sampling — just 1% of federal agencies have fully developed tracking systems — and some of the increase may reflect better reporting, says Mischel Kwon, who heads US-CERT at the Department of Homeland Security. Still, the reports are the best public accounting of such attacks and underscore concerns driving federal cybersecurity initiatives.

National Intelligence Director Dennis Blair told Congress last week that government networks are targeted by foreign nations seeking intelligence, such as China and Russia, as well as criminal groups and individuals who may want to disrupt power, communication or financial systems.

Some attackers may be less interested in stealing data than in undermining a system's ability to operate, such as by planting software that could slow critical networks in emergencies, Brenner adds.

Security officials are especially alarmed about phishing, in which seemingly legitimate e-mails solicit sensitive information, and

"web redirects," which shunt a computer to a website where it downloads malicious software, Kwon said.

As part of a Comprehensive Cyber Security Initiative launched by former president Bush, the government has cut the number of portals linking federal computer networks to the Internet from 4,500 to 2,500.

Last week, President Obama named Melissa Hathaway, who headed the initiative, to run a 60-day review of federal cybersecurity programs.

The review should spur more cybersecurity initiatives, Brenner says. "What's going on now is not enough, but it is the absolute necessary condition for the progress we have to make."

Lesson 4

Introduction

The U.S. government has a lot of fascinating information on its servers that other governments or cybercriminals would like to steal. Some just want to plant malicious software on the government's computers to make things messy. Either option could wreak havoc on the system and cause problems for the government and you. Read the article and discover how a successful hack on a government computer could affect your life.

Discussion

1. How many cyberattacks occurred on U.S. government computer networks in 2008?
2. How many occurred in 2007?
3. Why do you think there has been such an increase in the number of attacks?
4. Name as many government agencies (city, state and federal) as you can think of.
5. If these agencies' networks were attacked and compromised, what could happen? What could the infiltrators gain?
6. How could some of the problems caused by such attacks affect your state? Your city? Your school? Your house?

Activity

1. Take five minutes and write down ways a successful attack on a government network could wreak havoc on society or create a dangerous situation.
2. Now, find one partner and share the three worst things you think could happen. If your partner says something you like, add that to your list.
3. Next, find a different partner to share with.
4. As a class, create a top 10 list of the dangers of a successful cyberattack on a government network.
5. If someone were successfully prosecuted for cybercrime, what types of punishment do you think would be just and fit the crime? What creative punishments might discourage a cybercriminal from attacking again?

Watch a short, three-minute video of President Obama giving an overview of the importance of cybersecurity. Find out how everyone can help prevent cybercrime and what individuals can do to protect themselves online. Go to: www.youtube.com/watch?v=UIIY9AQSqbY&feature=player_embedded.

Extension

Inform teens about the serious cyberthreats the U.S. faces. Create your own YouTube video outlining the top 10 dangers a cyberattack on a government computer would pose.

Lesson 4

Overview:

In this lesson, students will:

- Read and discuss the article, "Raids on federal computer data soar."
- Analyze the dangers of cyberattacks on government computers.
- Prioritize the dangers.
- Share these dangers with two different partners.
- Create a class list of these dangers.
- Brainstorm possible punishments for cybercriminals.

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 article using the questions provided (10 minutes).
Step 3: Analyze and share the dangers of cyberattacks on the government (20 minutes).
Step 4: Watch a three-minute video from President Obama on how cybersecurity is everyone's job (5 minutes).
Extension: Time varies. To be completed outside class.
Total: 50 minutes in class (Times may vary depending upon students' grade and ability levels.)

Notes:

1. You may want to preteach the following vocabulary words: infiltration, malicious, undermine, solicit and shunt.
2. You'll need online access and a way to project the video of President Obama so all students can see. (Or, you can download the video ahead of time)

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