THE NATION'S NEWSPAPER

Special Reprint Edition

USA TODAY

NO. 1 IN THE USA

As seen in USA TODAY News

July 29, 2010

# Cybergang goes after job-seekers with check scam

By Byron Acohido
USA TODAY

LAS VEGAS — Job-seekers beware. A Russian cybergang is running a slick e-mail recruitment campaign offering to pay you up to $500 to cash expertly faked business checks of just under $3,000.

Such offers are being e-mailed to thousands of job-seekers who've posted their resumes at popular employment websites, the security firm SecureWorks disclosed Wednesday at the opening of the Black Hat cybersecurity conference here.

One recent recruit, a college student looking for part-time work, thought it was a legit offer until SecureWorks senior researcher Joe Stewart alerted him via Facebook.

"He was appreciative," Stewart says. "But he was genuinely disappointed that the job was not real."

The crooks would have sent the student a business check made out to him with detailed instructions on how to cash it, then wire the balance, less a generous handling fee, to a contact in Russia.

However, to earn the fee, the recruit would have to execute the transfer within 24 hours. The scam probably only works in a minority of cases, where the fake check is cashed and funds transferred quickly enough to escape detection, Stewart says.

But swarms of attempts are being made. Stewart recently discovered a computer server storing digital images of some $9 million worth of high-quality fake checks, each slightly less than $3,000, written against some 1,200 business accounts.

The criminals earlier hacked into the databases of three firms that archive images of business checks, stealing account numbers, names, addresses and even legitimate signatures. They then created their own business checks using legitimate check-writing software, paper and printing services.

SecureWorks turned its findings over to the FBI.

The check-kiting scheme underscores how creative cybercrooks have become. Multistage attacks that combine stolen data and social-engineering trickery are being refined to pilfer in novel ways.

"Cybercriminals are learning business patience," says Paul Ducklin, technology director at anti-virus company Sophos.

"They do research, acquire different pieces, put them together for specific purposes, take risks, and then profit handsomely."

# Cybergang goes after job-seekers with check scam

## Objectives

- Read the article "Cybergang goes after job-seekers with check scam"
- Identify the key components of a scam offer
- Discuss in small groups and list ways to protect yourself from specific online scams
- Report back or "teachback" tips on protecting yourself from specific scams to classmates

## Preparation

Each student will need:

- A copy of the article "Cybergang goes after job-seekers with check scam"
- A copy of the lesson
- Access to the internet or copies of the information found on the webpages listed in the activity, at least one copy per group

## Read the article and answer discussion questions (20 minutes)

1. How does this check scam work? What makes this a scam?
2. Are the checking accounts real? Where are cyberthieves getting these account numbers?
3. Why do you think this cybergang is asking job-seekers to cash these checks?
4. Do you think the college student looking for part-time work should have known this job was a scam? What clues were there that this job was not legitimate?

## Fight Back Teachback (35 minutes on day one, 40 minutes on day two for doing teachbacks)

1. As an introduction to the activity, show this video on information phishing: onguardonline.gov/videos/phishy-home.aspx

2. All students should be placed into groups of four to five students. Each group should be assigned (or may choose) one of the following areas where teens can be vulnerable to online scams: online shopping, P2P security, computer security, malware, social networking sites, and email scams.

3. Groups should then go to onguardonline.gov and click on "Topics" to investigate different cyber-vulnerabilities related to their specific topic. Groups should fill out their graphic organizer as they read and research information.

4. After groups fill out the graphic organizer, each student in each group should plan on sharing at least one fact or scam-prevention tip from their reading as a way of informing their classmates of other scams.

# Cybergang goes after job-seekers with check scam

**Topic:** _____

| Name of scam | Characteristics of scam | Tips to protect yourself |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Debrief/Application questions** (10 minutes)

Are there any characteristics that seem to be the same in many scams? What are they? What are some of the best tips you heard for avoiding becoming a scam victim? Which one tip do you think you will implement right away? Why?

For extra credit and fun, students can check out games at this website to see how scam-savvy they are: onguardonline.gov/games/overview.aspx

StaySafeOnline.org
National Cyber Security Alliance