Be on alert at work for cyber-scammers

by **Erin E. Arvedlund**, Inquirer Staff Writer

Those pesky cyber-criminals are targeting us where it hurts: on the job.

Hackers now pose as our bosses or supervisors, law enforcement officials say - asking us to send emails with sensitive W-2 tax returns or payroll information and employee Social Security numbers.

Main Line Health was just the latest victim, according to Brian Thomas, supervisor from the IRS criminal investigations branch, and Benjamin Stone, who leads the new cyber criminal squad for the FBI's Philadelphia office. The two agencies are working together to alert businesses in the region and their customers that scam artists have gotten more sophisticated.

"If your CEO or CFO appears to be emailing you for a list of company employees and personal information, check with the person by phone or face-to-face before you respond," Thomas said. "Get out of your chair and ask them in person or call. It's easier to just hit 'reply,' but if it's a hacker, they'll thank you for the effort."

In recent weeks, a Pennsylvania mortgage borrower was scammed out of $240,000 for a house wired to a hacker posing as the mortgage banker, said Michael Bantner, special agent with the FBI's Fort Washington office.

As the bureau's liaison contact for Bucks and Montgomery Counties, Bantner gets one or two calls a week from local business owners, particularly mortgage brokers and settlement companies "spoofed" by hackers.

"Bucks and Montco are heavily populated with white-collar employers," Bantner said. "The hackers crack these small companies' email systems, monitor the lingo between employees and customers, then pose as the boss or a supplier."

Mortgage companies often email borrowers' loan files and closing documents, making them ripe targets.

"The hackers intercept and say the bank account information changed, send your mortgage payment money to some other account," Bantner added.

If you're sending sensitive information through email, always call to confirm within 24 hours that the money arrived. If it didn't, the FBI can help get it back.

"After 72 hours without notifying us, it's too late to get the wire transfer reversed and get your money back," he said.

As local IRS and FBI officials investigate "phishing" and "spoofing" against local businesses and employees, they advise preventive steps.

"Any time someone wants to initiate a wire transfer, call them to repeat the account number and amount verbally along a prearranged keyword," the FBI's Stone said.

Never rely on just an email or a phone call from the requester. Hackers will often call claiming to be someone else.

Insist on two-person verification, similar to the way the military sets up nuclear launch codes, said Dallas-based Rod Griffin, director of public education at the credit bureau Experian. (Griffin himself was a victim last year, through the IRS break-in.)

If you receive an "urgent" email from an executive asking for money, don't hit reply, law enforcement officials added.

"You, as the recipient, need to initiate confirmation with a new email," Bantner said.

On Feb. 16, a Main Line Health employee responded to an email believed to be a legitimate request for information about 11,000 Main Line employees that also included names, addresses, and salaries.

"I've never seen criminals focus on employers like they are now," said David Rosenbaum, a principal at the accounting firm Citrin Cooperman.

Rosenbaum added that employees should never change shipping instructions based on emails or phone calls. Always call the customer or intended recipient, or create new emails to confirm the change in instructions.

Businesses can institute formal data-breach plans, including compliance with state-notification laws, and training for employees on cybersecurity issues such as "phishing" (illustrated by the Main Line Health case) and "spoofing," targeted email scams that appear to be from an individual you know.

If your company has been hacked or received suspicious emails from customers, vendors, or executives, the local Philadelphia IRS and FBI offices ask that you contact them.

Contact Brian Thomas at the IRS at 267-941-6373. The FBI's Cyber Criminal Squad's phone number is 215-418-4000. Special Agent Bantner said he welcomes phone calls from local businesses in Bucks and Montgomery Counties at 215-641-8910.

If scammers are targeting your finance or investment firm, you also can contact the Department of Banking and Securities consumer hotline, 1-800-722-2657 to file a complaint or ask questions. Learn more at www.dobs.pa.gov.

And you can file a report with the local police department, as you would in the case of an individual identity theft.