

From: Taillon, Jeff

To: Godfrey, Rob <RobGodfrey@gov.sc.gov>

Taillon, Jeff <JeffTaillon@gov.sc.gov>

churchl@email.sc.edu <churchl@email.sc.edu>

Stirling, Bryan <BryanStirling@gov.sc.gov>

Haltiwanger, Katherine <KatherineHaltiwanger@gov.sc.gov>

LeMoine, Leigh <LeighLeMoine@gov.sc.gov>

Walls, Courtney <CourtneyWalls@gov.sc.gov>

Soura, Christian <ChristianSoura@gov.sc.gov>

Pitts, Ted <TedPitts@gov.sc.gov>

Baker, Josh <JoshBaker@gov.sc.gov>

Bondurant, Kate <KateBondurant@gov.sc.gov>

Walker, Madison <MadisonWalker@gov.sc.gov>

Veldran, Katherine <KatherineVeldran@gov.sc.gov>

Patel, Swati <SwatiPatel@gov.sc.gov>

Schimsa, Rebecca <RebeccaSchimsa@gov.sc.gov>

Peters, Hal <HalPeters@gov.sc.gov>

Date: 11/16/2012 10:52:50 AM

Subject: WBTW: Man says hackers stole SC bank information (Video)

WBTW: Man says hackers stole SC bank information (Video)

<http://www2.wbtw.com/news/2012/nov/15/man-says-hackers-stole-bank-information-ar-4978845/>

By: Brie Jackson

MYRTLE BEACH, SC - The state of South Carolina continues to take steps to better protect taxpayers personal information from hackers.

This week, Governor Nikki Haley signed an executive order that requires her cabinet agencies to use a state computer monitoring service and hires new people to monitor new equipment around the clock. The move comes after a hacker apparently stole personal information from more than 3 million South Carolina Taxpayers.

Bill Jennings was surprised when he received a letter in the mail stating that his direct deposit account changed.

"None of that happened from my actions" he said. It was apparently from someone else who hacked in to my social security account."

Jennings manages businesses in various states including South Carolina. He said he believes the same foreign hacker who stole from the state's database may have gained access to his account.

Jennings said it has been weeks since his private information was stolen and he has yet to see his social security check deposited to the proper account.

He said straightening out his hacked information has been a long and confusing process. He hopes sharing his story can be a valuable lesson for victims of computer hackers.

"As soon as you realize you've been hacked, make immediate contact with the social security office or the proper agency" he said. "Also be prepared to go to the social security office so they can handle an emergency payment."

While Jennings hopes to receive his payment by next week, he said the most frustrating part is that this could all happen again.

"If I change my direct deposit account, the hackers still have my personal information and can gain access to my accounts" he said.

Jennings said he's sure his information was stolen but he can't prove that the thief is the same person who hacked the state computers.

Jeff Taillon

(803) 734-5129|Direct Line

(803) 767-7653|Cell