Hackers apparently fooled Clinton official with bogus email

October 29 2016, by Tami Abdollah And Michael Biesecker

In this Oct. 5, 2016 file photo, Hillary Clinton's campaign manager John Podesta speaks to members of the media outside Clinton's home in Washington. New evidence appears to show how hackers earlier this year stole more than 50,000 emails of Hillary Clinton's campaign chairman, an audacious electronic attack blamed on Russia's government and one has resulted in embarrassing political disclosures about Democrats in the final weeks before the U.S. presidential election. (AP Photo/Andrew Harnik, File)

New evidence appears to show how hackers earlier this year stole more than 50,000 emails of Hillary Clinton's campaign chairman, an audacious electronic attack blamed on Russia's government and one that has resulted in embarrassing political disclosures about Democrats in the final weeks before the U.S. presidential election.

The hackers sent John Podesta an official-looking email on Saturday, March 19, that appeared to come from Google. It warned that someone in Ukraine had obtained Podesta's personal Gmail password and tried unsuccessfully to log in, and it directed him to a website where he should "change your password immediately."

Podesta's chief of staff, Sara Latham, forwarded the email to the operations help desk of Clinton's campaign, where staffer Charles Delavan in Brooklyn, New York, wrote back 25 minutes later: "This is a legitimate email. John needs to change his password immediately."

But the email was not authentic.

The link to the website where Podesta was encouraged to change his Gmail password actually directed him instead to a computer in the Netherlands with a web address associated with Tokelau, a territory of New Zealand located in the South Pacific. The hackers carefully disguised the link using a service that shortens lengthy online addresses. But even for anyone checking more diligently, the address—"google.com-securitysettingpage"—was crafted to appear genuine.

In the email, the hackers even provided an internet address of the purported Ukrainian hacker that actually traced to a mobile communications provider in Ukraine. It was also notable that the hackers struck Podesta on a weekend morning, when organizations typically have fewer resources to investigate and respond to reports of such problems.

Delavan, the campaign help-desk staffer, did not respond immediately to The Associated Press' questions about his actions that day.

It is not immediately clear how Podesta responded to the threat, but five months later hackers successfully downloaded tens of thousands of emails from Podesta's accounts that have now been posted online. The Clinton campaign declined to discuss the incident. Podesta has previously confirmed his emails were hacked and said the FBI was investigating.

The suspicious email was among more than 1,400 messages published by WikiLeaks on Friday that had been hacked from Podesta's account.

It was not known whether the hackers deliberately left behind the evidence of their attempted break-in for WikiLeaks to reveal, but the tools they were using seven months ago still indicate they were personally targeting Podesta: Late Friday, the computer in the Netherlands that had been used in the hacking attempt featured a copy of Podesta's biographical page from Wikipedia.

The U.S. Office of the Director of National Intelligence and the Homeland Security Department have formally accused Russian state-sponsored hackers for the recent string of cyberattacks intended to influence the presidential election.

The help-desk staffer, Delevan, emailed to Podesta's chief of staff a separate, authentic link to reset Podesta's Gmail password and encouraged Podesta to turn on two-factor authentication. That feature protects an account by requiring a second code that is separately sent to a cell phone or alternate email address before a user can log in. "It is absolutely imperative that this is done ASAP," Delevan said.

Tod Beardsley, a security research manager at the Boston-based

cybersecurity firm Rapid7, said the fact that an IT person deemed the suspicious email to be legitimate "pretty much guarantees the user who is not an IT person is going to click on it."

Other emails previously released by WikiLeaks have included messages containing the password for Podesta's iPhone and iPad accounts.