
From: CyberScoop <news@cyberscoop.com>
Sent: Thursday, November 10, 2016 12:24 PM
To: Haley, Nikki
Subject: The Russians haven't stopped trying to hack us

Not rendering correctly? View this email as a web page [here](#).



Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

THURSDAY

November 10, 2016

Election Day is over but 2016's cyberwar carries on. The fight over encryption is gearing up for its next round. And that email from OPM talking about bank information isn't real. Don't open it! This is CyberScoop for Thursday, November 10.

HERE WE GO AGAIN: Prominent American think tanks say they were targeted—again—by a spearphishing campaign from Russian hackers who don't seem to have changed their habits after the Trump victory. Attacks against think tanks have been ongoing for months and, given the intelligence value of the individuals inside these institutions, they can expect to be targeted for a long time to come. [Patrick O'Neill looks at what happened](#).

CRYPTO FIGHT COMING: In 2017, we're going back to the future. With Trump's team swinging into Washington and James Comey still atop the FBI, the encryption debate that dominated news in late 2015 and early 2016 is going to hit headlines once again as Americans and the world figure out the future of security and privacy in cyberspace. Washington and Silicon Valley are gearing

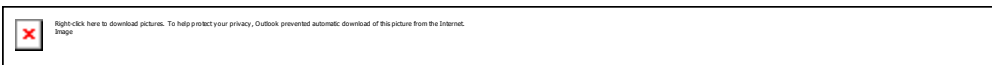
up for a fight in which the implications are enormous. Patrick O'Neill looks [at the future fight](#) coming your way.

WHAT WE'RE WATCHING

A NEW PARADIGM: RSA President Amit Yoran recently spoke with CyberScoop's Greg Otto about why organizations need to shift their thinking when it comes to cybersecurity, and why this year's events show the thinking needs to shift quickly. [WATCH HERE](#).

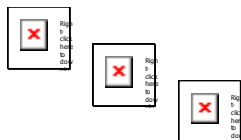
NOT REALLY OPM: A specially tailored ransomware campaign designed to take advantage of prior cyberattacks on the Office of Personnel Management went out to thousands of government workers Tuesday morning. Emails containing malware laden attachments appeared to come from OPM, with the messages describing suspicious activity spotted on the receiver's bank account. Researchers tell CyberScoop that the ransomware campaign was in no way inspired by Election Day, but rather was timed to impact people who were checking their emails in the morning across the country. When opened the computer virus takes control of a victim computer, encrypting files and threatening to block access unless a bitcoin payment is received. [Chris Bing has more](#).

TWEET OF THE DAY



Big, if true.

In the meantime, how about tossing your favorite new website a follow on [Twitter](#) and a like on [Facebook](#)? Click those shiny social buttons below to get the best we have to offer across the social web.



This newsletter is produced by Scoop News Group.
Visit cyberscoop.com to read this newsletter on the web.

CyberScoop News 1150 18th Street NW Suite 850 Washington District of Columbia 20036 United States

You received this email because you are subscribed to CyberScoop | Newsletter from CyberScoop News.

Update your [email preferences](#) to choose the types of emails you receive.

[Unsubscribe from all future emails](#)