

---

**From:** CyberScoop <news@cyberscoop.com>  
**Sent:** Tuesday, November 29, 2016 12:04 PM  
**To:** Haley, Nikki  
**Subject:** Wait, people are posting their credit card numbers \*WHERE\*??!

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.

---

**TUESDAY**

**November 29, 2016**

*The president-elect is running into some trouble regarding his phone calls. That Muni ransomware may have been in the wild for months. And the #creditcardchallenge makes us wonder why we even bother. This is CyberScoop for Tuesday, November 29.*

---

**THAT'S NOT HOW THIS WORKS:** Given his angry criticism of Democratic rival Hillary Clinton's use of a personal email account and private server during her tenure as Secretary of State, you might think that President-elect Donald Trump would be taking scrupulous care to color within the lines when it comes to his transition team's communications. Well, you'd be wrong. Two Democratic lawmakers including the ranking member of the powerful House Committee on Oversight and Government Reform are asking federal auditors to probe the incoming administration's cyber and communications security after press reports that Trump has spoken to world leaders on his personal cell phone, rather than on government-provided secure lines. [As Shaun Waterman reports](#), it's not clear yet whether the GAO will launch a probe, but if they do, it will likely be unprecedented.

**BACK ON TRACK:** San Francisco's Muni looks to have recovered from the ransomware attack that locked down its systems, but not before we learned a bunch about what exactly happened. Ransomware used in a cyberattack may be the mutated offspring of an older variant discovered by researchers in September, experts tell CyberScoop. Dubbed "Mamba," this ransomware is among the first to do full disk encryption by leveraging Disk Cryptor, an open-source software product. The ransomware operators were likely able to quickly compromise a significant number of SFMTA's machines because of how the malware collects credentials. [Chris Bing has more.](#)

---

## EVENT

**NETWORK OF THE FUTURE:** With GSA's new Enterprise Infrastructure Solutions (EIS) contract, agencies will replace current Networx Universal and Enterprise contracts as well as regional and local contracts for government telecommunications and infrastructure solutions. Federal agencies now have a more flexible, affordable, and easy vehicle for the more than \$2 billion-worth of managed network services they buy each year. Join us Nov. 30 at the Next Gen Network Summit to explore how the new vehicle, set to launch in 2017, will impact agencies - allowing you to balance a tight budget while fulfilling your ever-increasing need for more bandwidth, speed and security. [REGISTER HERE.](#)

---

**IN CASE YOU MISSED IT:** A hacker broke into Navy systems last week and accessed the personal data of more 130,000 current and former U.S. Navy sailors, the service announced. "The Navy takes this incident extremely seriously — this is a matter of trust for our sailors," said Chief of Naval Personnel Vice Adm. Robert Burke. The attacker was reportedly able to break into the Navy's IT infrastructure through a compromised laptop belonging to an employee of Hewlett Packard Enterprise Services, a supporting U.S.-based government tech and defense contractor. [Chris has more.](#)

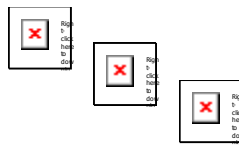
---

## TWEET OF THE DAY

We don't have a single tweet today, just the directive to go search for the [#creditcardchallenge](#) on Twitter. If you want the back story, check out [this Reddit thread](#). Hey, everyone! It's almost like no one cares about basic cybersecurity! LOL! \*laughs turn to sobs\*

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](http://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](#)