POTUS IS POSTING: SOCIAL MEDIA & NATIONAL SECURITY

Dr. Kenneth Geers
Senior Research Scientist
Comodo Group
@KennethGeers

James C. Foster
CEO
ZeroFOX
@FirstNameFoster
Social Media

17K years old.
Seeing is Believing

Early Photoshop
Intelligent phones

National springs and color revolutions
One Internet

One Cyberspace
New Nations

- Facebook: 2,047,000,000
- YouTube: 1,500,000,000
- WhatsApp: 1,200,000,000
- Facebook Messenger: 1,200,000,000
- WeChat: 938,000,000
- QQ: 861,000,000
- Sina Weibo: 313,000,000
- Twitter: 328,000,000
- Tumblr: 357,000,000
- Baidu Tieba: 300,000,000
- Viber: 260,000,000
- Line: 214,000,000
- Instagram: 700,000,000
- QZone: 638,000,000
- Skype: 300,000,000
- Snapchat: 255,000,000
- Pinterest: 175,000,000
Old Nation-States
TILLERSON PRINTS OUT TRUMP’S TWEETS TO HELP SET FOREIGN POLICY

BY ABIGAIL TRACY
JANUARY 17, 2018 6:15 PM

The secretary of state says it’s “not a bad system.”

Foreign Policy

VANITY FAIR
Russian Bots Are Spreading False Information After The Florida Shooting

February 20, 2018 · 4:38 PM ET
Heard on All Things Considered

It's known that Russian groups used Facebook and other social media platforms to spread false information during the 2016 election, but now Russian bots are doing the same after the Florida shooting. So, how are tech giants thinking about tackling these issues?
<table>
<thead>
<tr>
<th>TWEETS</th>
<th>FOLLOWING</th>
<th>FOLLOWERS</th>
<th>FAVORITES</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,678</td>
<td>1,268</td>
<td>110K</td>
<td>30</td>
</tr>
</tbody>
</table>

**U.S. Central Command @CENTCOM**

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.*

📍 MacDill AFB, Tampa, FL

🔗 centcom.mil

📅 Joined March 2009

---

** Tweets **

**Pentagon Networks Hacked. Korean Scenarios**
Bank of Melbourne
@BankofMelb

ATTN: Unauthorised DMs sent bw 4-5pm today, do not click link. No customer/personal data compromised. Apologies for the inconvenience. ^TT
Have you asked the question...

Who’s running your social media accounts?
Account Hijacking

@vergecurrency
>privacy coin
>lead developer gets hacked
>1b $XVG stolen

2:58 PM - 13 Mar 2018
Social-Powered Social Engineering

How I Infiltrated a Fortune 500 Company with Social Engineering

Getting into the company proved surprisingly easy during a contest. Find out how to make your company better prepared for real-world attacks.
Mia Ash
Riddle, Mystery, Enigma

Propagation
Payload
Virtual Plots

Real Revolution

counterwording Counter தியுரம
@RayMajik Did you know that Facebook is disabling the accounts of activists? http://is.gd/c3sQH
27 minutes ago

counterwording Counter தியுரம
@mikeydee1010 Did you know that Facebook is disabling the accounts of activists? http://is.gd/c3sQH
1 hour ago

counterwording Counter தியுரம
@HagamosAficion Did you know that Facebook is disabling the accounts of activists? http://is.gd/c3sQH
2 hours ago

counterwording Counter தியுரம
@liannestewart Did you know that Facebook is disabling the accounts of activists? http://is.gd/c3sQH
3 hours ago
I never said Russia did not meddle in the election, I said “it may be Russia, or China or another country or group, or it may be a 400 pound genius sitting in bed and playing with his computer.” The Russian “hoax” was that the Trump campaign colluded with Russia - it never did!

12:33 PM - Feb 18, 2018

126K people are talking about this
Deep State, Deep Fake
No Pressure

Atmospheric Ignition
Employees can use social media
Employees will use social media
Social media will be exploited
There are pictures of you taken in Ukraine, and pictures of me taken in the same spot in Ukraine.
What to do?

WikiLeaks Task Force
@WLTaskForce

We are thinking of making an online database with all "verified" twitter accounts & their family/job/financial/housing relationships.

10:03 AM - 6 Jan 2017

41 80
Social threat intelligence
APPLY 1: Build a social media policy

- Work with communications teams to build a social media policy
- What can and can’t be posted?
- Who and how should employees interact online?
- How to report abuses and potential threats?
- Best practices for hardening account
- Breach notification and lost credentials
- Document policies and share with company
APPLY 2: Harden social accounts

- Enable 2FA
- Audit who has access to what accounts
- Ensure stakeholders have proper controls on personal accounts/devices
- Leverage a management platform
- Audit 3rd party applications
- Enable a monitoring tool to lock accounts in case of a takeover
APPLY 3: Train employees, work with comms

- Distribute the social media policy
- Establish employee training and testing on social media
- Monitor for abuses
- Run penetration tests
APPLY 4: Ingest data into the SOC

- Leverage network APIs to stream data into your SOC
- Leverage a social media protection platform to identify targeted threats