48%
System HACKED

# Scope of the Problem

# Scope of the Problem

# Scope of the Problem

# Scope of the Problem

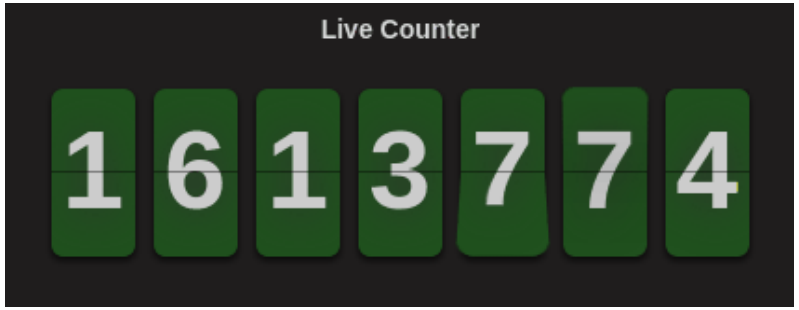
One million seconds is roughly equal to 11.5 days.

One billion seconds is roughly equal to 31.75 years.

In 2017, there were 8.4 billion IoT devices.

By 2020, that number exceeded 20.4 billion devices.

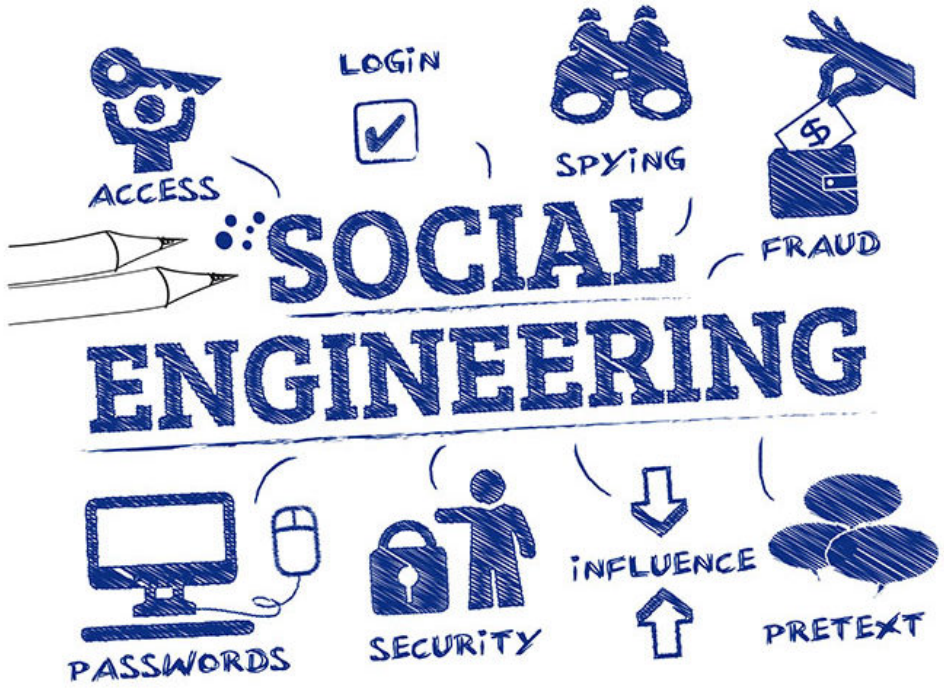
Every second, another 127 devices are connected to the internet



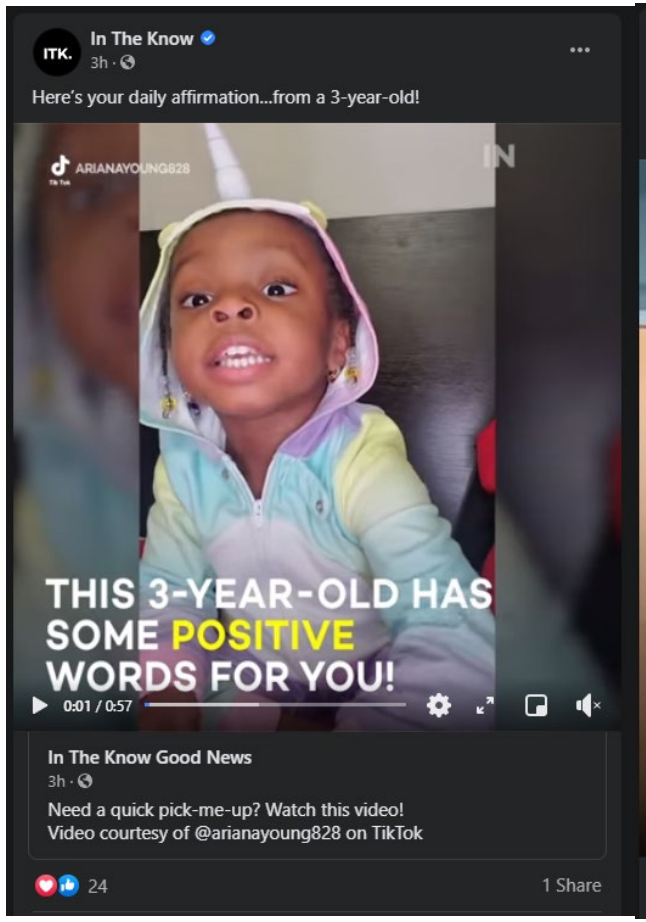
# What is Social Engineering?

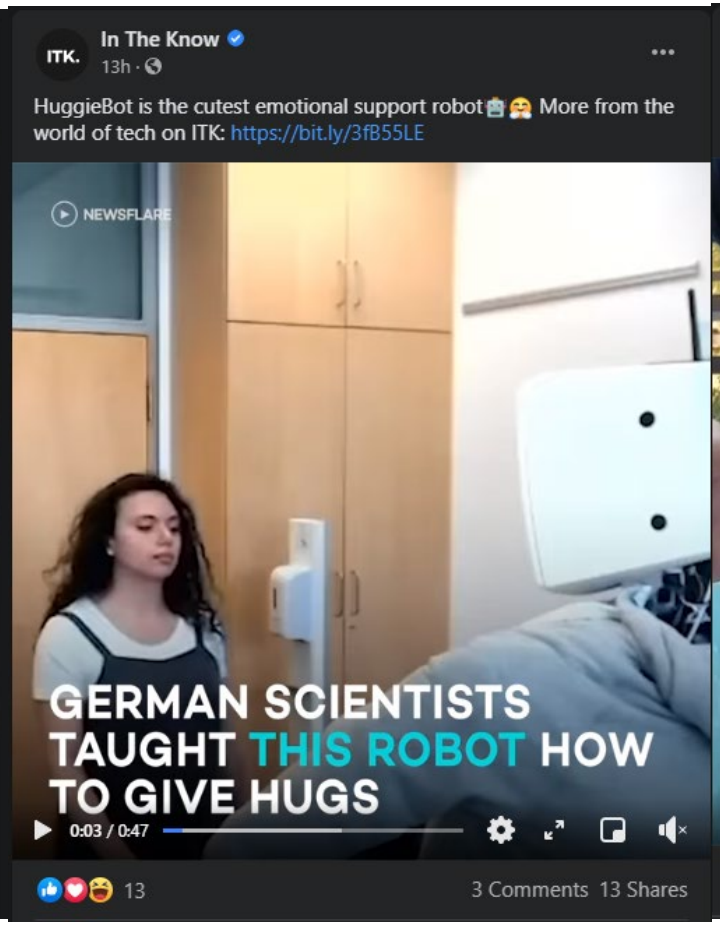
**so·cial en·gi·neer·ing**
/ˈsōSHəl ˌenjəˈni(ə)riNG/

*noun*
the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.



# Disinformation on Facebook



# Page Transparency

**In The Know**
News & Media Website

## Organizations That Manage This Page

The person or group responsible for this Page hasn't completed our verification process yet.

## Page History

**Merged with the Page Broternity**
June 10, 2020

**Merged with the Page In The Know: Life**
September 17, 2018

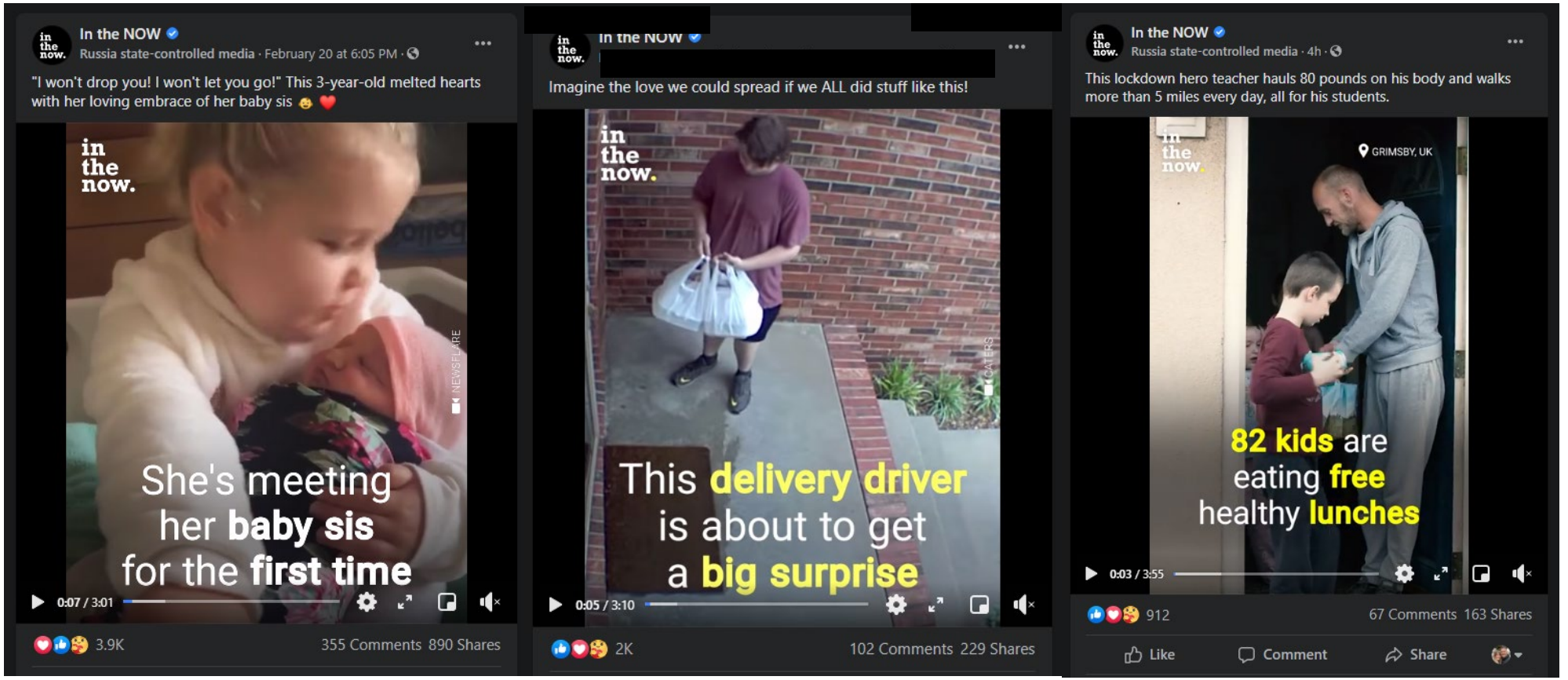
**Changed name to In The Know**
July 20, 2016

See 2 More

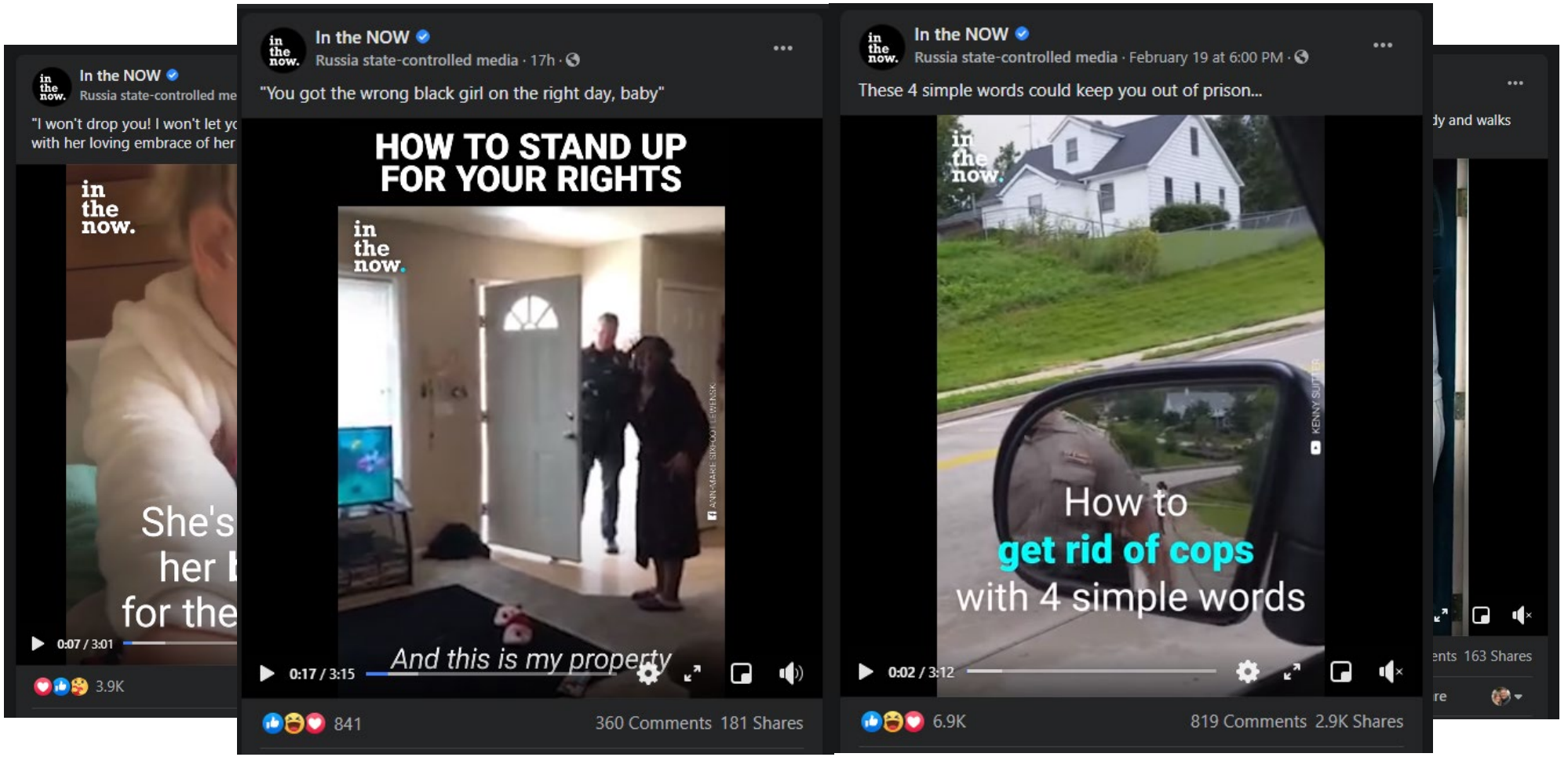
## People Who Manage This Page

**Primary country/region location for people who manage this Page includes:**
United States (93)
Australia (5)
Hong Kong (1)
Singapore (1)
Taiwan (1)

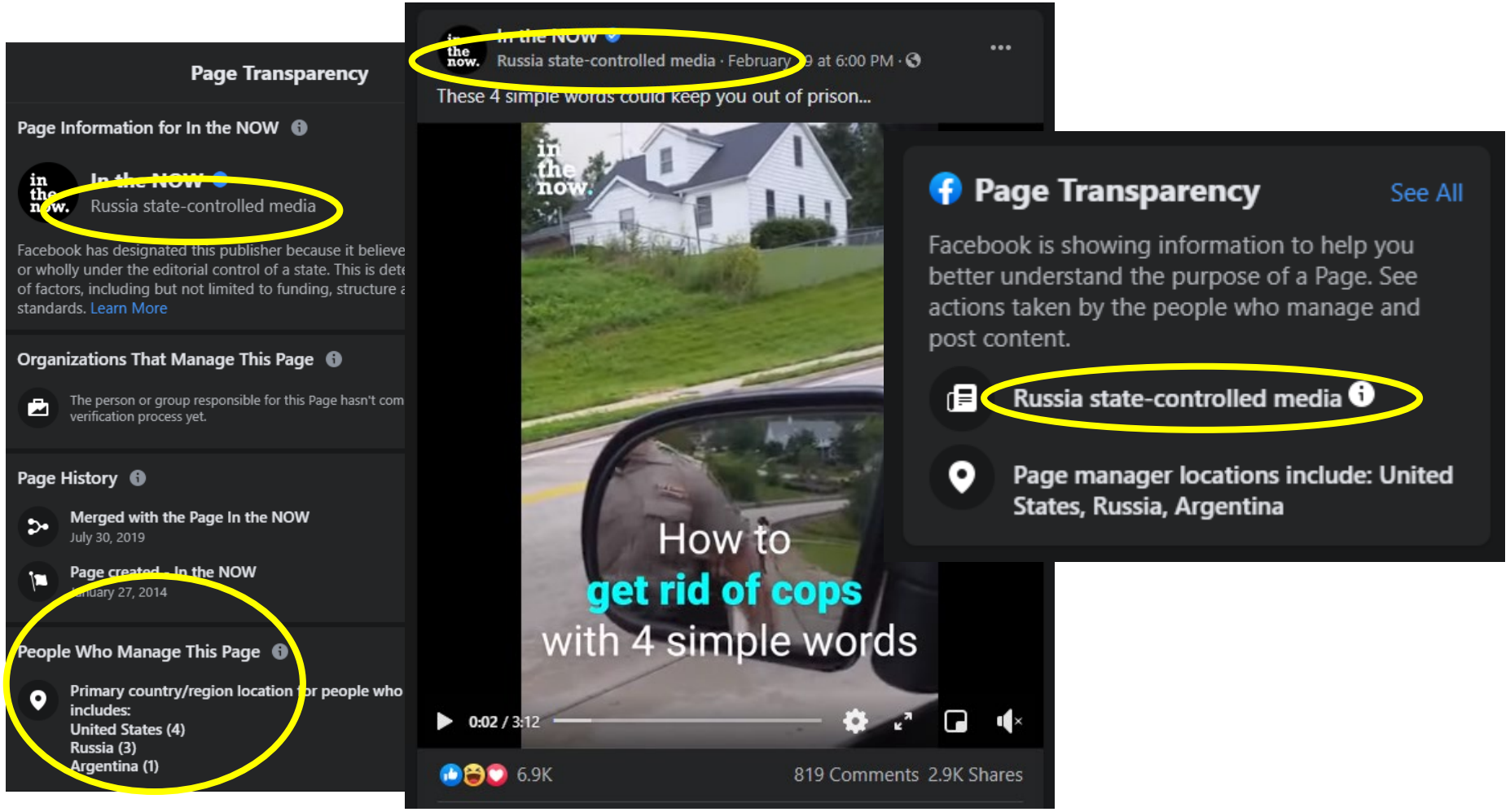
# Disinformation on Facebook



# Disinformation on Facebook



# Disinformation on Facebook



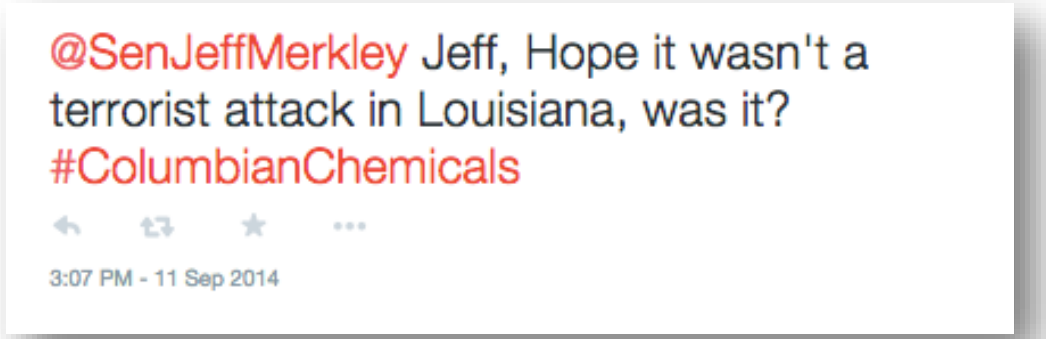
# Disinformation on Social Media

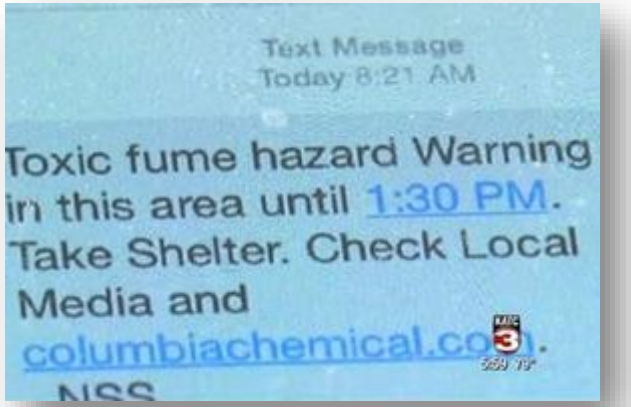
September 11th, 2014
Centerville, St Mary Parish, Louisiana

ADITYA BIRLA
BIRLA CARBON

Columbian Chemicals

# Disinformation on Social Media



The Columbian Chemicals Co explosion occurred on September 11, 2014 at a chemical plant located in Centerville, an unincorporated community in St. Mary Parish, Louisiana, United States.[1] The explosion could be a catastrophic failure of a heat exchanger.

Contents [hide]


1 Background
2 Event
3 Reaction
4 Causes
  4.1 Chemical threat
  4.2 Terrorist attack
5 Investigations
6 Aftermath
7 See also
8 References


## Background

Columbian Chemicals Co was founded in 1922 and is based in Marietta, Georgia with plants and sales offices in Centerville, Louisiana. Columbian Chemicals Company, Inc. operates as a subsidiary of Aditya Birla Management Corporation Pvt. Ltd. As of 2014, Columbian Chemicals Company, Inc. operates as a subsidiary of SKI Carbon Black (India) Private Limited.

The company manufactures carbon black additives for rubber, plastic, liquid, and other industrial applications.

## Event

The effects of the explosion were felt several miles away.

## Reaction

This section **needs expansion**. You can help by adding to it. *(September 2014)*

## Causes

This section **needs expansion**. You can help by adding to it. *(September 2014)*

### Chemical threat

According to media, there is a potential chemical threat not only to neighborhood, such as Franklin, Morgan City, Patterson and Baldwin, but also to New Orleans and Baton Rouge.

### Terrorist attack

According to media[2], the terrorist attack took place at chemical plant.

# Statement on Hoax Regarding Toxic Gas Release from Birla Carbon's Columbian Chemicals Plant Near Centerville, Louisiana

September 11, 2014

We have been informed by the community that a text message has been received by several individuals indicating a release of toxic gas from the Birla Carbon's Columbian Chemicals Plant near Centerville, Louisiana.

The content as stated by the text message is not true. There has been no release of such toxic gas, explosion or any other incident in our facility. We are not aware of the origin of this text message.

Law enforcement authorities have been contacted and are following up on this matter.

# Disinformation on Social Media

https://www.nytimes.com/2015/06/07/magazine/the-agency.html

# What is Cybersecurity?

**cy·ber·se·cur·i·ty**
/ˌsībərsiˈkyo͝orədē/

*noun*
measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Simply put, cybersecurity is protection against digital attacks.

The Department of Homeland Security says it best: “Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.”

# Colonial Pipeline incident

# Colonial Pipeline incident

May 12, 2021
7:02 PM EDT

Energy

Colonial Pipeline has no

Menu Search **Bloomberg** Sign In

Cybersecurity

## Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs
May 13, 2021, 10:15 AM EDT *Updated on May 13, 2021, 7:01 PM EDT*

- Payment came shortly after attack got underway last week
- FBI discourages organizations from paying ransom to hackers

It's not

# Regional Impact

# What's the big deal about Cybersecurity?

**Georgia State Patrol**

July, 2019 - State officials say Georgia is recovering more rapidly than expected from a ransomware attack on the Georgia State Patrol (GSP) computer system.

The hack cost the GSP much of its ability to quickly communicate with troopers in the field and put a cyber scare into much of the rest of state government, but its reach isn't as far as officials first feared.

# What's the big deal about Cybersecurity?

# Local Impact

**Jasper County Incident – Oct 2019**

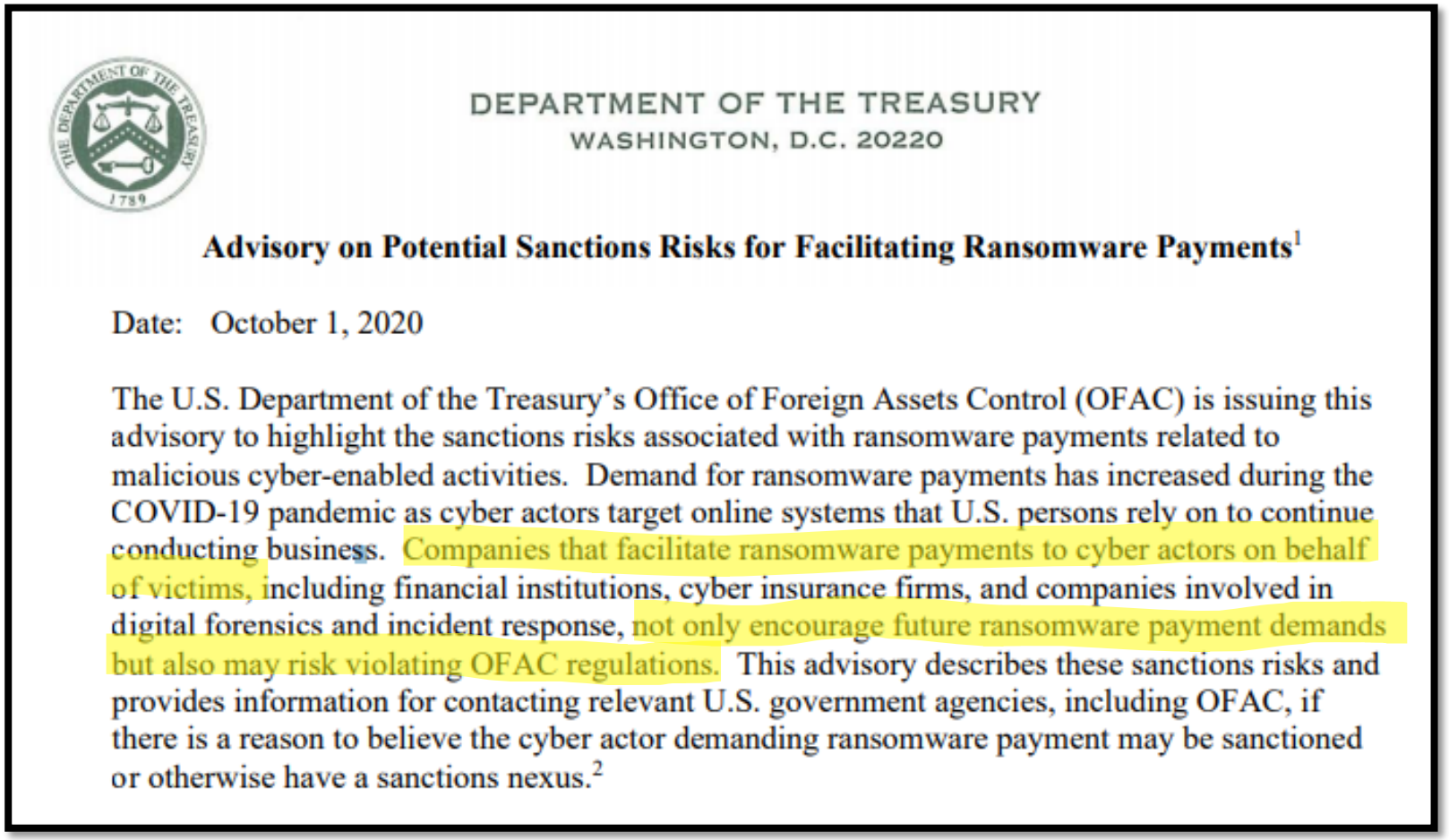
**Headline:** "County computers attacked by ransomware in Jasper County"

Jasper County is trying to get back on track after hackers were able to get into the county's computer systems. County officials say the problem started about three weeks ago.

Details on the origin of the ransomware and who put it into the system are still being investigated. Since it was found, the county has spent thousands of dollars trying to combat the issue, according to County Council Chairman Tom Johnson.

The systems are reportedly back up and running at this point, but Jasper County Sheriff Chris Malphrus is asking people to be patient when paying county taxes or bills until everything returns to normal. The sheriff also said his office will be working hard to catch up on entering data back into the system from the last few weeks.

# Local Impact



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

**Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments**[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

# Leaked Credentials

- The Verizon 2021 Data Breach Investigations Report found that 61 percent of data breaches are caused by leaked credentials.

***Credentials are highly sought out by hackers!***

- The largest password leak in history occurred in June 2021; a collection of **8.4 billion** passwords make up the stolen credential forum, further proving the value of stolen credentials, whether personal or professional.

https://www.verizon.com/business/resources/reports/dbir/
https://www.techrepublic.com/article/billions-of-passwords-leaked-online-from-past-data-breaches/

# Cyber Crime by the Numbers

**Let's put it in perspective:**

- Tesla, Facebook, Microsoft, Apple, Amazon, and Walmart combined annual revenue totals "just" **$1.28 trillion**. Cyber crime earns **$1.5 trillion** annually.
- The **$1.5 trillion** that cybercriminals earn is equal to Russia's gross domestic product (GDP)
- If cybercrime were a country, it would have the 13th highest GDP in the world.

https://www.darkreading.com/vulnerabilities---threats/cybercrime-may-be-the-worlds-third-largest-economy-by-2021/a/d-id/1337475
https://www.darkreading.com/cloud/cybercrime-is-skyrocketing-as-the-world-goes-digital/a/d-id/1331905

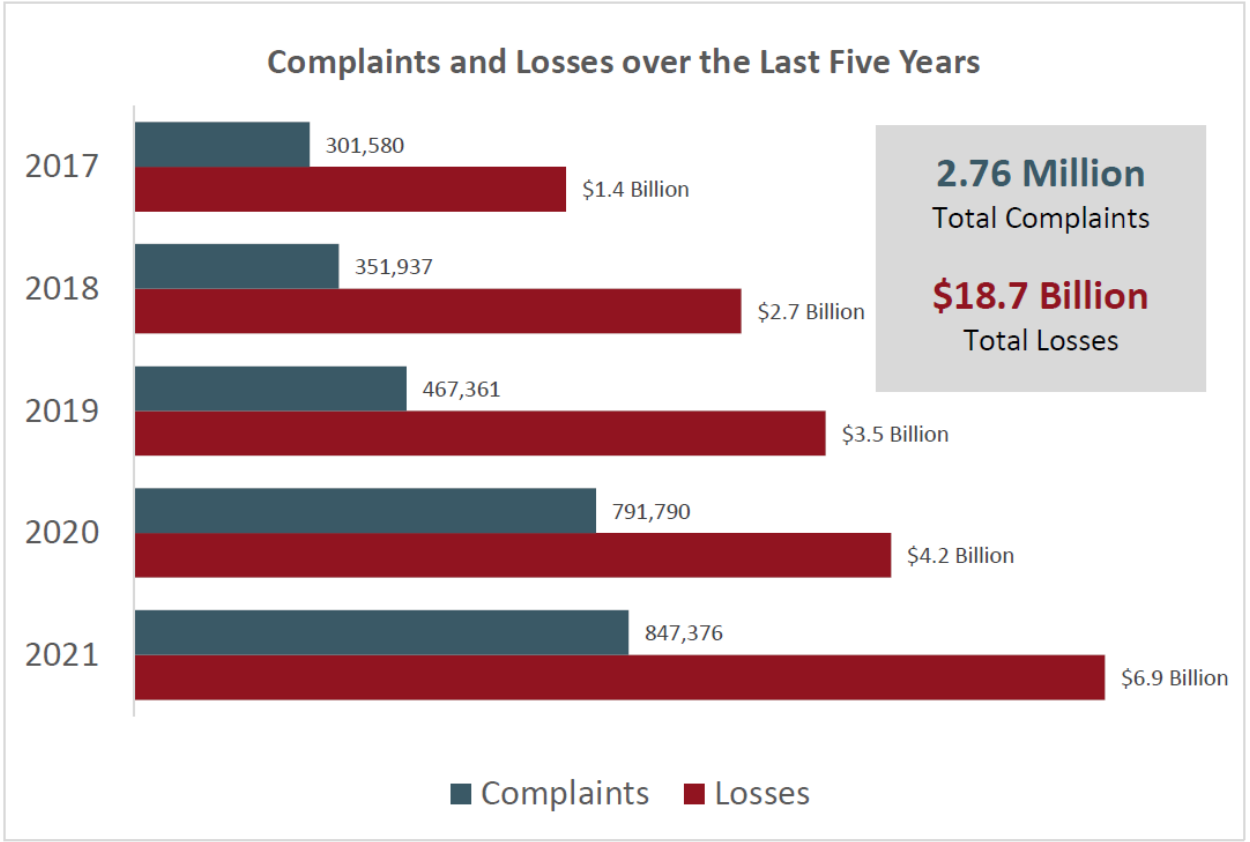
# Cyber Crime by the Numbers

**Let's put it in perspective:**

- It's estimated that cybercrime will cost the world **$10.5 trillion** annually by 2025.
- Organized criminal gangs account for **55%** of attacks
- According to the FBI's IC3's 2021 Internet Crimes Report, there were **847,376** complaints of suspected internet crimes in the US, an increase of 7% from 2020.
- Those reported losses exceeded **$6.9 billion**, an increase of 41% from 2020.

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
https://www.securitymagazine.com/articles/94842-fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report

# Internet Crimes Complaint Center (IC3.gov)




https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

# How can we help?

1. Call law enforcement. Report it. Report it to IC3!

2. Be positive advocates for change and security!

3. Ensure you have backups and test your restoration process.

4. Patch. Patch. Patch. Its not a fun process but its critical.

6. Change how you train employees. Conduct IN PERSON training as well as online. Everyone needs training!

7. Insist on multi-factor authentication for external access (email, OneDrive, VPN) to business apps and for important, personal apps for yourself (email, banking)

8. Does your organization have a cyber incident response plan? Have you ever tested it?

# How can we help?

9. Trust but verify. Have a third party come in for an audit.

10. Don’t try bypass security features and don’t let others.

11. Talk about cyber attacks in your social settings, at work, in the classroom, and at home.

Try to get others to understand the impact of the attack. Make it relatable to how it would impact their lives. We can no longer shrug it off.

# South Carolina Critical Infrastructure Cybersecurity (SC-CIC) Program

# SC Critical Infrastructure
# Cybersecurity Program

cyber@sled.sc.gov