

48%



System HACKED

```
/ address logged <[if] ret:log.origin set(278,56,34,#)if=frame origin?
[net]script src={#wq,xk,#89_method}
response?
348) [lock.command]#>>access:derial
#key-input <chair>={d fg#6 nr 4:h61l04u)
lo 1 068,789,848)
```



## Scope of the Problem





## Scope of the Problem







## Scope of the Problem





## Scope of the Problem

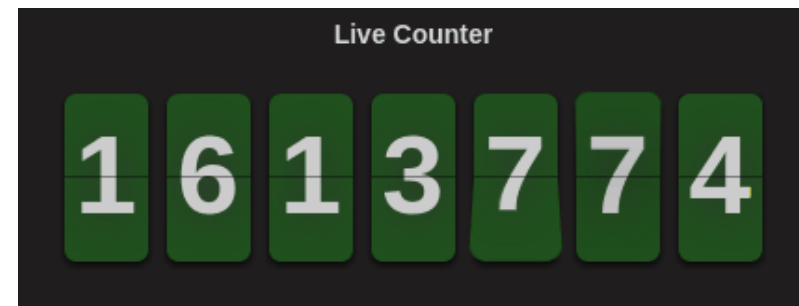
One million seconds is roughly equal to 11.5 days.

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





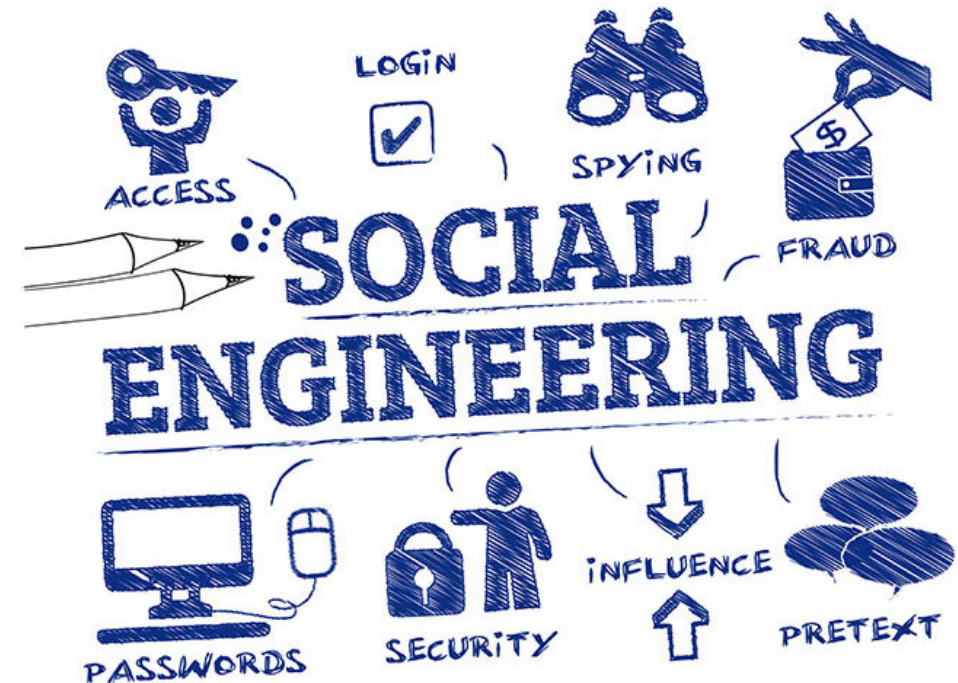
## What is Social Engineering?

so·cial en·gi·neer·ing

/ˈsōSHəl ˌenjəˈni(ə)rɪŋ/

*noun*

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





## Disinformation on Facebook

**ITK. In The Know** 3h · 🌐

Here's your daily affirmation...from a 3-year-old!

**THIS 3-YEAR-OLD HAS SOME POSITIVE WORDS FOR YOU!**

0:01 / 0:57

In The Know Good News  
3h · 🌐

Need a quick pick-me-up? Watch this video!  
Video courtesy of @arianayoung828 on TikTok

24 1 Share

**ITK. In The Know** 13h · 🌐

HuggieBot is the cutest emotional support robot 🤖💖 More from the world of tech on ITK: <https://bit.ly/3fB55LE>

**GERMAN SCIENTISTS TAUGHT THIS ROBOT HOW TO GIVE HUGS**

0:03 / 0:47

13 3 Comments 13 Shares

**ITK. In The Know** 14h · 🌐

Innovative tool allows users to clean paint rollers in seconds 🛠️ More from the world of tech on ITK: <https://bit.ly/3fB55LE>

**THIS GENIUS GADGET HELPS PREVENT MESSSES...**

0:05 / 0:37

424 131 Comments 168 Shares



## 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

Three Facebook posts from the account "In the NOW" (Russia state-controlled media) are displayed side-by-side, each featuring a video and a text overlay.

**Post 1 (Left):** The video shows a young girl hugging a baby. The text overlay reads: "I won't drop you! I won't let you go!" This 3-year-old melted hearts with her loving embrace of her baby sis 🥰❤️. Below the video, it says "She's meeting her baby sis for the first time". Engagement: 3.9K likes, 355 Comments, 890 Shares.

**Post 2 (Middle):** The video shows a delivery driver standing on a sidewalk with a large white bag. The text overlay reads: "Imagine the love we could spread if we ALL did stuff like this!". Below the video, it says "This delivery driver is about to get a big surprise". Engagement: 2K likes, 102 Comments, 229 Shares.

**Post 3 (Right):** The video shows a man in a grey hoodie interacting with a young boy. The text overlay reads: "This lockdown hero teacher hauls 80 pounds on his body and walks more than 5 miles every day, all for his students." Below the video, it says "82 kids are eating free healthy lunches". Location: GRIMSBY, UK. Engagement: 912 likes, 67 Comments, 163 Shares.



## Disinformation on Facebook

Three overlapping screenshots of Facebook posts from the page "In the NOW" (Russia state-controlled media). The posts feature videos with inflammatory titles and content.

**Post 1 (Left):** The video shows a person in a white hoodie. The text overlay reads: "She's her for the". The video has 3.9K likes and 0:07 / 3:01 duration.

**Post 2 (Center):** The video shows a man and a woman in a doorway. The text overlay reads: "HOW TO STAND UP FOR YOUR RIGHTS" and "And this is my property". The video has 841 likes, 360 comments, and 181 shares. The duration is 0:17 / 3:15.

**Post 3 (Right):** The video shows a car's side mirror reflecting a police officer. The text overlay reads: "How to get rid of cops with 4 simple words". The video has 6.9K likes, 819 comments, and 2.9K shares. The duration is 0:02 / 3:12.



## Disinformation on Facebook

The image shows a Facebook post from the page "In the NOW" (Russia state-controlled media) dated February 9 at 6:00 PM. The post text reads: "These 4 simple words could keep you out of prison...". The video content shows a white house and a car's side-view mirror with the text "How to get rid of cops with 4 simple words". The video has 6.9K likes, 819 comments, and 2.9K shares.

Overlaid on the left is the "Page Transparency" section for "In the NOW". It includes the following information:

- Page Information for In the NOW**: States that Facebook has designated this publisher as "Russia state-controlled media" because it believes or wholly under the editorial control of a state. A "Learn More" link is provided.
- Organizations That Manage This Page**: States that the person or group responsible for this Page hasn't completed the verification process yet.
- Page History**: Shows the page was merged with the Page "In the NOW" on July 30, 2019, and was created on January 27, 2014.
- People Who Manage This Page**: Lists the primary country/region location for people who include: United States (4), Russia (3), and Argentina (1).

Overlaid on the right is another "Page Transparency" section, which states: "Facebook is showing information to help you better understand the purpose of a Page. See actions taken by the people who manage and post content." It lists the page manager locations as: United States, Russia, and Argentina.





## Disinformation on Social Media



September 11<sup>th</sup>, 2014  
Centerville, St Mary Parish, Louisiana



Columbian Chemicals



## Disinformation on Social Media

 **Anna Russel**  
@AnnRussela

⚙️ Follow

Chemical plant exploded in Centerville,  
Louisiana [#ColumbianChemicals](#)

⬅️ ↻ ⭐ I ...



RETWEETS 376 FAVORITES 2

8:29 AM - 11 Sep 2014

@SenJeffMerkley Jeff, Hope it wasn't a  
terrorist attack in Louisiana, was it?  
[#ColumbianChemicals](#)

⬅️ ↻ ⭐ ...

3:07 PM - 11 Sep 2014

Text Message  
Today 8:21 AM

Toxic fume hazard Warning  
in this area until **1:30 PM**.  
Take Shelter. Check Local  
Media and  
[columbiachemical.com](#).  
NCS

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](#).<sup>[1]</sup> 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<sup>[2]</sup>, 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  
/ˌsībərˈsiˈkyʊrədē/

*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

NEWS

Full Episodes Podcasts Subscribe Live

**'Panic buying' is driving the fuel shortage after Colonial Pipeline hack, expert says**

May 11, 2021 6:45 PM EDT

buyers that love your sty

An aerial photograph of a large parking lot filled with numerous cars, likely at a gas station or retail center, is visible at the bottom of the news snippet.



## 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 under way last week
- ▶ FBI discourages organizations from paying ransom to hackers

It's not





## Regional Impact

### Cyberattack Hit 10% of Servers

Louisiana's technology office says one in ten of the 5,000 core servers were hit by this week's cyberattack.

By Associated Press, Wire Service Content Nov. 22, 2019, at 12:15 p.m.



### Ryuk ransomware implicated in City of New Orleans shutdown

Adam Bannister 18 December 2019 at 12:57 UTC  
Updated: 06 January 2020 at 11:26 UTC

Cyber-attacks Ransomware Government

The malware has struck several US municipalities in 2019



**ANALYSIS** The cyber-attack that prompted the City of New Orleans' mayor to declare a state of emergency on Friday (December 13) is the latest in a string of attacks on city and state governments to be linked to the Ryuk ransomware.

LETTERS EVENTS PAPERS NAVIGATOR SEARCH

GovTech Biz Emerging Tech Cloud Gov

### After Louisiana

Offices remained closed Monday as state officials investigated the impact of a cyberattack that hit state servers two days ago.







# What's the big deal about Cybersecurity?

## Georgia State Patrol

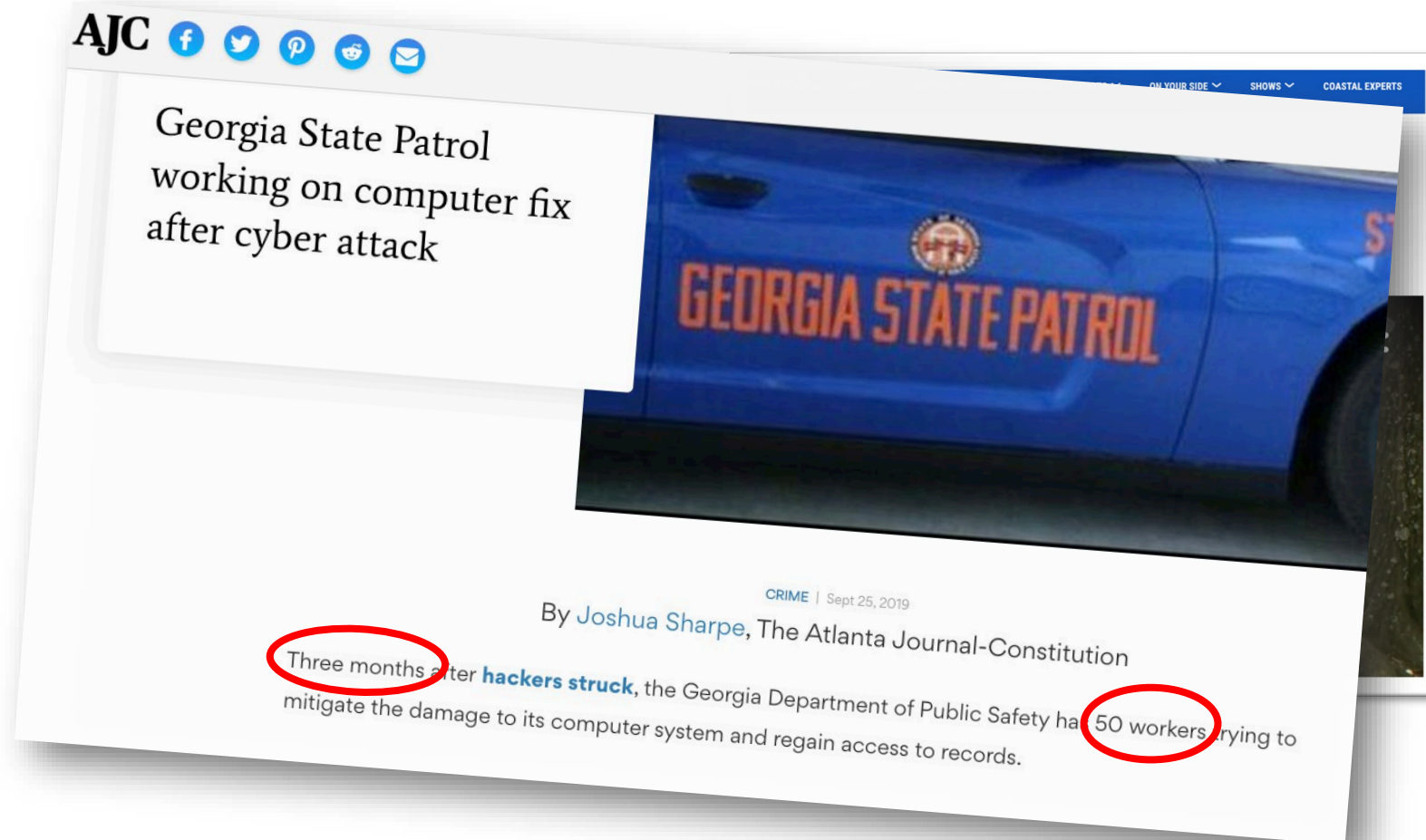
July, 2019 - State officials say Georgia is recovering more rapidly than expected from a ransomware attack on the Georgia State Patrol (GSP) computer system.

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<sup>1</sup>**

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.<sup>2</sup>



## 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.

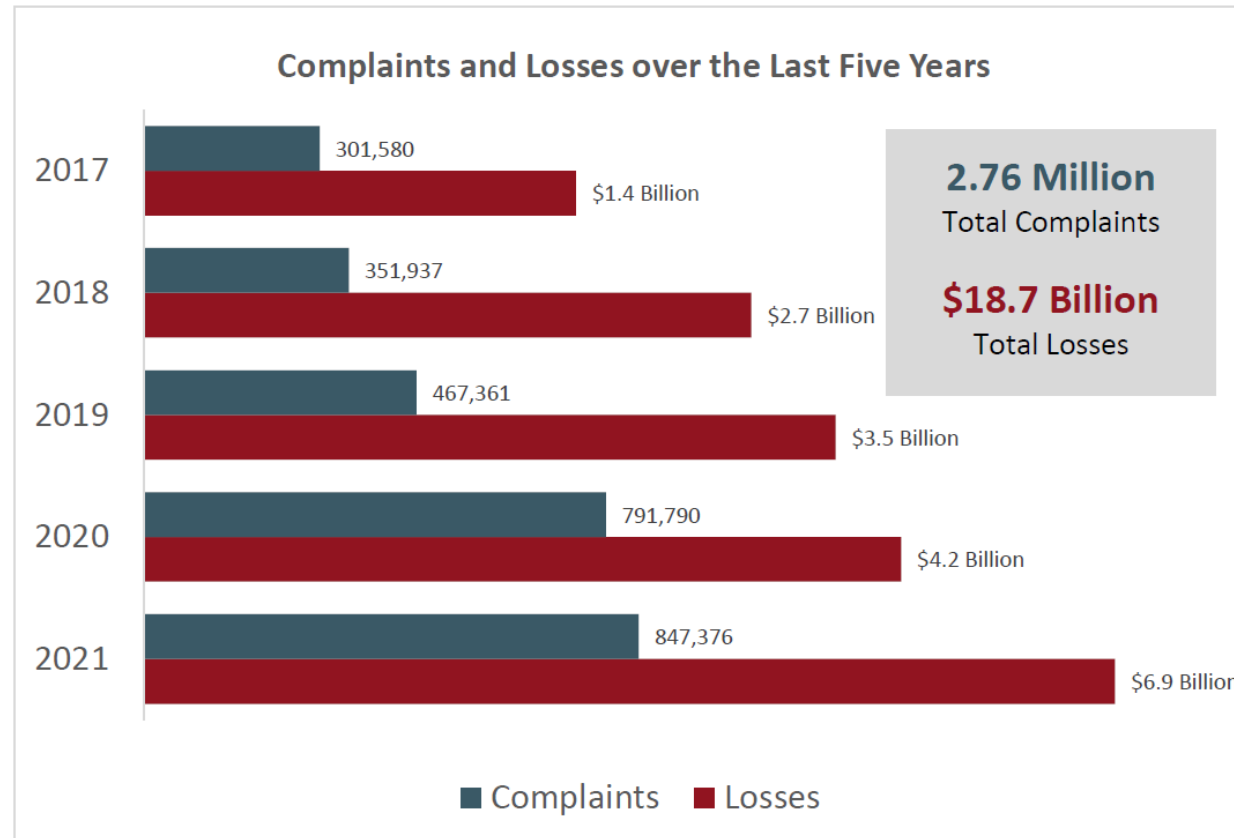


[https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

<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](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

VULNERABILITY  
SCANNING



ACTIVE DIRECTORY  
SECURITY ASSESSMENT



CYBER POSTURE  
REVIEW



INCIDENT  
RESPONSE



ADVERSARY  
EMULATION



CYBER THREAT  
INTELLIGENCE



CYBERSECURITY  
TRAINING







[cyber@sled.sc.gov](mailto:cyber@sled.sc.gov)