PRIVACY AT RISK:

THE DANGERS OF PII/PHI IN RENTAL/LEASE CARS LEFT BEHIND

By: Chris "BLu3f0x" Huffstetler

#WHOAMI

- US Army 9 years in Communications Security 25C/25S
- Several years as DoD and DoS contractor(CONUS & OCONUS)on secure communication networks
- DoS ComSec Custodian – Afghanistan
- Currently a web app penetration tester for 5 months with background on Network PenTest/Incident Response/AppSec

- Associate Degrees in General Studies and Cyber Security
- Graduate of PHSC Law Enforcement Academy – 2015
- Once a upon a time, I did have Security+ce

- Member of:
- InfraGard – Tampa Chapter
- US Marine Corp Cyber Auxiliary
- HackMiami, DC813, DC727, BSides Orlando
- Cyber Security Forum Initiative, Diana Initiative
- OWASP Tampa Bay

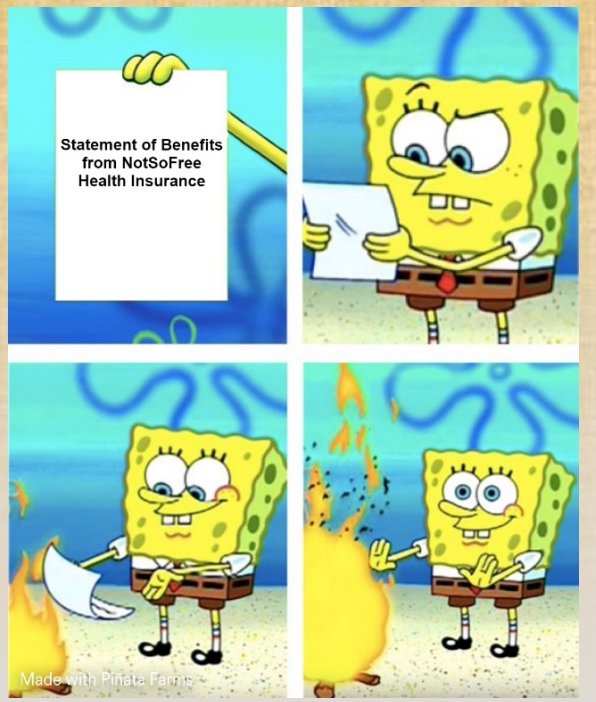
STATS A.K.A. SOME INTERESTING NUMBERS

- **There were about 44.5 million cars rented in the U.S. in 2019.**
- In 2020, however, there were only about 17.3 million cars rented. Almost twice as many were rented in 2021 (29.2 million) as in 2020, and it's estimated that the industry will see 46.8 million rentals in 2024.

- Source: 20 Crash-Tested Car Rental Industry Statistics [2023]: What Is The Car Rental Industry - Zippia

LET'S TALK ABOUT PAPER INFORMATION

Paper documents are still being required for some services

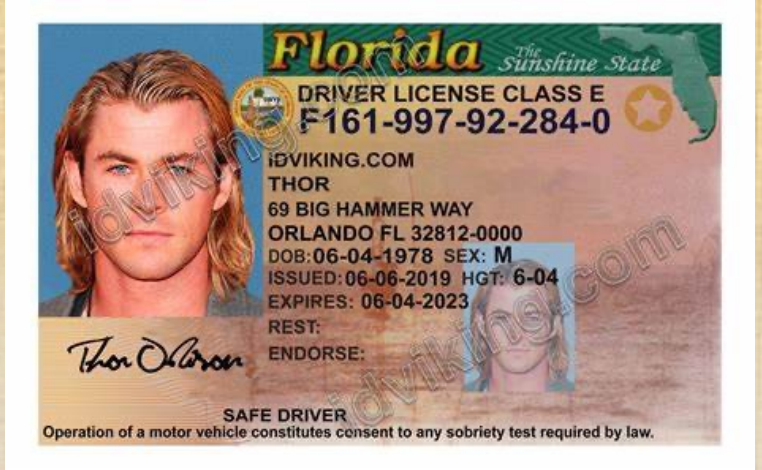


WHAT IS PII/PHI?

- **Personally Identifiable Information (PII)**: Information that can be used to identify an individual, such as name, home address, and social security number
  - PII is sensitive because it can be used for identity theft and other malicious purposes
- **Protected Health Information (PHI)**: Information related to an individual's health status or medical treatment, such as medical records and prescriptions
  - PHI is sensitive because it can be used to discriminate against individuals or compromise their medical privacy

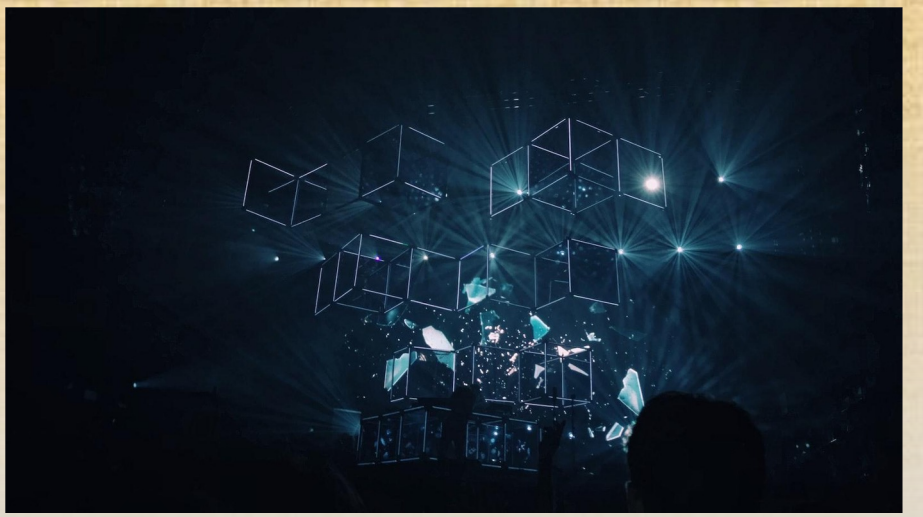
PII/PHI IN RENTAL/LEASE CARS

- **Types of PII/PHI**: Driver's license, credit card information, medical records, and other personal information
  - PII/PHI can be left behind in rental/lease cars by previous renters or owners
- **Risks of Data Breaches**: Identity theft, financial fraud, medical identity theft, and other malicious activities
  - Data breaches can have serious consequences for individuals and businesses



COMMON CAUSES OF DATA BREACHES

- **Theft**: Unauthorized access to rental/lease cars or their contents
  - Theft can occur through physical or digital means
- **Loss**: Accidental misplacement or abandonment of rental/lease cars or their contents
  - Loss can occur due to human error or other factors
- **Improper Disposal**: Failure to properly dispose of rental/lease cars or their contents
  - Improper disposal can occur due to lack of awareness or negligence



DATA BREACHES THAT AFFECTED ME

- ## OPM Breach
- In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting personnel records. Approximately 22.1 million records were affected, including records related to government employees, other people who had undergone background checks, and their friends and family.

- ## Equifax Breach
- September 2017, Equifax announced a cyber-security breach, which it claims to have occurred between mid-May and July 2017, where cybercriminals accessed approximately 145.5 million U.S. Equifax consumers' personal data, including their full names, Social Security numbers, birth dates, addresses, and driver license numbers. Equifax also confirmed at least 209,000 consumers' credit card credentials were taken in the attack. On March 1, 2018, Equifax announced that 2.4 million additional U.S. customers were affected by the breach, increasing the number of affected to 147.9 million Americans. The company claims to have discovered evidence of the cybercrime event on July 29, 2017. Residents in the United Kingdom (15.2 million) and Canada (about 19,000) were also impacted. The vulnerability in which Chinese hackers leveraged was CVE-2017-5638, the hackers managed to stay in Equifax systems undetected for approximately 134 days.

LEGAL AND REGULATORY FRAMEWORK

- **General Data Protection Regulation (GDPR)**: European Union regulation governing data privacy and protection
  - Applies to all organizations that process personal data of EU citizens
- **California Consumer Privacy Act (CCPA)**: California state law governing data privacy and protection
  - Applies to all organizations that process personal data of California residents
- **Health Insurance Portability and Accountability Act (HIPAA)**: US federal law governing medical privacy and protection
  - Applies to all organizations that handle protected health information

IMPACT OF DATA BREACHES

Individuals: Loss of privacy, identity theft, financial fraud, and other negative consequences

- Data breaches can have serious consequences for individuals, including financial losses and emotional distress

Businesses: Reputational damage, legal liability, and financial losses

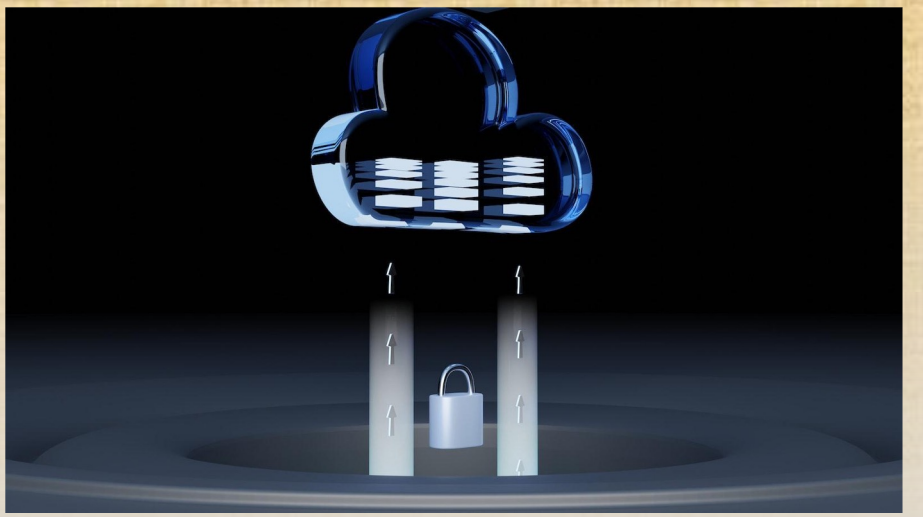
- Data breaches can have serious consequences for businesses, including loss of customer trust and legal penalties

Society: Erosion of trust, loss of confidence in institutions, and other negative consequences

- Data breaches can have serious consequences for society as a whole, including erosion of trust in institutions and loss of confidence in the ability of organizations to protect sensitive data

PREVENTION STRATEGIES

- **Employee Training**: Educate employees on data privacy best practices and the importance of protecting sensitive data
  - Training can help to reduce the risk of human error and improve overall data security
- **Encryption**: Use encryption to protect sensitive data from unauthorized access or disclosure
  - Encryption can help to prevent data breaches and protect sensitive data from theft or loss
- **Secure Disposal**: Properly dispose of rental/lease cars and their contents to prevent unauthorized access or disclosure
  - Secure disposal can help to prevent data breaches and protect sensitive data from theft or loss



RESPONSE PLAN

- **Importance of Response Plan**: A response plan is essential for minimizing the impact of data breaches and protecting sensitive data
  - A well-designed response plan can help to reduce the risk of further data breaches and protect sensitive data from unauthorized access or disclosure
- **Guidance on Developing and Implementing a Response Plan**: Develop a response plan that includes clear procedures for identifying, containing, and mitigating data breaches
  - Implement the response plan through regular training and testing to ensure that it is effective and up-to-date

COMPLIANCE AND AUDITING

- **Importance of Compliance and Auditing**: Compliance and auditing are essential for maintaining data privacy in rental/lease cars and ensuring that organizations are meeting legal and regulatory requirements
  - Compliance and auditing can help to identify areas of weakness and improve overall data security
- **Best Practices for Compliance and Auditing**: Implement regular compliance and auditing procedures, including risk assessments, vulnerability scans, and penetration testing
  - Use industry standards and best practices to guide compliance and auditing efforts

INDUSTRY STANDARDS AND BEST PRACTICES

Data Privacy in Rental/Lease Cars

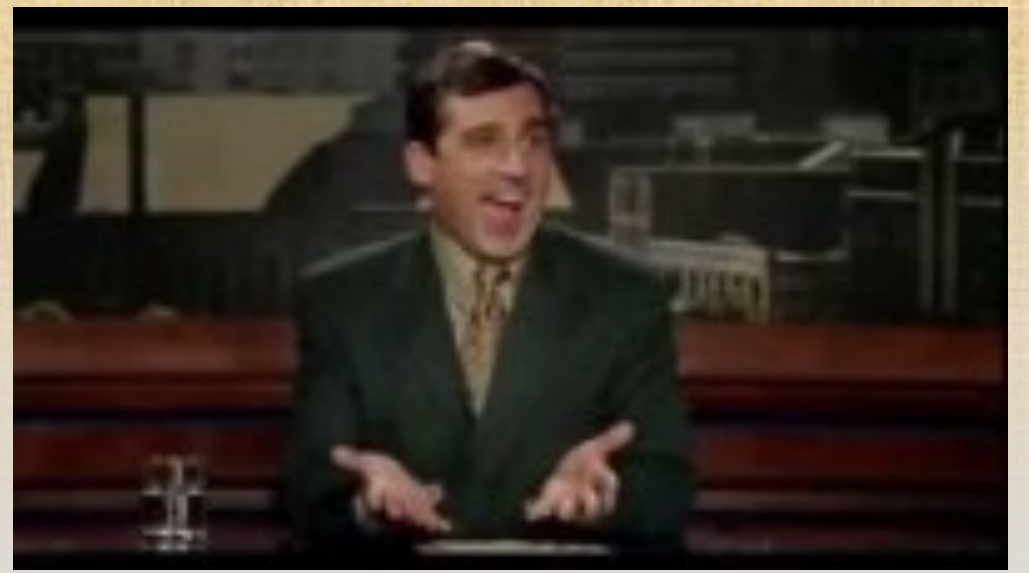
- **Industry Standards**: NIST Cybersecurity Framework, ISO 27001, and other industry standards provide guidance on data privacy and protection
  - Organizations can use these standards to guide their data privacy efforts and ensure that they are meeting best practices
- **Best Practices**: Implement data encryption, access controls, and other best practices to protect sensitive data
  - Use secure disposal methods and employee training to reduce the risk of data breaches

CASE STUDY

- **Case Study**: Rental car company SixtRent-A-Car in Germany experiences data breach due to a cyber attack in 2022
  - Sixt Rent-a-Car, LLC confirmed that the company experienced a data breach after an unauthorized party gained access to sensitive consumer data contained on the network. Based on the available information, it appears as though the incident affected employees, their dependents, and possibly customers.

I EMAILED A MAJOR CAR COMPANY

- So back in 2019 before BSides Puerto Rico, I did email a major car company regarding the bluetooth profiles that contain PII and MAC address from the previous owner.
- There was no response back from this car company.
- My wishful reply:



CONCLUSION

Treat your car like a Hard Drive

- Data privacy is essential for protecting sensitive information in rental/lease cars
- PII and PHI are two types of sensitive data that require special protection
- Common causes of data breaches include theft, loss, and improper disposal
- Compliance and auditing are essential for maintaining data privacy and meeting legal and regulatory requirements
- Prevention strategies, response plans, and industry standards can all help to reduce the risk of data breaches and protect sensitive data
- Reduce your information surface from attack/loss/theft

QUESTIONS?

TREAT YOUR CAR LIKE A HARD DRIVE

BECAUSE THERE ARE OTHERS WHO WILL SELL OR STEAL YOUR INFORMATION

WE ARE NOW MOVING TO A PRACTICAL PORTION OF THE TALK OUTSIDE FOR 5 MINS
PLEASE JOIN ME OTHERWISE HAVE A GOOD DAY