CYBER
SECURITY:
AWARENESS

UNDERSTANDING THREATS AND BEST PRACTICES

RUSHI MOLIYA AU2240020
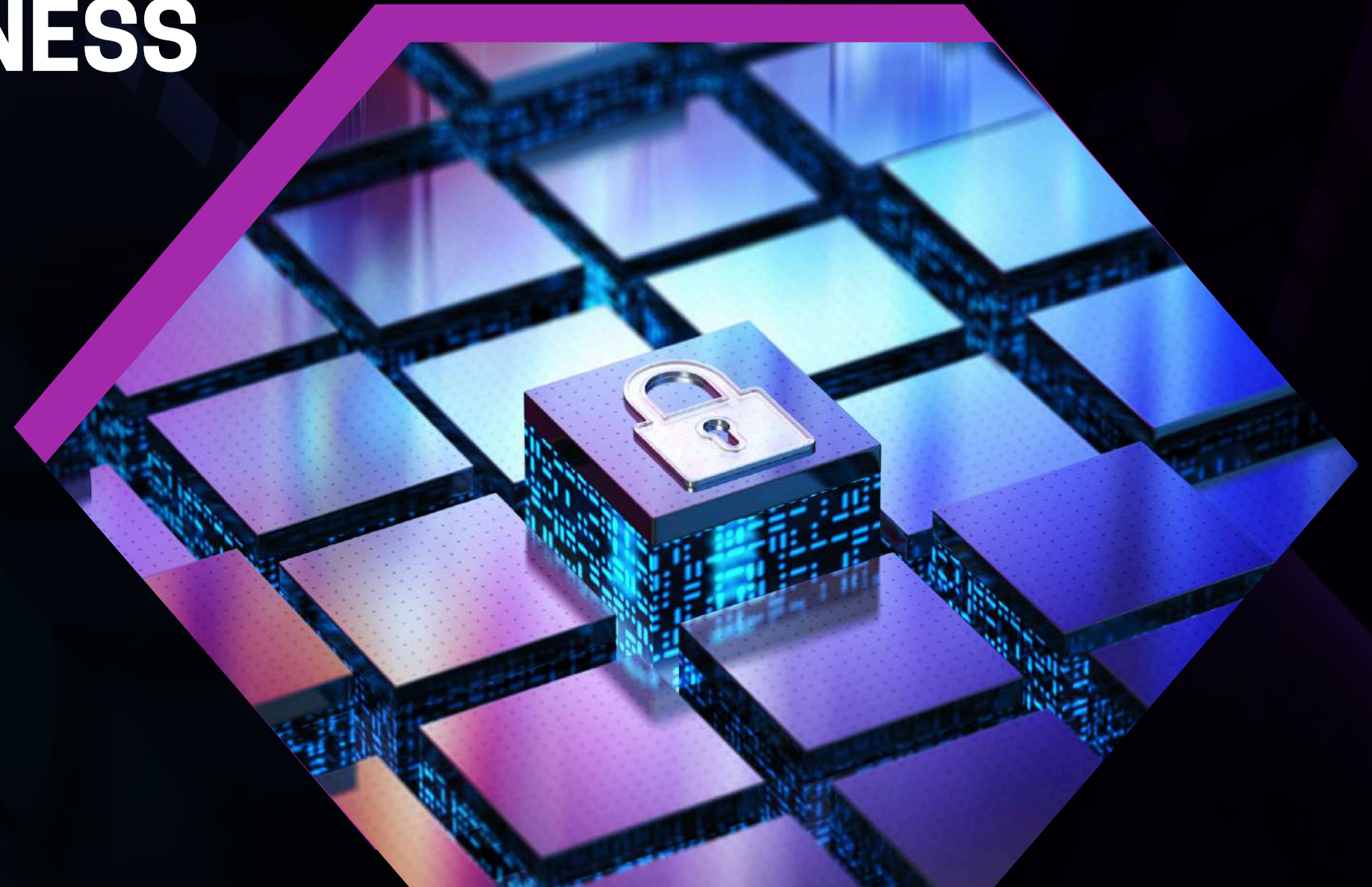
RUSHI MOLIYA AU2240020

INTRODUCTION
CYBERSECURITY AWARENESS

The knowledge of cyber threats and ways to protect personal & organizational data.

Why It's Important:
- Cybercrime costs $4.88M per breach (IBM, 2024)
- 80% of breaches result from human error (Verizon, 2022)

LEARN MORE

WHAT DO YOU
PHISHING?

- Definition: Fake emails or messages trick users into revealing data.
- Impact: 30% of breaches involve phishing (Verizon, 2022)
- Prevention: Verify sender details, don't click unknown links.

WHAT DO YOU
SOCIAL ENGINEERING?

- Definition: Fake emails or messages tricking users into revealing data.
- Impact: 30% of breaches involve phishing (Verizon, 2022)
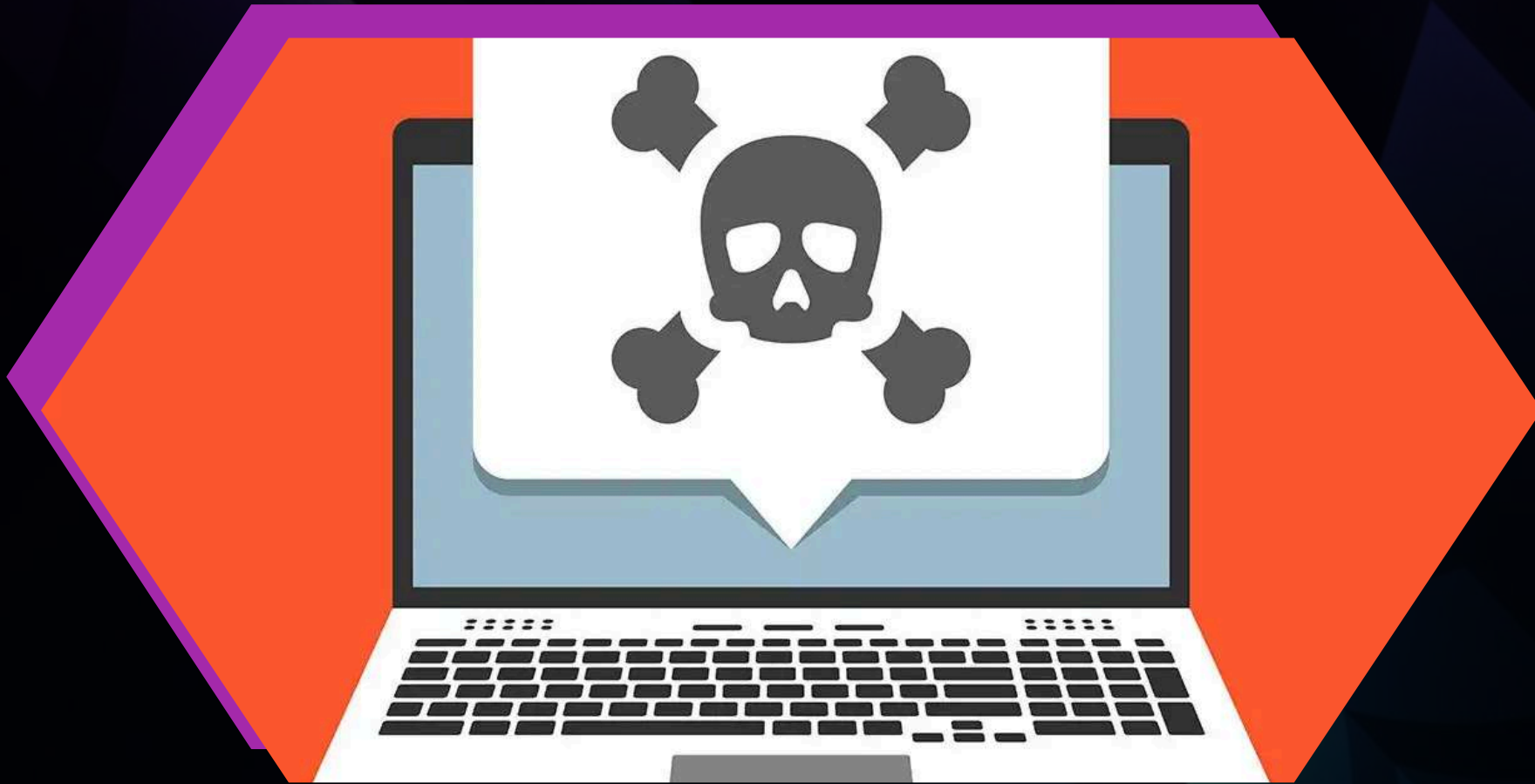- Prevention: Verify sender details, don't click unknown links.

WHAT DO YOU
RANSOMWARE?

- Definition: Malware encrypts files, demanding ransom for access.
- Impact: $5.12M average cost per attack (IBM, 2024)
- Prevention: Regular backups, strong security policies.

RUSHI MOLIYA AU2240020

WHAT DO YOU MALWARE?

- Definition: Harmful software that steals or damages data.
- Impact: Spreads via downloads, USBs, email attachments.
- Prevention: Install antivirus, don't download unverified files.
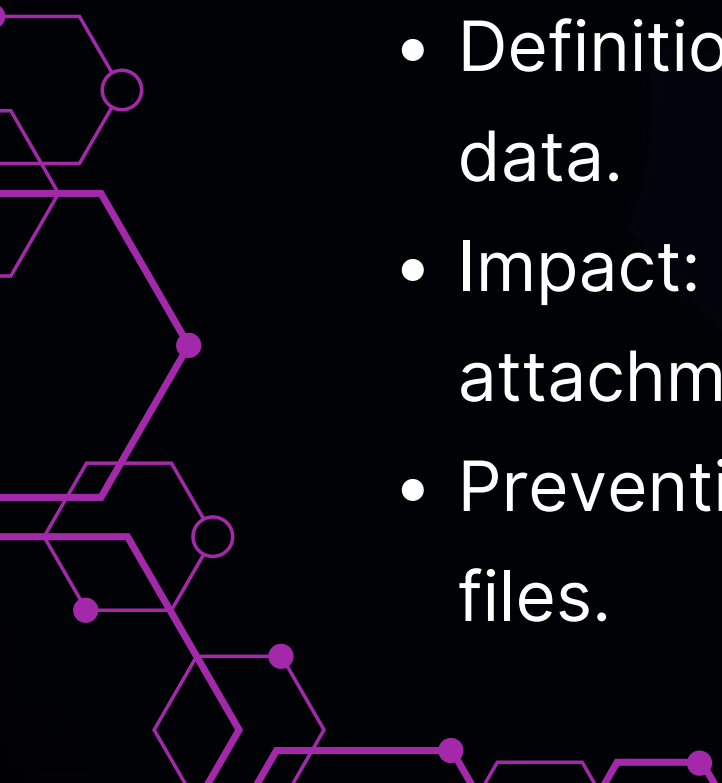
WHAT DO YOU
DDOS ATTACKS?

- Definition: Overloading a server to make it unavailable.
- Impact: Disrupts business operations, government services.
- Prevention: Use firewalls & anti-DDoS solutions.

RUSHI MOLIYA AU2240020

WannaCry Ransomware

REAL-WORLD CYBERSECURITY INCIDENTS

WANNACRY RANSOMWARE ATTACK (2017)

- **Impact**: Hit 200,000+ computers in 150 countries.

- **Lessons**: Update software, back up data.

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin
ACCEPTED HERE

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw   Copy

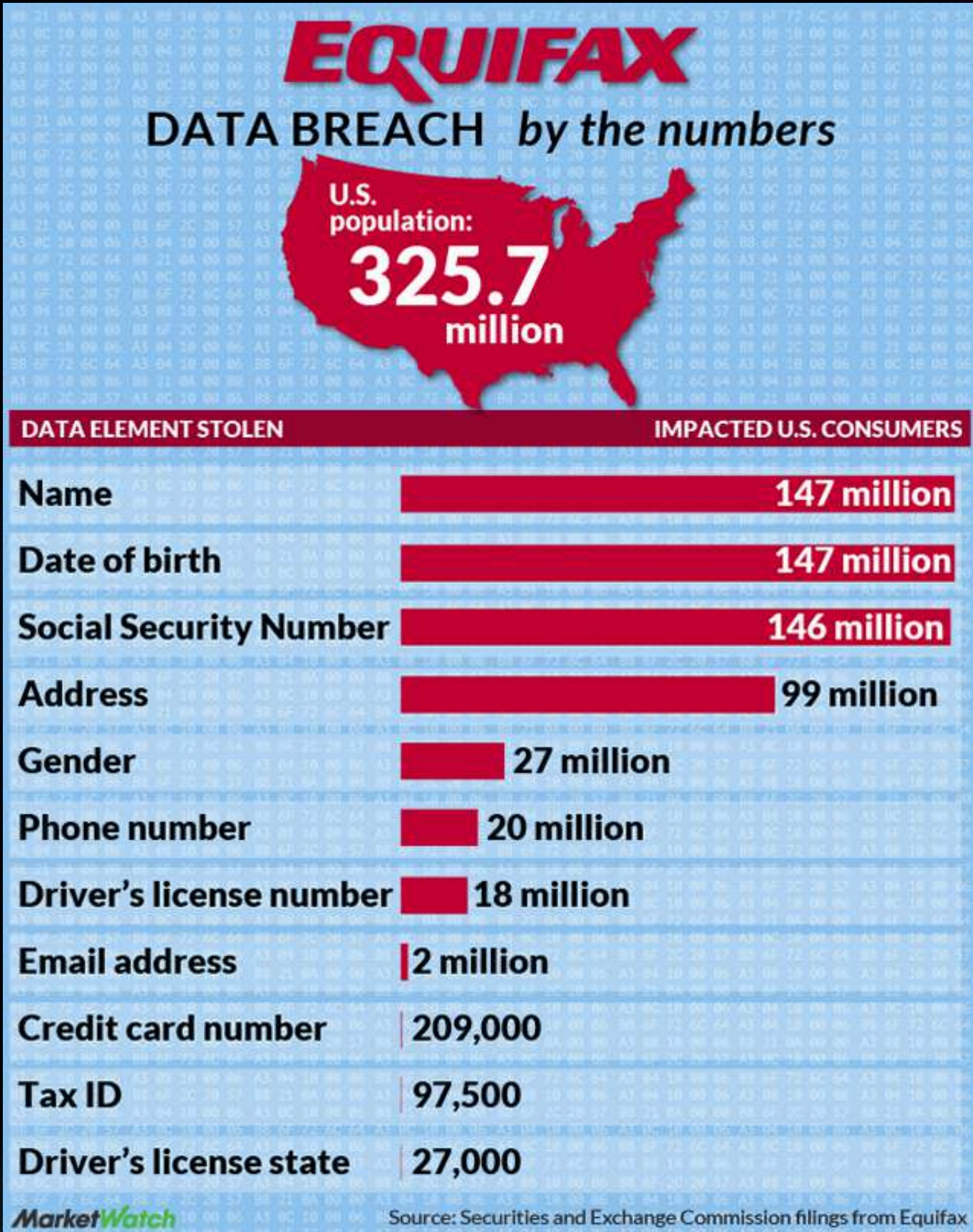Check Payment   Decrypt

REAL-WORLD CYBERSECURITY INCIDENTS

EQUIFAX DATA BREACH (2017)

- **Impact: 147 million users' sensitive data exposed.**

- **Lessons: Patch systems, monitor for suspicious activity.**

EQUIFAX
DATA BREACH *by the numbers*

U.S. population: 325.7 million

DATA ELEMENT STOLEN	IMPACTED U.S. CONSUMERS
Name	147 million
Date of birth	147 million
Social Security Number	146 million
Address	99 million
Gender	27 million
Phone number	20 million
Driver's license number	18 million
Email address	2 million
Credit card number	209,000
Tax ID	97,500
Driver's license state	27,000

MarketWatch   Source: Securities and Exchange Commission filings from Equifax

REAL-WORLD CYBERSECURITY INCIDENTS

SOLARWINDS SUPPLY CHAIN ATTACK (2020)

- **Impact:** US agencies and global businesses are affected by malware-infected software updates.

- **Lessons:** Secure supply chains, adopt zero-trust policies.
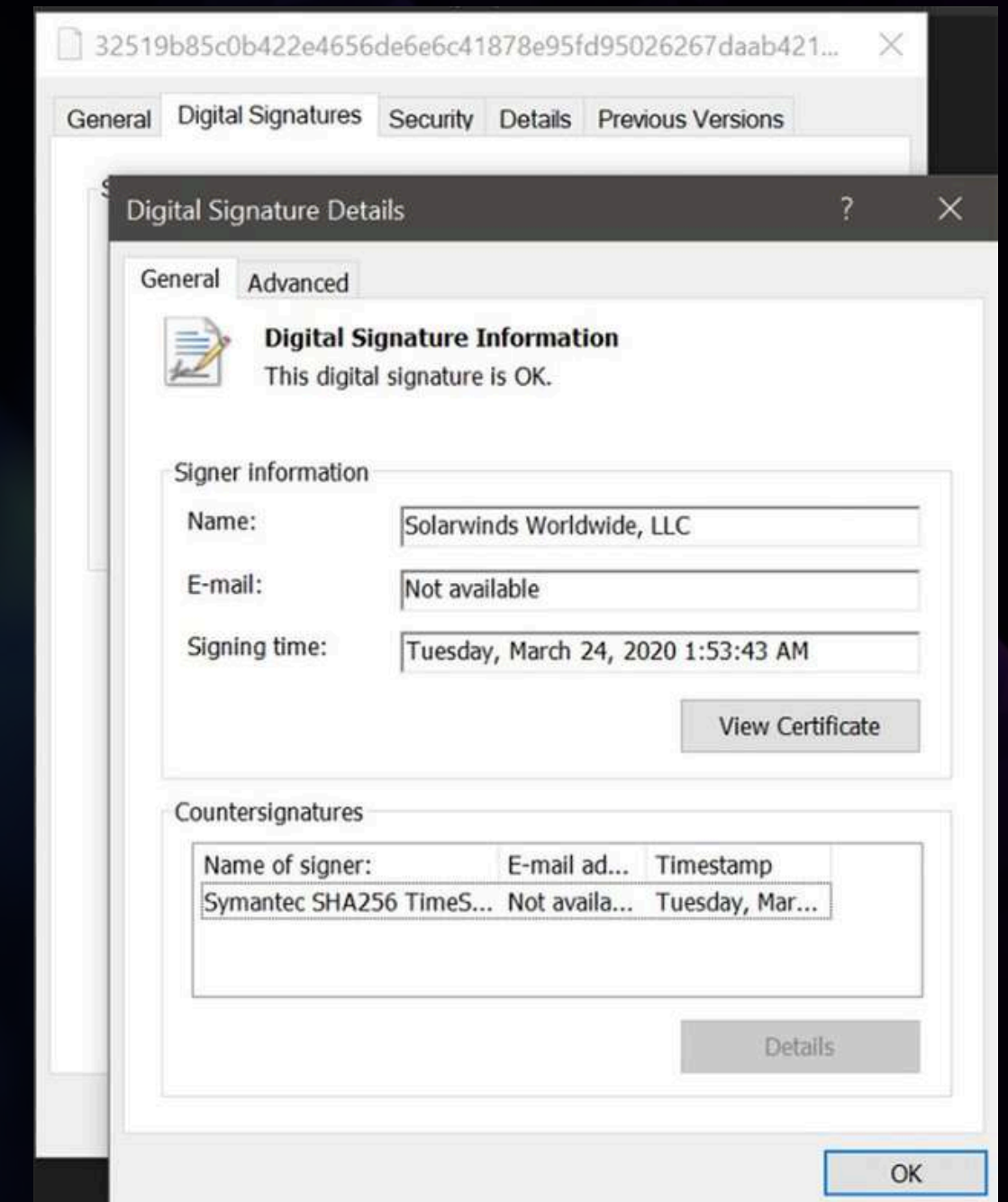
CONCLUSION & CALL TO ACTION

- **Key Takeaways:**

  ○ Cyber threats are evolving; awareness is critical.

  ○ Follow best practices to stay protected.

  ○ The cost of cybercrime is rising—prevention is key.

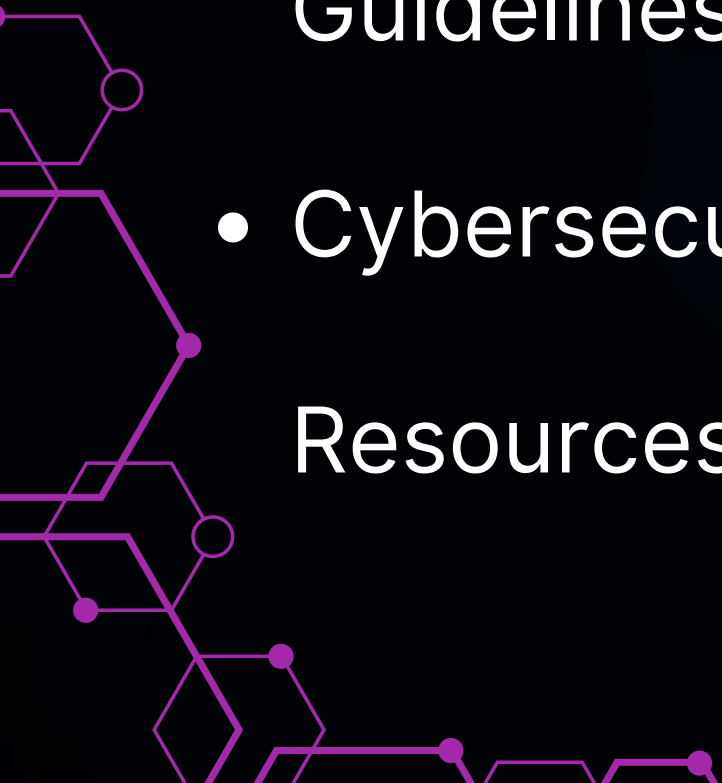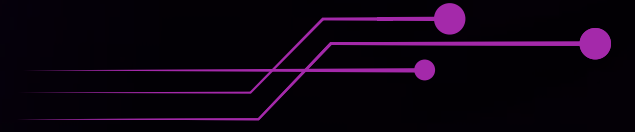 *"Cybersecurity is everyone's responsibility."*

IT STARTS WITH YOU

REFERENCES & FURTHER READING

- IBM Cost of a Data Breach Report 2024

- Verizon 2022 Data Breach Investigations Report

- National Institute of Standards and Technology (NIST) Guidelines

- Cybersecurity & Infrastructure Security Agency (CISA) Resources (cisa.gov)

Q&A
SESSIONS