
LSU

The Dangers of Information Exposure

Offensive Team

LSU Cyber Clinic

An Overview

Information exposure:

The **intentional** or **unintentional** disclosure of information that is considered sensitive.

Sensitive:

Information whose **loss**, **misuse**, or **unauthorized access** or modification could adversely affect security.

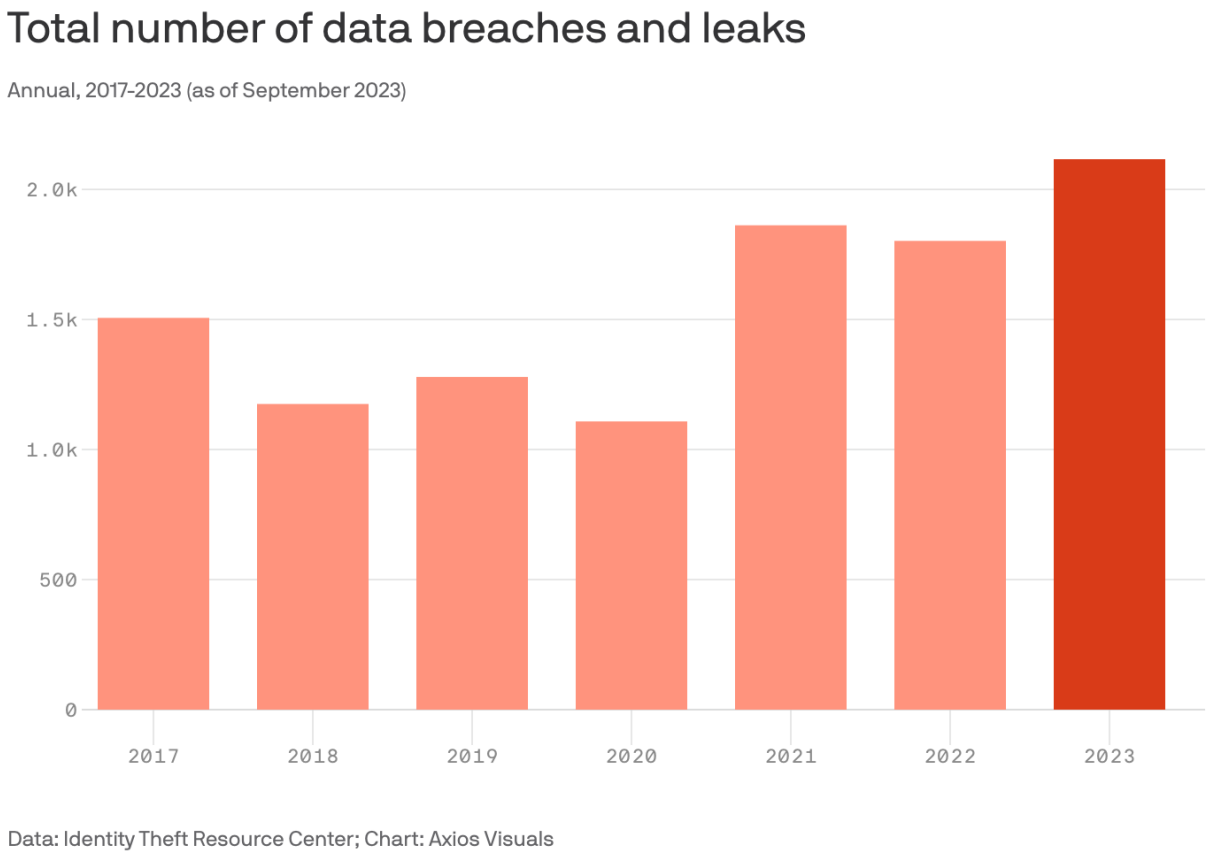
Information Exposure Today

74% of data breaches include a human element (2023), and 46% of all cyber breaches impact businesses with fewer than 1,000 employees. (2021)

– Verizon Data Breach Investigations Reports

The global average cost of a data breach in 2023 was $4.45 million, a 15% increase over 3 years.

– IBM



Forms of Information Exposure

Forms of Information Exposure

Data Leaks (Unintentional release)

Occur when sensitive information is exposed through unintentional or accidental means without explicit malicious intent behind the exposure.

Data Breaches (Unauthorized access)

Involve unauthorized access to or acquisition of sensitive, protected, or confidential data by an individual or group of attackers with malicious intent.

...Causes

Accidental Exposure

- Lost or Stolen Device
- Misconfiguration
- Email sent to wrong recipient
- Improper Documents Disposal

Deliberate Exposure

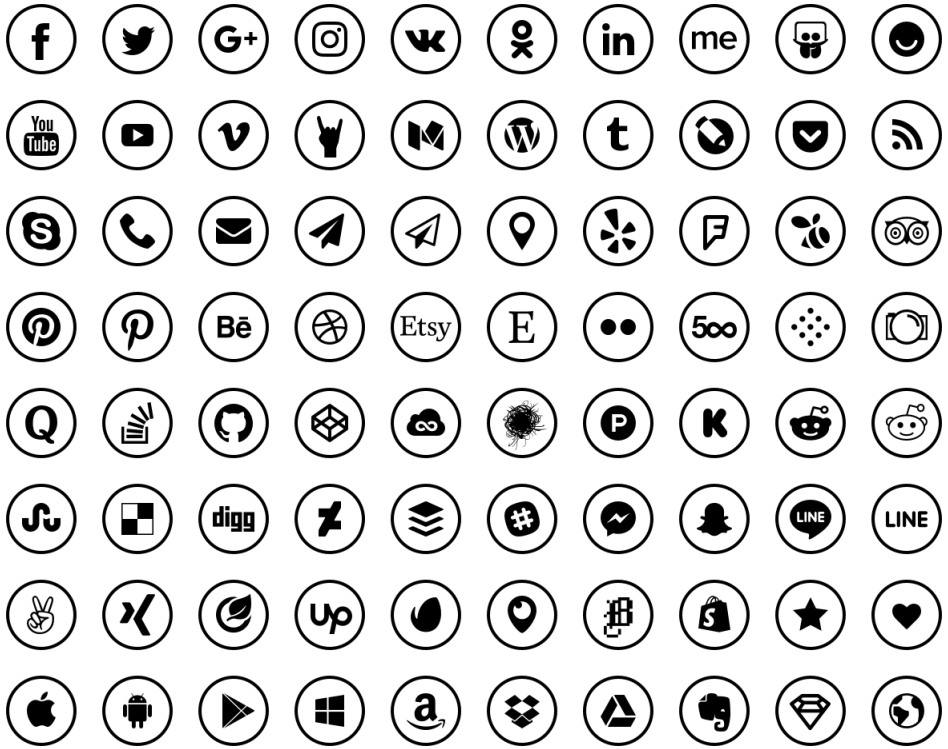
- Phishing Attack
- Ransomware Attack
- Insider Threat
- Credential Stuffing

Source Of Exposure

- Social Media Platforms And Company Website
- Search Engines
- Data Brokers
- Forums

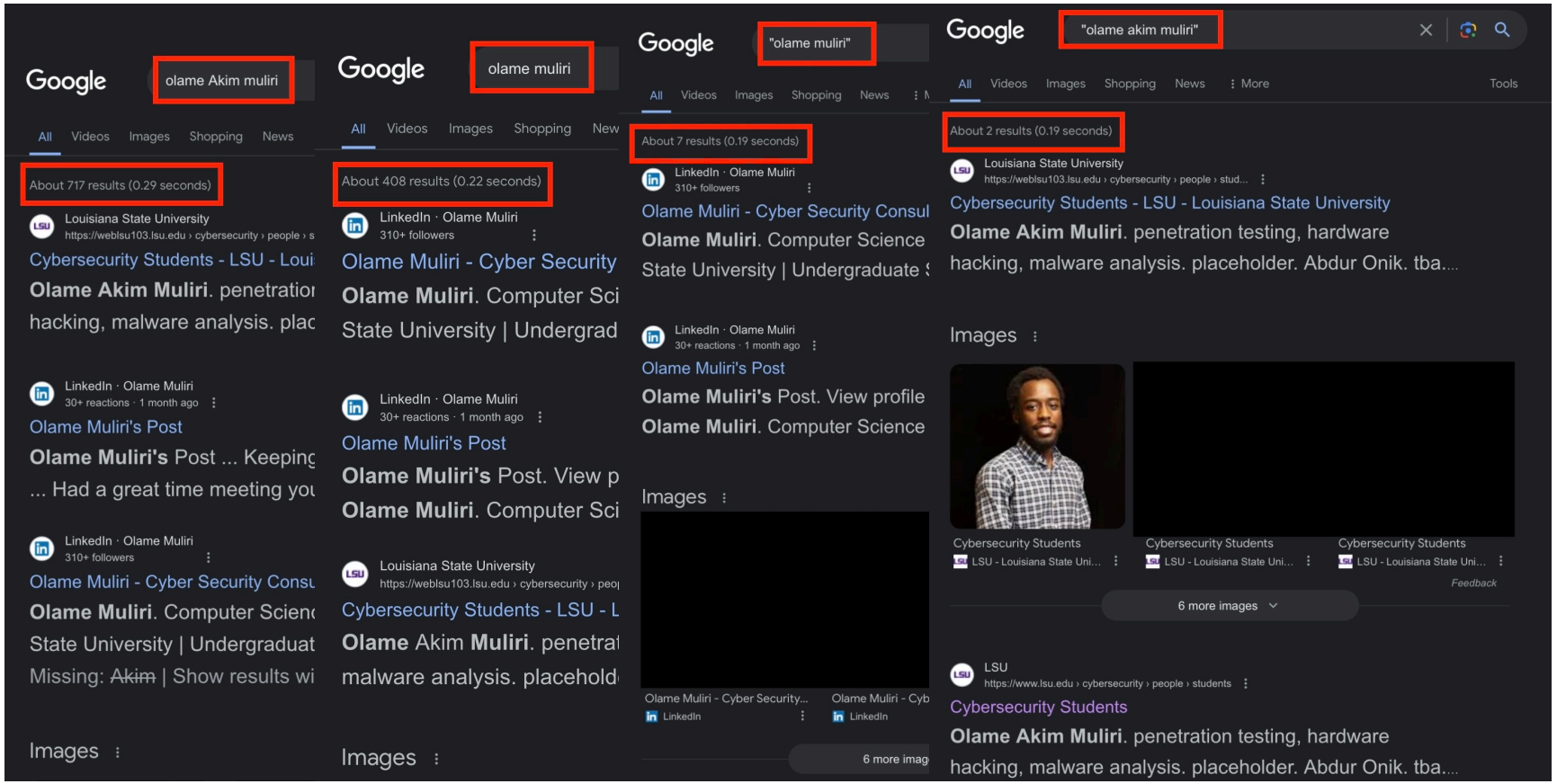
Social Media Platforms And Company Website

- Company Website
- LinkedIn
- Facebook
- Instagram
- X (Twitter)



Search Engines

- Google
- Yandex
- Baidu
- Shodan



Data Brokers

- Data brokers are companies that collect, analyze, and sell personal information about consumers to third parties.
- They gather data from various sources including public records, online activities, loyalty programs, and more, to create detailed profiles of individuals.

Role:

  - Marketing and Advertising
  - Credit and Risk Assessment (Credit Bureaus)

Data Brokers

WIRED Jeffrey Epstein's Island Visitors Exposed by Data Broker

Tracking Visitors to Epstein's Private Island

Near Intelligence collected the precise locations where visitors used their devices on Epstein's island."

Source: Exposed location data from Near Intelligence, imagery from Google, imagery from Google WIRED

Forums

AT&T confirms 70M+ dataset was leaked on hacker forum – yet again

Updated on: April 01, 2024 8:07 PM

Stefanie Schappert, Senior journalist

Image by sdx15 | Shutterstock

Threat actors leak data of 1.3 million PandaBuy customers on hacking forum

Alina BÎZGĂ
April 02, 2024

Threat actors Sangierro and IntelBroker have just leaked a huge database that allegedly contains the information of over 1.3 million PandaBuy customers.

Hacker leaks millions more 23andMe user records on cybercrime forum

Lorenzo Franceschi-Bicchierai @lorenzofb / 11:33 AM CDT • October 18, 2023

Comment

Image Credits: Paul Morris/Bloomberg via Getty Images / Getty Images

The same hacker who leaked a trove of user data stolen from the genetic testing company 23andMe two weeks ago has now leaked millions of new user records.

LSU

DEMO

Who can be affected?

- The company
  - Exposure to cyber-attacks, legal consequences, and reputational damage
- Employees
  - Personal information such as bank routing info leaked
- Clients
  - Breaking of trust and privacy of data they share
- The Attacker
  - Getting paid

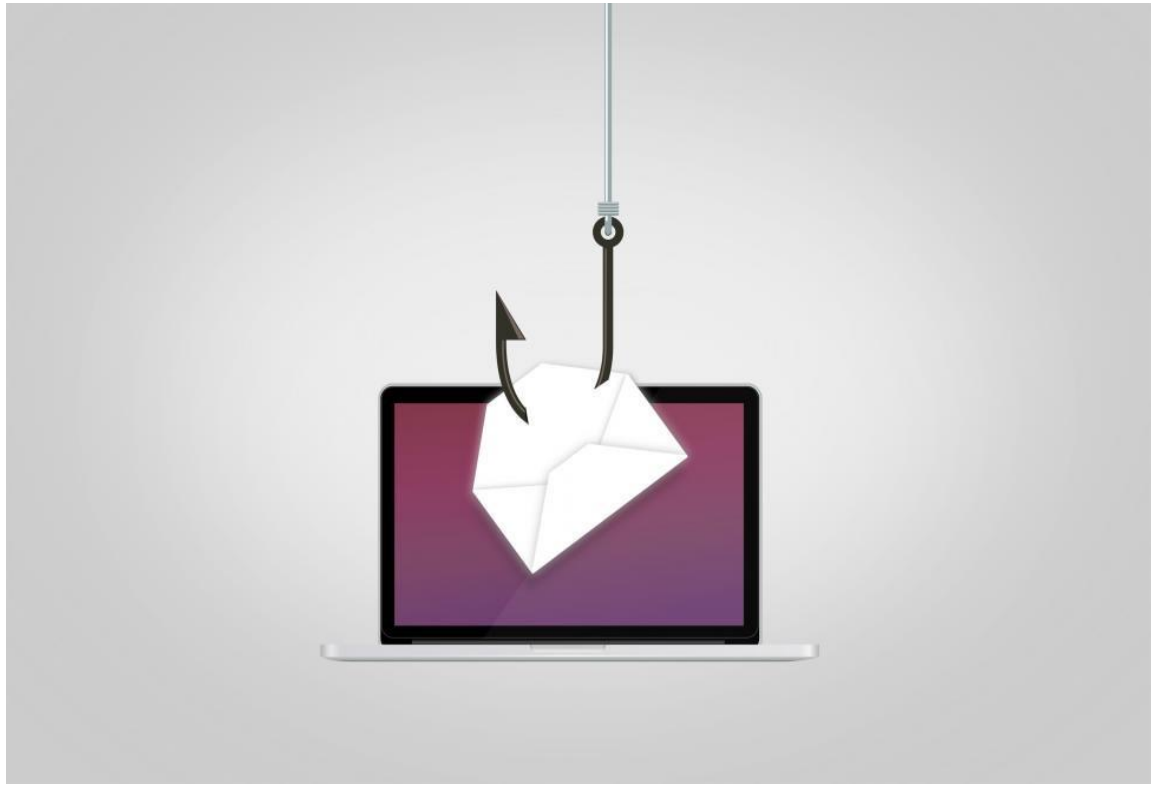
What can be Done?

The Key...

- Be Knowledgeable
  - Some things cannot be helped
- Be Proactive
- Be Controlled

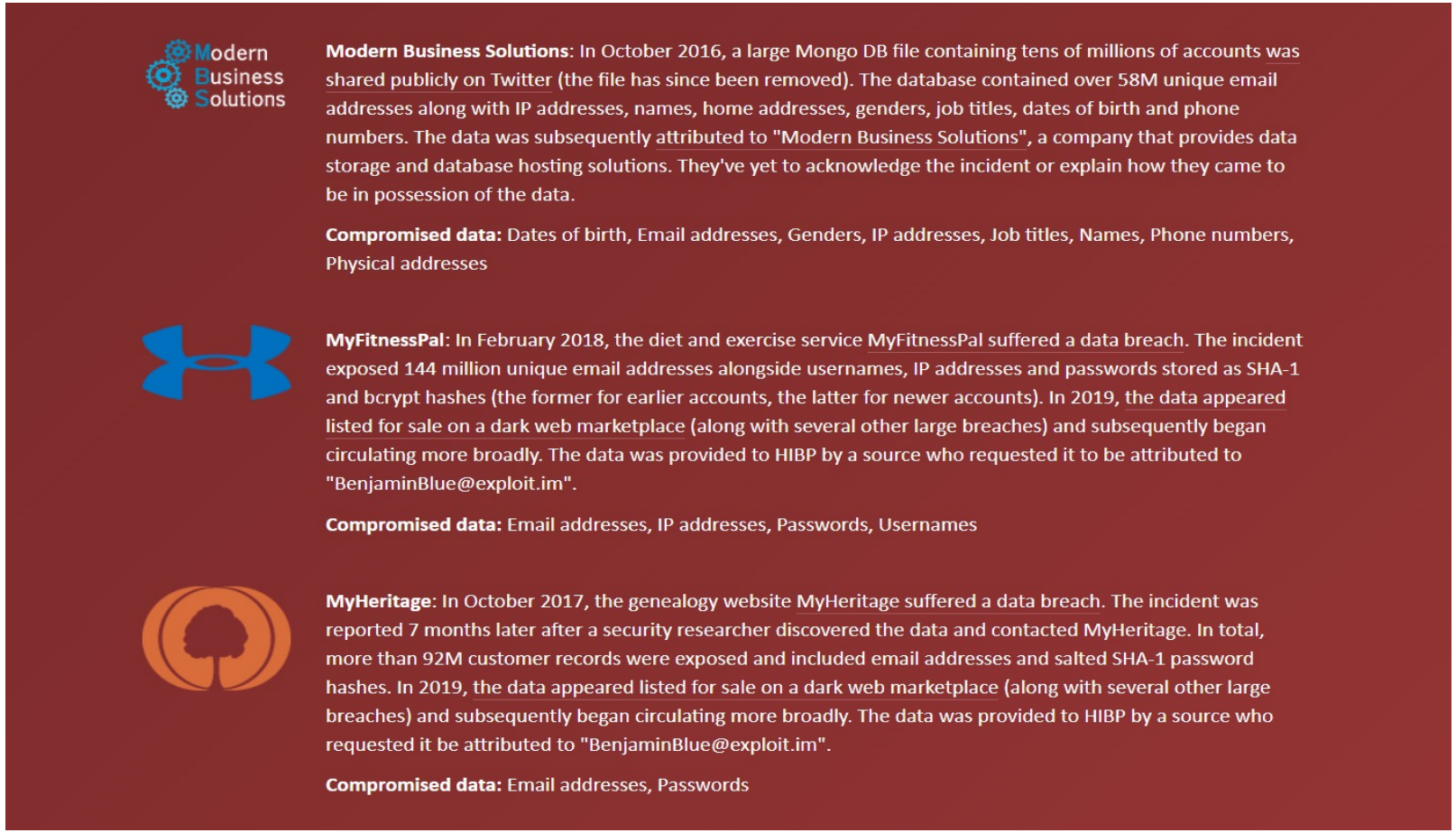
Mitigations: Emails

- Flag external emails or separate internal and external folder in outlook
- Employee cyber awareness training
  - Phishing
  - Service Sign-ups



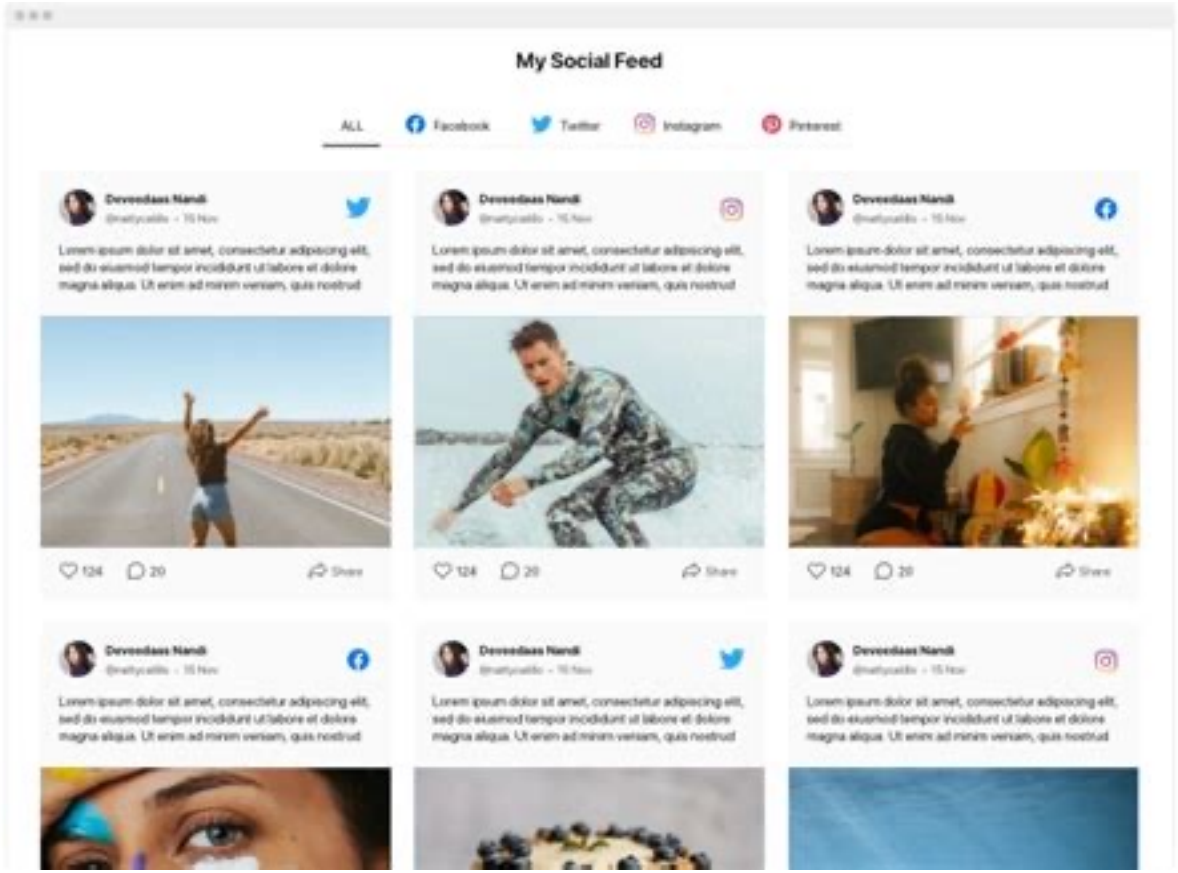
Mitigations: Data Breaches

- Breaches may be Unavoidable
- Monitoring
- Changing to Unique Passwords
- MFA



Mitigations: Unintentional Leaks

- Social Media and Forums (Employee Training)
- Improper/No Disposal of Data

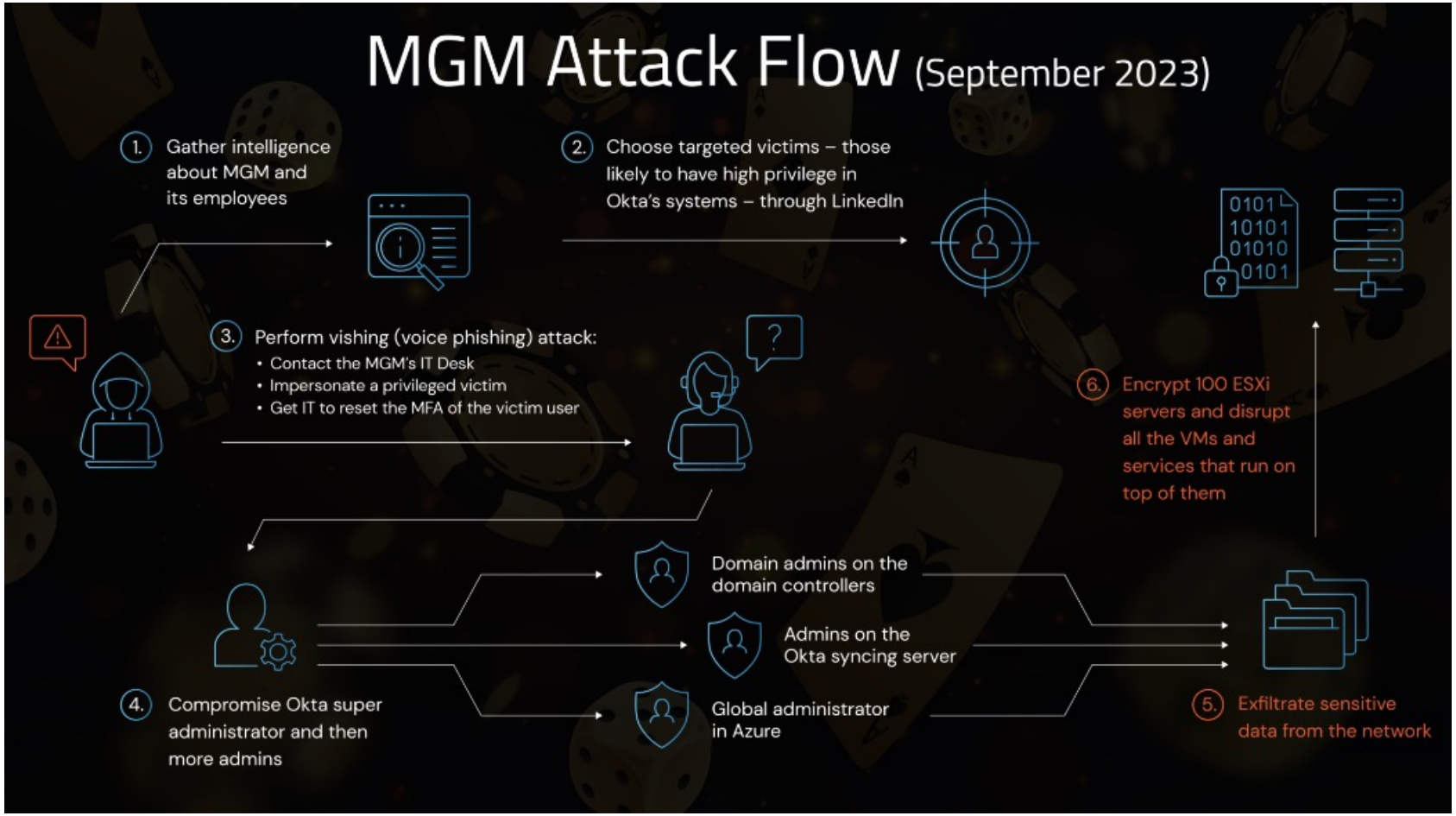


Final Mitigation Takeaways

- Social Engineering is Prominent
- Have an Incident Response Plan (IRP)

Case Study: MGM

- Frequent posting on Social Media
- Employees not Trained
- Lack of MFA
- Lack of Access Control



https://www.cyberark.com/resources/blog/the-mgm-resorts-attack-initial-analysis


QUESTIONS?