## WELCOME

# Antonio Archer

# THE DILEMMA

# Passwords:

**Problem Statement: Password Vulnerabilities**

- **Weakness of Memorable Passwords**: Easy-to-remember passwords are inherently weak, making them easy targets for attackers.
- **Risk of Password Reuse**: Users often reuse passwords across accounts, creating a single point of failure—compromising one account risks exposure across all.
- **Impact on Sensitive Data**: These habits enable unauthorized access to sensitive data, increasing the potential for data breaches and loss of control over personal or business information.

# OUR FINDINGS

## Cybersecurity Challenges in Emerging Technology

- **Evolving Threat Landscape**: Quantum computing and AI amplify risks, with current protections (encryption, firewalls) expected to struggle against future threats.
- **Key Vulnerabilities**:
  - **Brute Force Attacks**: Account for **5% of breaches** and may accelerate with quantum advancements.
  - **Social Engineering**: Contributes to **95% of successful intrusions**; AI-powered deepfakes make detection harder.
- **Limitations of MFA**:
  - **78% of large companies** use MFA, yet it has weak points:
    - User lockouts (e.g., changed contacts), privacy concerns with biometrics.
    - MFA fatigue can lead to compromised access.
- **Future Solutions**:
  - Minimize human error via **automation** (e.g., biometrics, behavior-based verification).
  - **Quantum-resistant cryptography** to counter new computational threats.

intel Security

HOW PASSWORD LENGTH WINS THE INTERNET

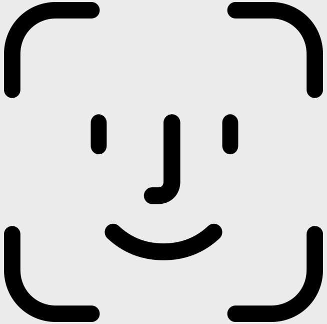
Passwords 102

***Credits to Cloudflare learning, Cisco,  cisa, and core security***

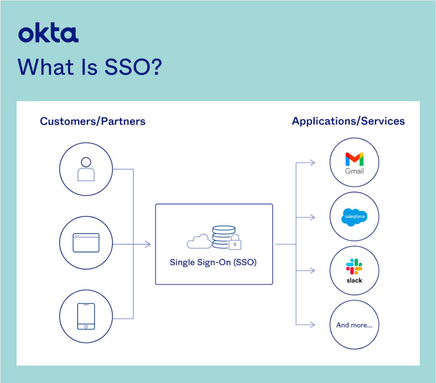
ADD IMAGE HERE

# WHAT SOLUTIONS ALREADY EXIST

## Biometric Identification



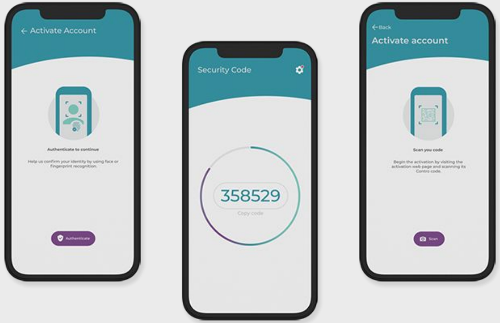
## Single Sign On



okta

What Is SSO?

## Mobile Authenticator



← Activate Account

Authenticate to continue

Help us confirm your identity by using face or fingerprint recognition.

Security Code

358529

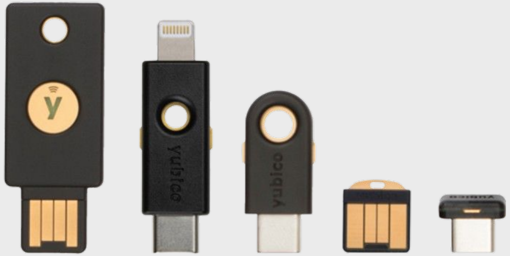
← Back

Activate account

Scan you code

Begin the activation by visiting the activation web page and scanning its Contro code.

## Physical Keys

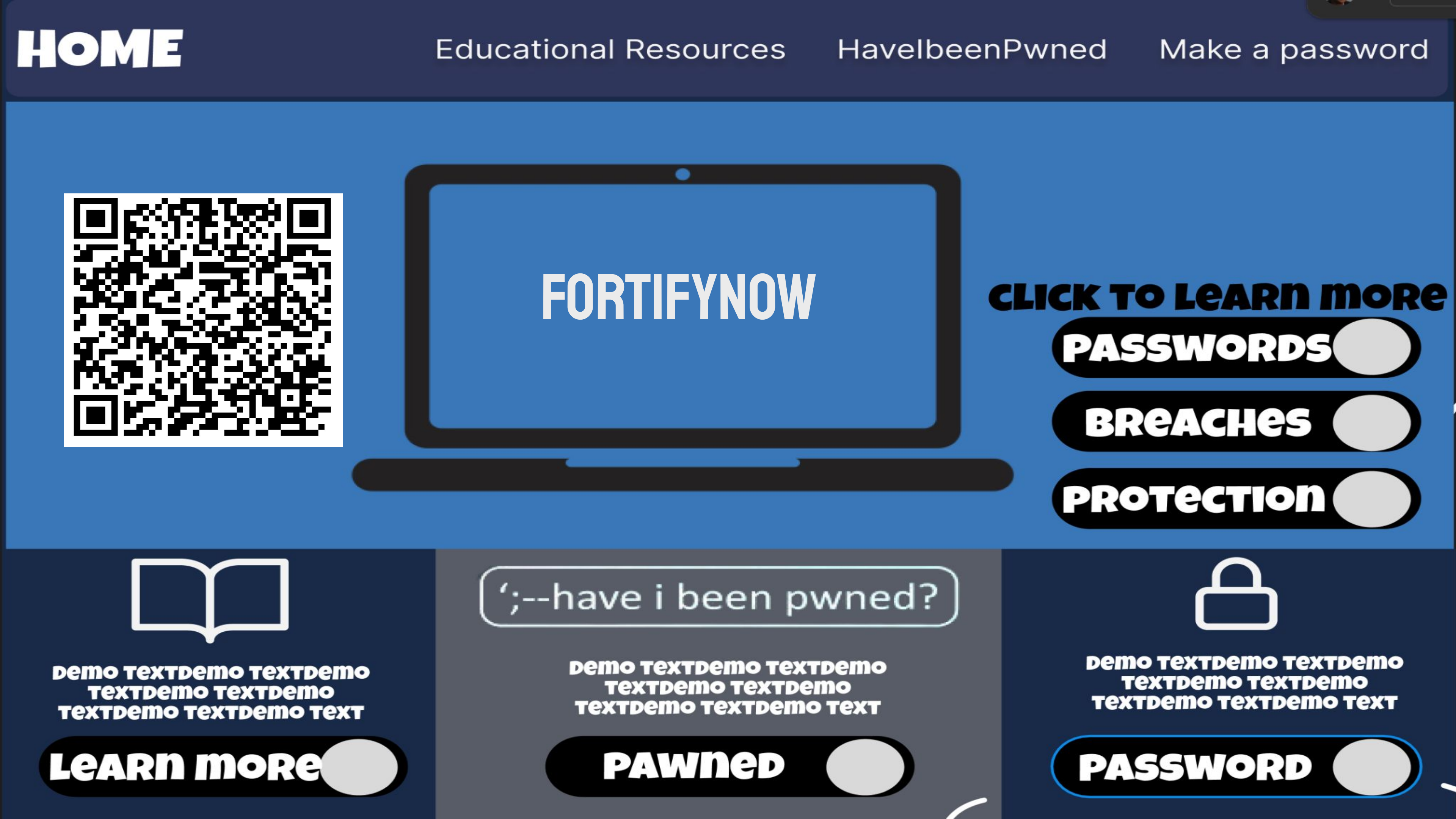


# Why Security Tools Fall Short

## Why Security Tools Fall Short

- **Lack of Awareness**: Many users are unaware of essential cybersecurity tools, such as password managers and multi-factor authentication.
- **Knowledge, Not Availability**: The challenge isn’t the absence of security tools, but a lack of user knowledge and training on how to implement them effectively.
- **Resulting Vulnerability**: Without proper understanding, even available security measures go unused, leaving both personal and organizational data at increased risk.

# MY SOLUTION



HOME

Educational Resources HaveIbeenPwned Make a password

FORTIFYNOW

CLICK TO LEARN MORE

PASSWORDS

BREACHES

PROTECTION

DEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXT

LEARN MORE

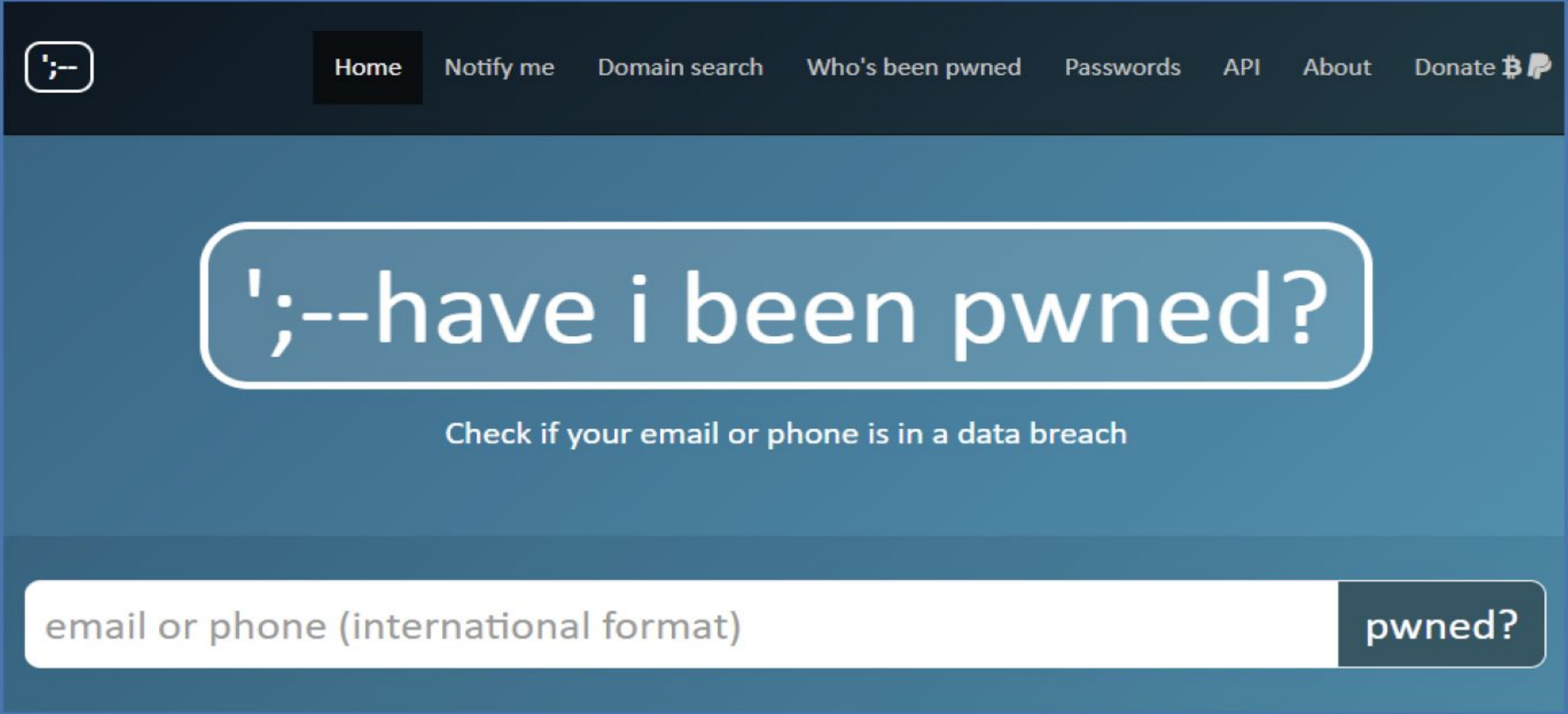
';--have i been pwned?

DEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXT

PAWNED

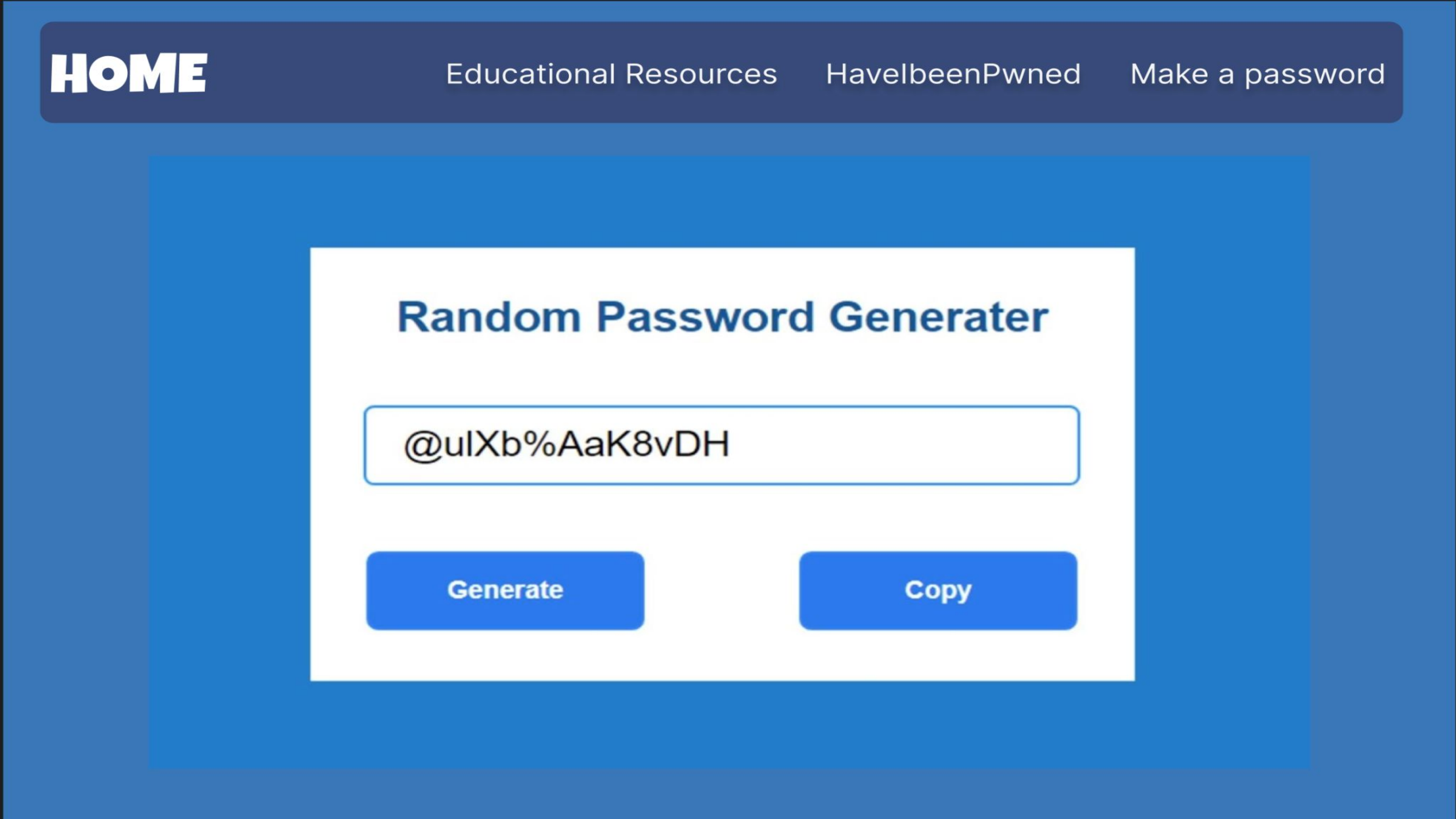
DEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXTDEMO TEXT

PASSWORD



';--have i been pwned?

Check if your email or phone is in a data breach



## Random Password Generater

@ulXb%AaK8vDH

# THE

# IMPORTANCE

# PERSONA I

## ETHEL A.

A 70-year-old retiree who uses the same password across multiple sites and has lost access to several accounts. She relies on a physical password book rather than digital tools.

### IDENTITY

Ethel is older and isn’t as technical so she carries around a password book and doesn’t trust her passwords to be online but she often

### NEEDS

Simple, memorable passwords and a way to create unique credentials for each site without the complexity of digital solutions

### BEHAVIORS

Prefers physical records over digital tools, prioritizing security but wary of online storage solutions. Seeks a reliable and user-friendly way to enhance online security.

# PERSONA 2

## MIKE R.

A 35-YEAR-OLD WHO HAS USED THE SAME PASSWORD SINCE HE WAS 14, APPLYING IT UNIVERSALLY, INCLUDING FOR SENSITIVE ACCOUNTS LIKE BANKING. HE'S NEVER EXPERIENCED AN ISSUE WITH IT.

### IDENTITY

Mike Ross uses the same password for everything and never had any issues with it. He made his password when he was 14 and uses it everywhere including his bank account

### NEEDS

A simple, reliable way to maintain his current system without needing to change passwords or adopt new practices, unless absolutely necessary.

### BEHAVIORS

Mike is an internet veteran, confident in his current approach, and sees no reason to change his long-standing password despite security risks.

# PROBLEMS

**What if people don’t listen?**

Our goal is to plant the seeds of cybersecurity awareness. Even if users don’t fortify their accounts immediately, we aim to leave a lasting impression, encouraging them to secure their accounts in the future.

# AND

**How will creating a password but not saving it benefit people?**

While saving passwords online can create vulnerabilities, we encourage users to store passwords securely in physical password managers. For those who prefer digital methods, we will recommend safe and encrypted options to mitigate risks.

# SOLUTIONS

**What problems do we solve?**

We focus on education, not as a direct protection tool, but as a call to action. Our mission is to empower users with the knowledge to secure their accounts and protect their personal data.

# QUESTIONS?