Webinar

Look Ma, No Password!

Multi-Factor Authentication and Going Passwordless

Thursday, March 30
2pm ET/ 11am PT

NATIONAL CYBERSECURITY ALLIANCE

yubico

Please note…

- This webinar is being recorded
  - The recording will be uploaded to staysafeonline.org and Youtube
- Please use the Q&A chat box to ask questions at any time

Today's Speakers

Role

Lisa Plaggemier

Executive Director

National Cybersecurity Alliance

Role

Abby Guha

VP, Product Marketing

Yubico

We empower a more secure, interconnected world.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.

CYBERSECURITY AWARENESS MONTH

CyberSecure MY BUSINESS

HBCU Career Program

Data Privacy Week

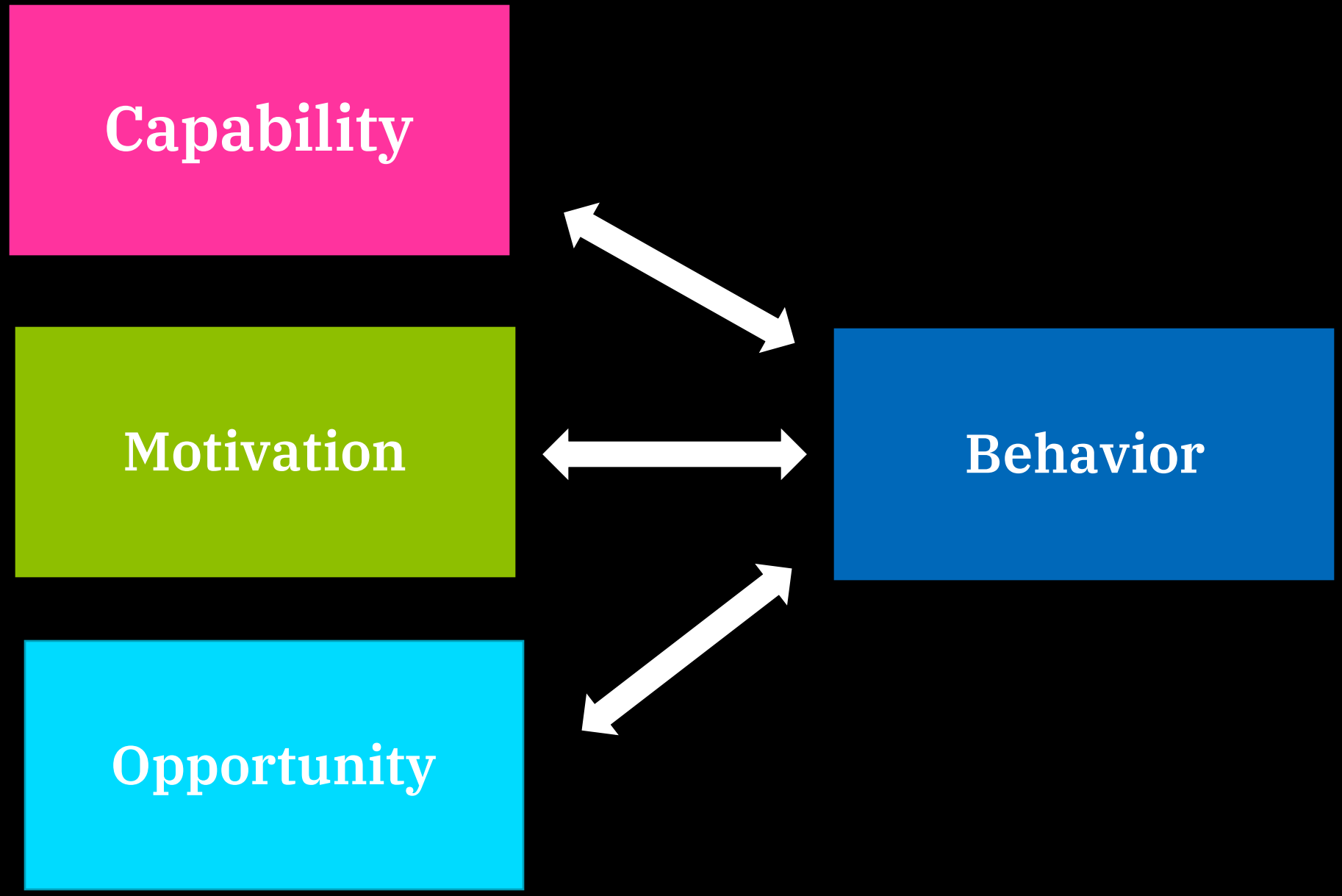
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

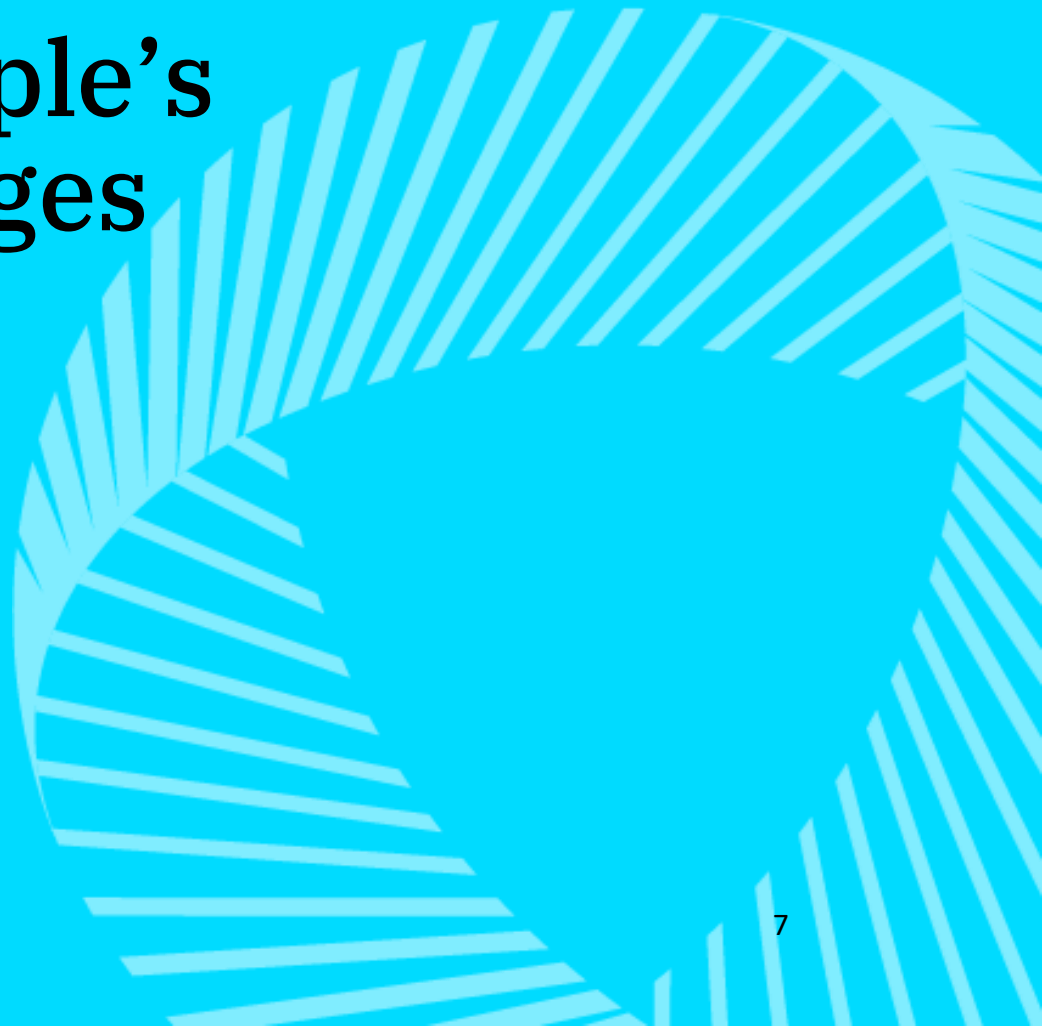
The Annual Cybersecurity Attitudes and Behaviors Report 2022

TABLE OF CONTENTS


Capability
Motivation
Opportunity
Behavior

“Facts don’t change people’s behavior. Emotion changes people’s behavior.”

Seth Godin



Feelings

Poll Question

Q. Staying secure online is under my control.

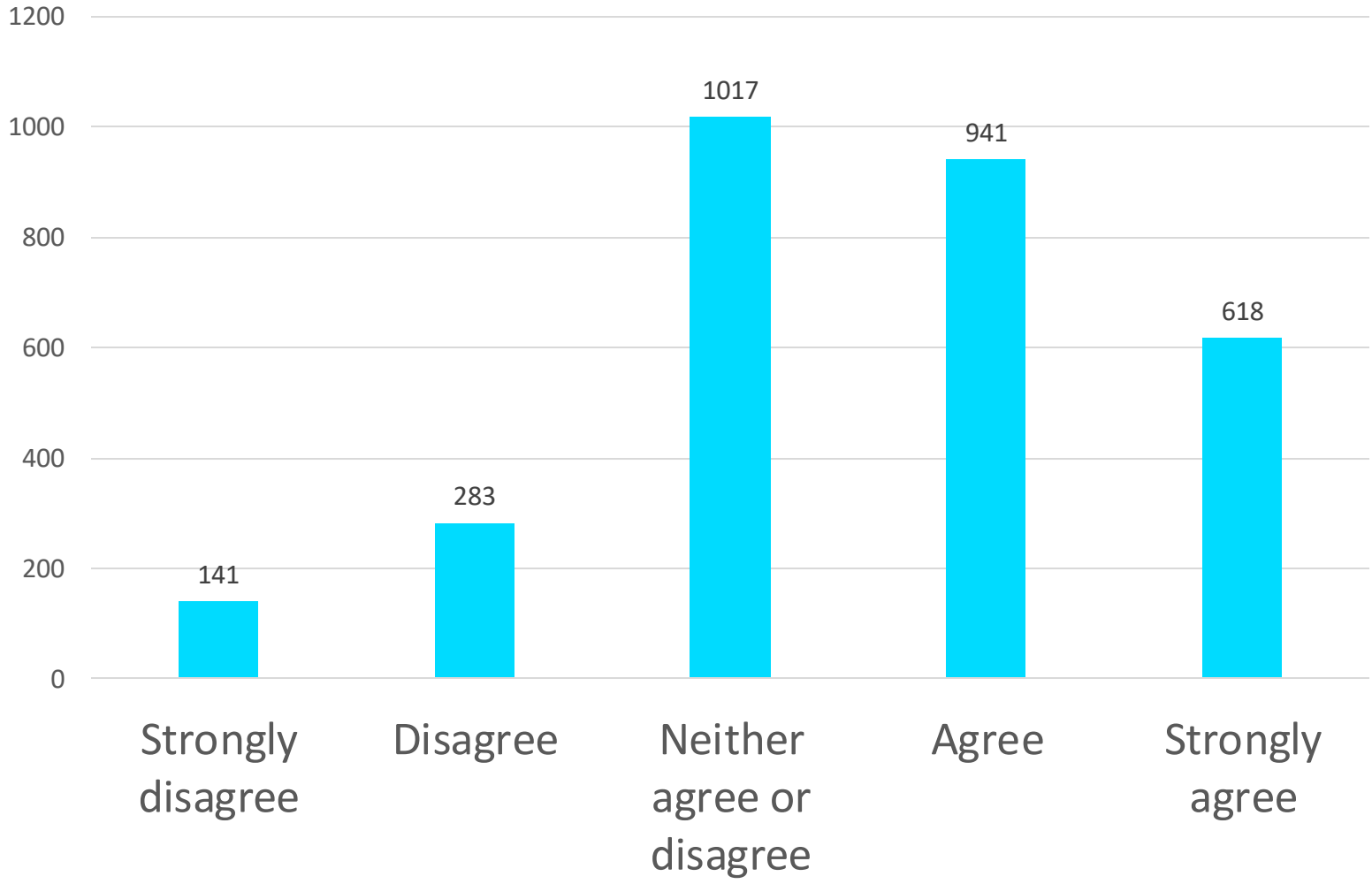
a. Strongly Disagree
b. Somewhat Disagree
c. Neither Agree nor Disagree
d. Somewhat Agree
e. Strongly Agree

Feelings

Q: How do you feel about cyber security?

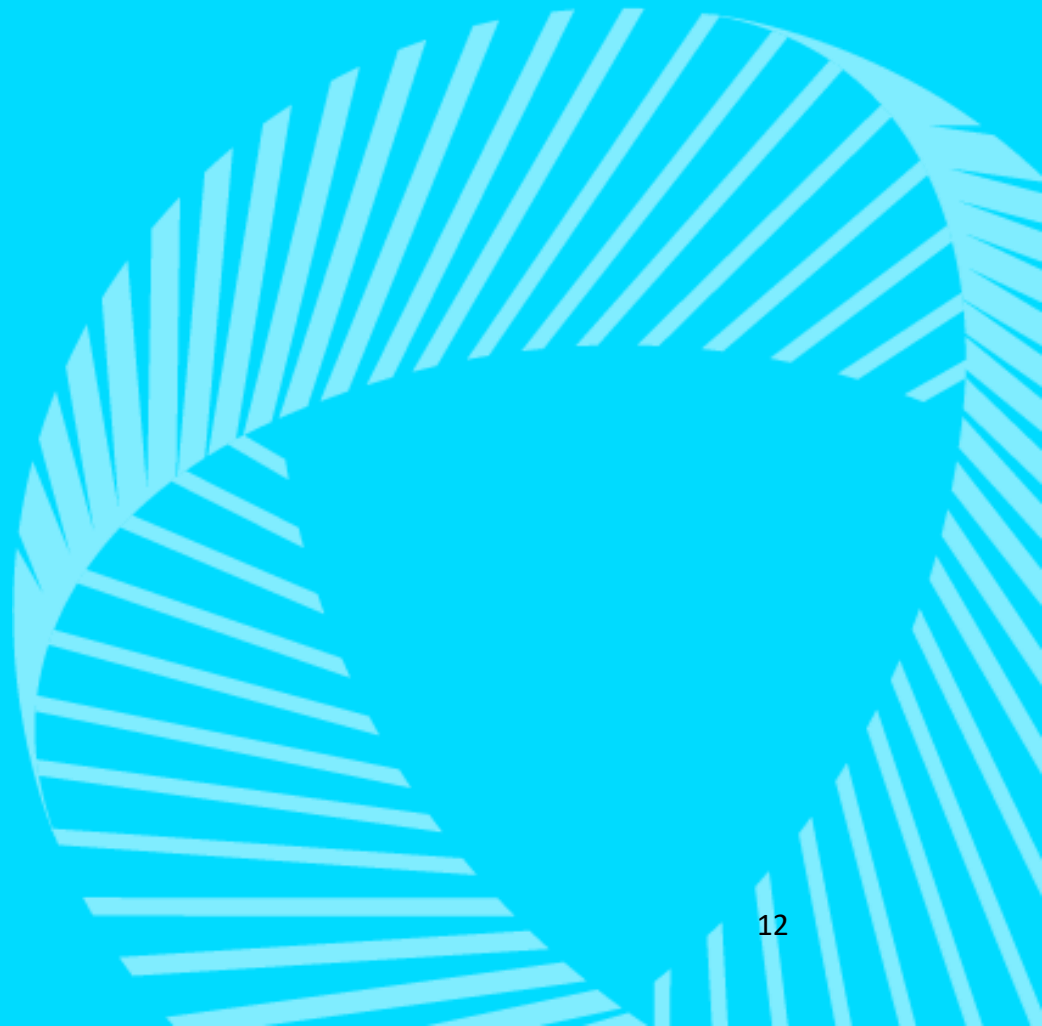
Statement:

"Staying secure online is under my control."



Behaviors

Passwords

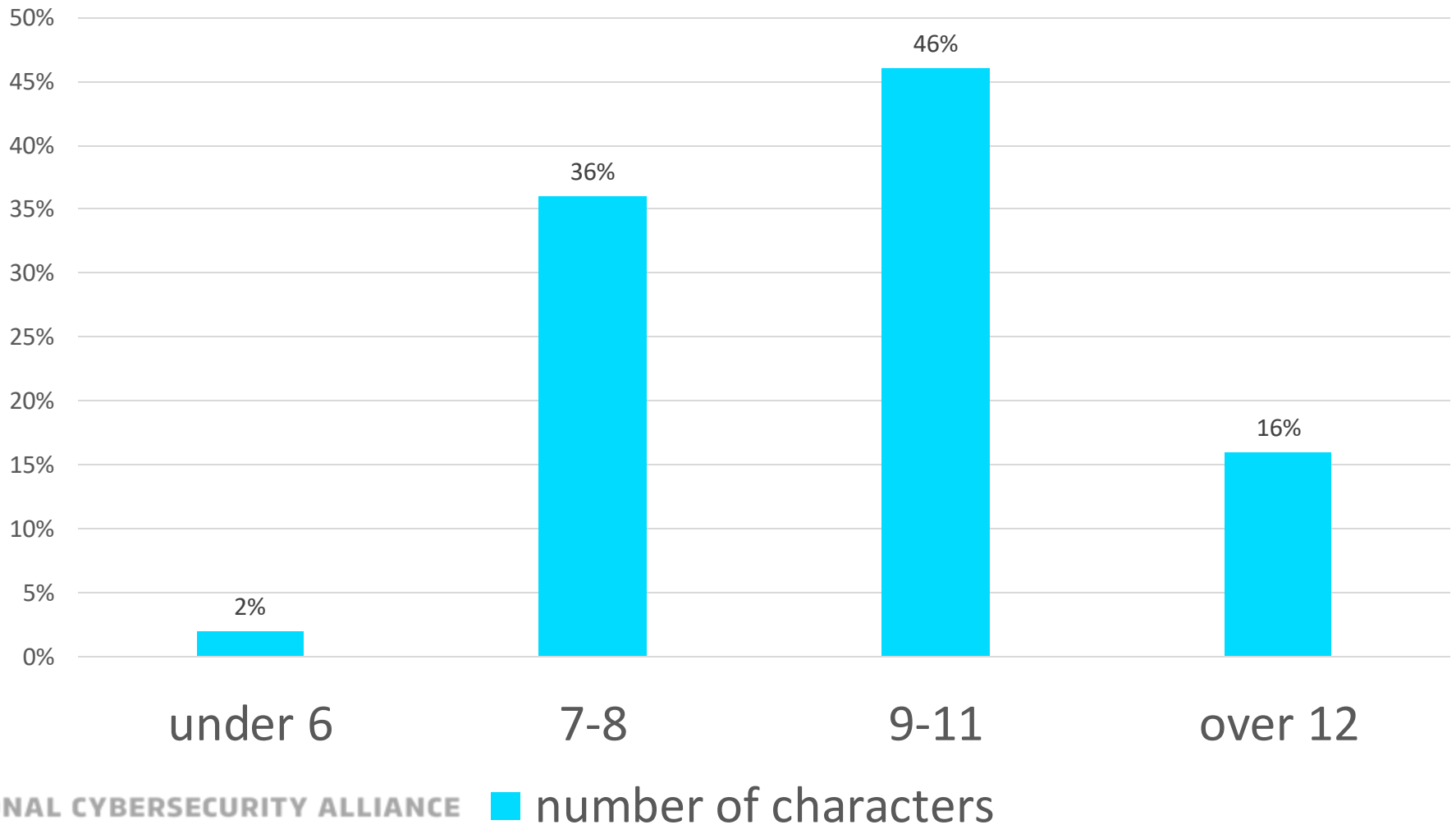


Poll Question

Q. What is the typical length of your passwords?

a. Under 6 character
b. 7-8 characters
c. 9-11 characters
d. Over 12 characters

Password Length



Poll Question

Q. How often do you use unique passwords for your important online accounts (e.g., email, social media)?

a. Never
b. Sometimes
c. Half of the time
d. Most of the time
e. All the time

Q. How often do you use different passwords for your important online accounts (e.g., email, social media)?

a. Never **3%**
b. Sometimes **13%**
c. Half of the time **20%**
d. Most of the time **31%**
e. All the time **33%**


YAHOO!

Q. What is your preferred method of remembering multiple passwords?

a. I write them down in a notebook **37%**
b. I write them down in a document on my computer **9%**
c. I store them in my phone **13%**
d. I store them in my email **6%**
e. I just remember them (without writing them down) **22%**
f. I save passwords in the browser **6%**
g. I use a password manager application **7%**

Multi-Factor Authentication

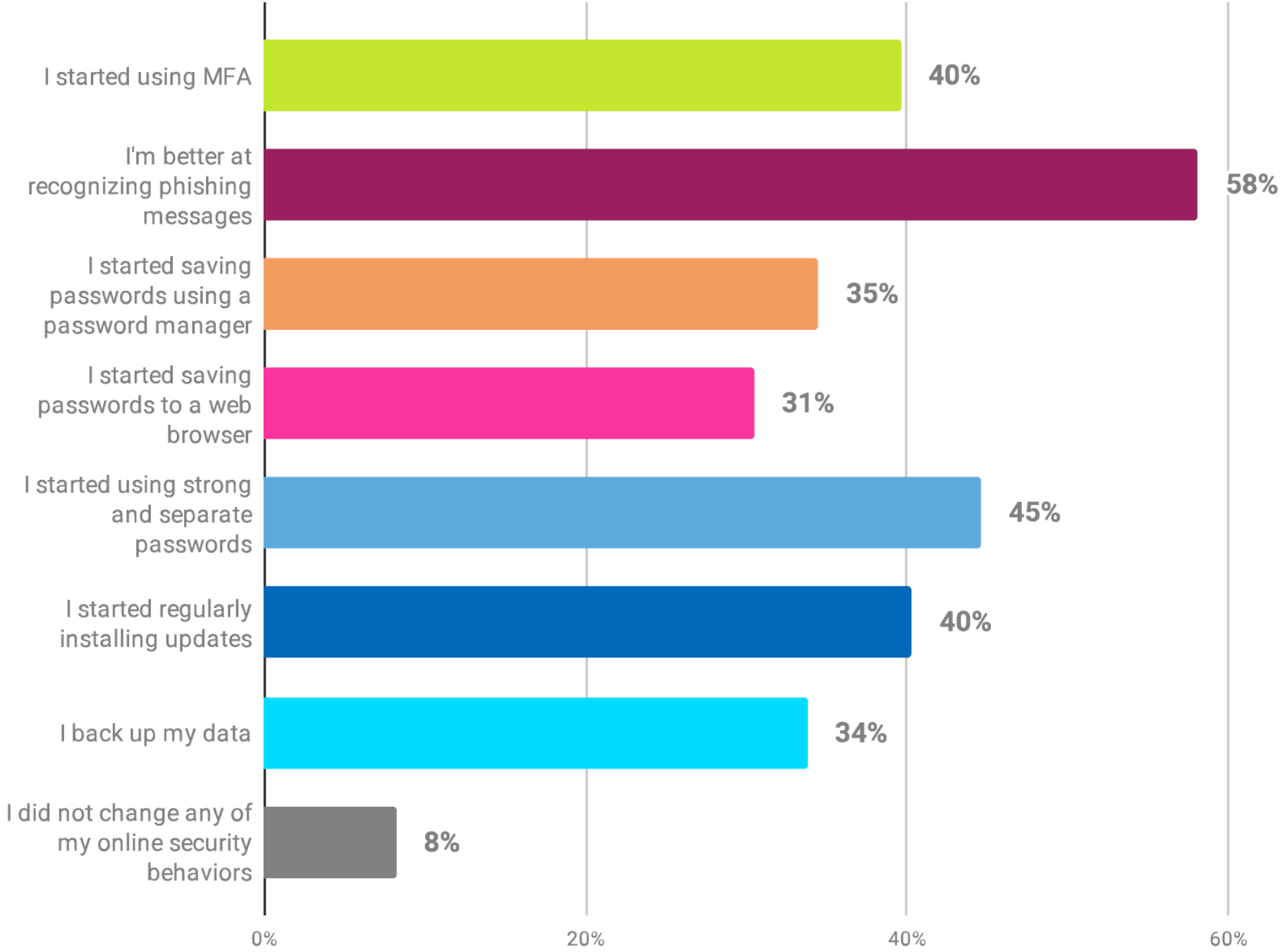
Use of Multi-Factor Authentication (MFA)

43% of the participants had never heard of MFA

Out of the 57% of the participants who had heard about it:

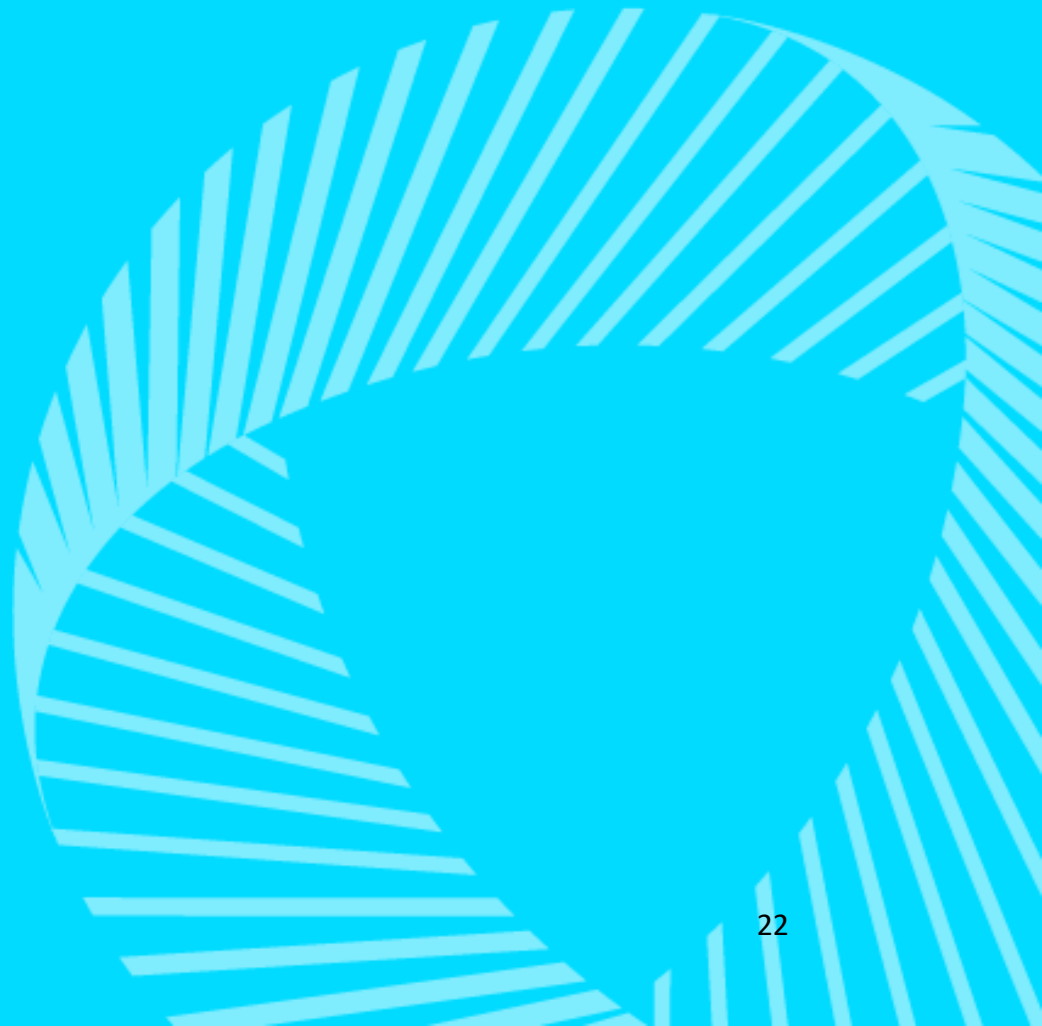
- **79%** applied it at least once
- **94%** of them reporting that they were **still using MFA**

Security Behavior

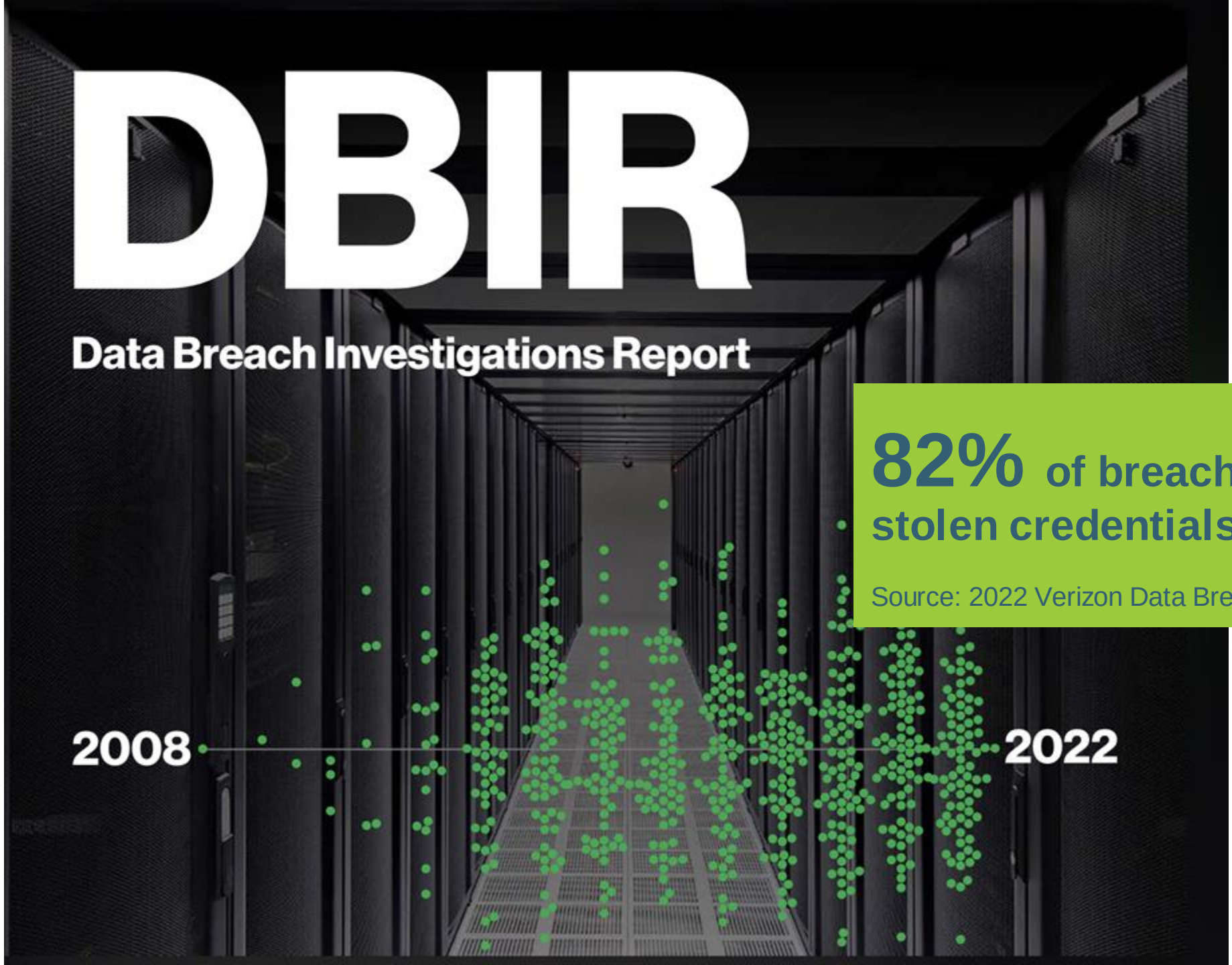


NATIONAL CYE

Peace of Mind



The need for phishing-resistant MFA



82% of breaches caused by stolen credentials

Source: 2022 Verizon Data Breach Investigations Report

Phishing, a growing cyber threat

/’fiSHiNG/

The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Phishing poses the biggest cyber threat

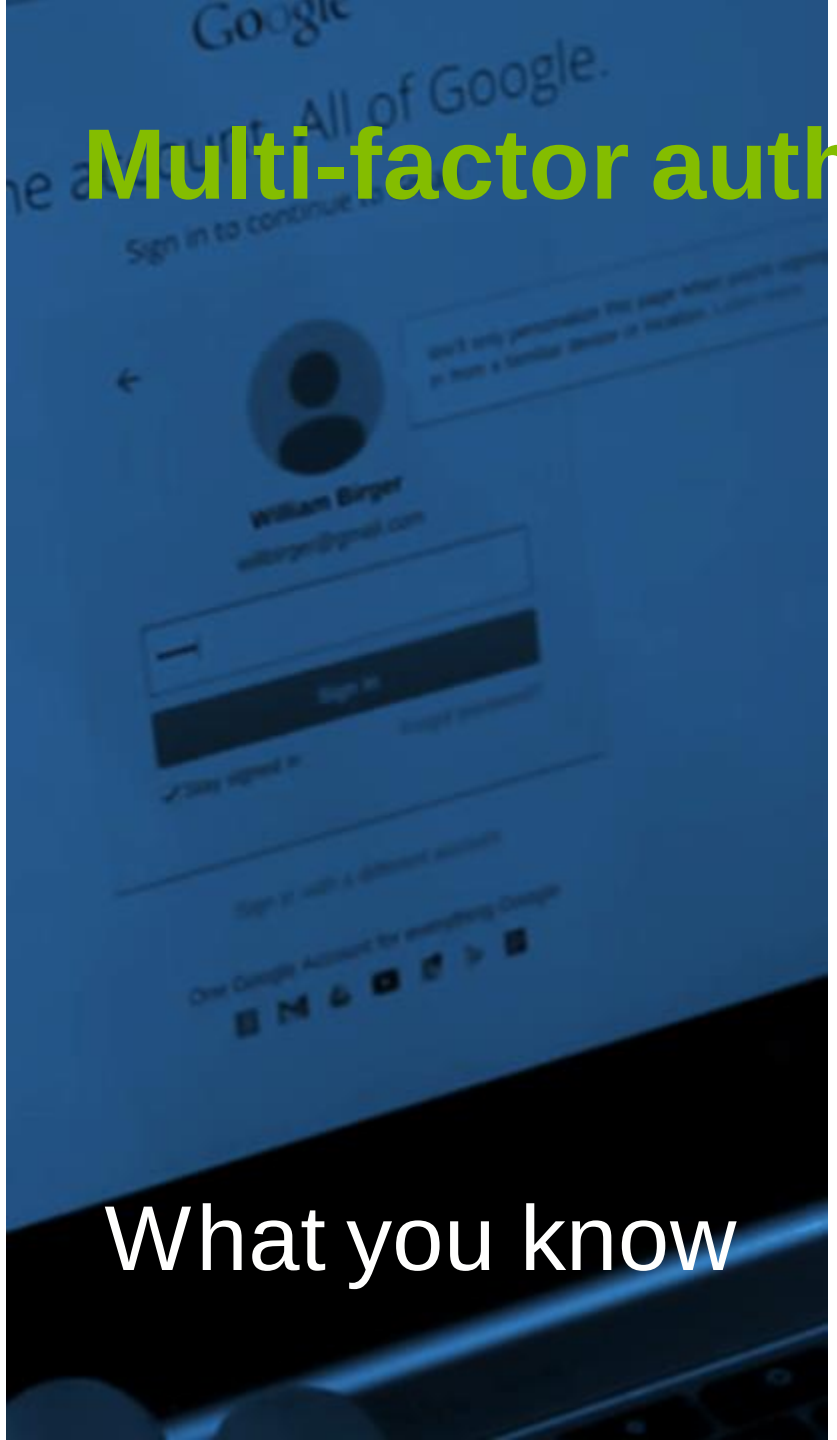
It works!...so very lucrative for malicious actors

Source: Statista 2021

So, passwords aren’t great because they’re easy targets for phishing…

but what’s better?

Multi-factor authentication (MFA)

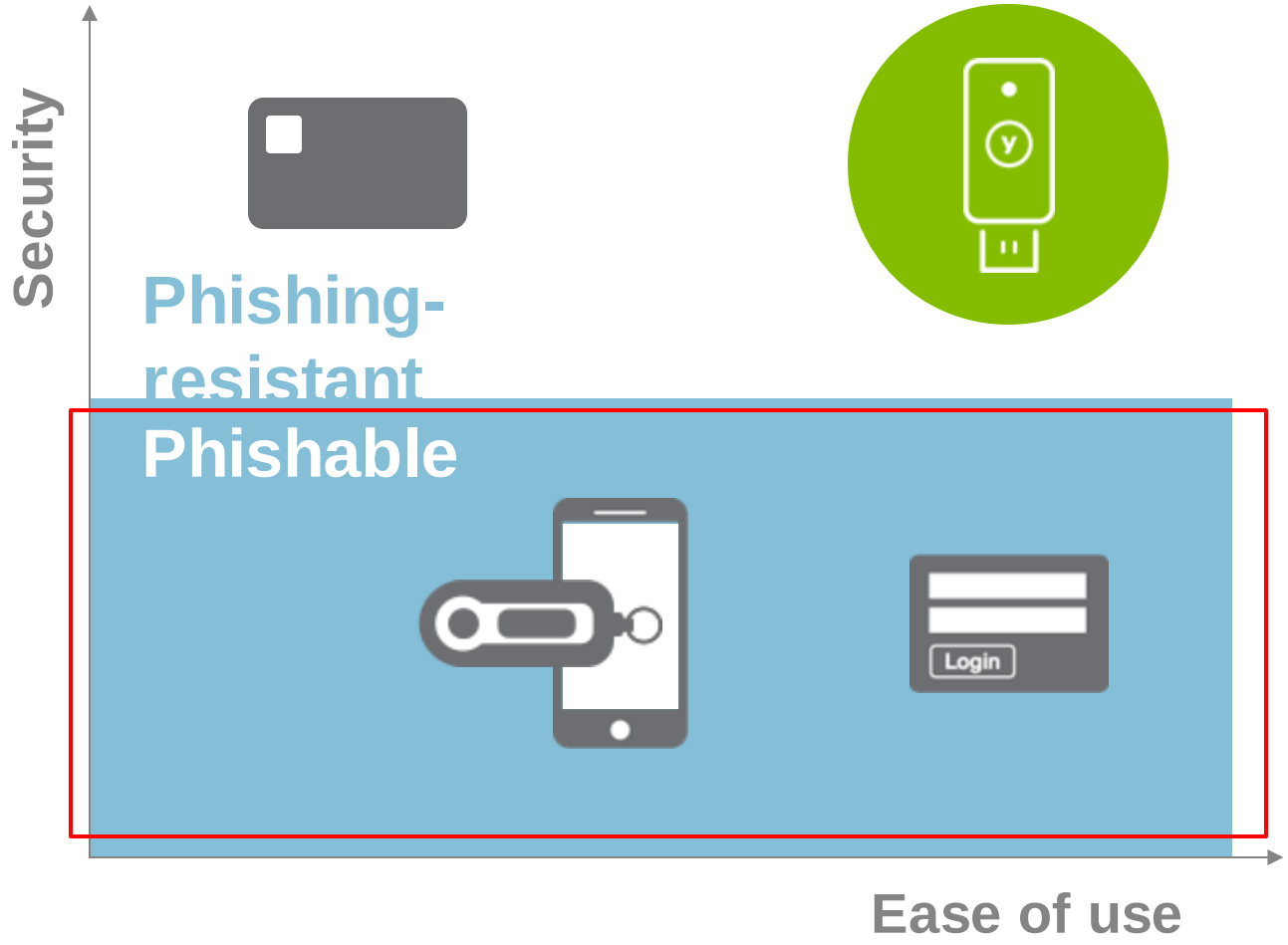


What you know

What you have

Who you are

Not all MFA created equal



Legacy MFA is phishable and easily bypassed by hackers

MANAGE > SECURITY

Cyberattacks Are Bypassing Multi-Factor Authentication

Cyber attackers are learning how to bypass MFA and data centers need to start looking at more advanced security measures. Until then, compensating controls need to be put in place to protect against breaches.

Attack detection | Aug 19, 2022 | 5 min

5 ways attackers bypass MFA

Author : **Anupama. A**

Share Tweet Share

NEWS

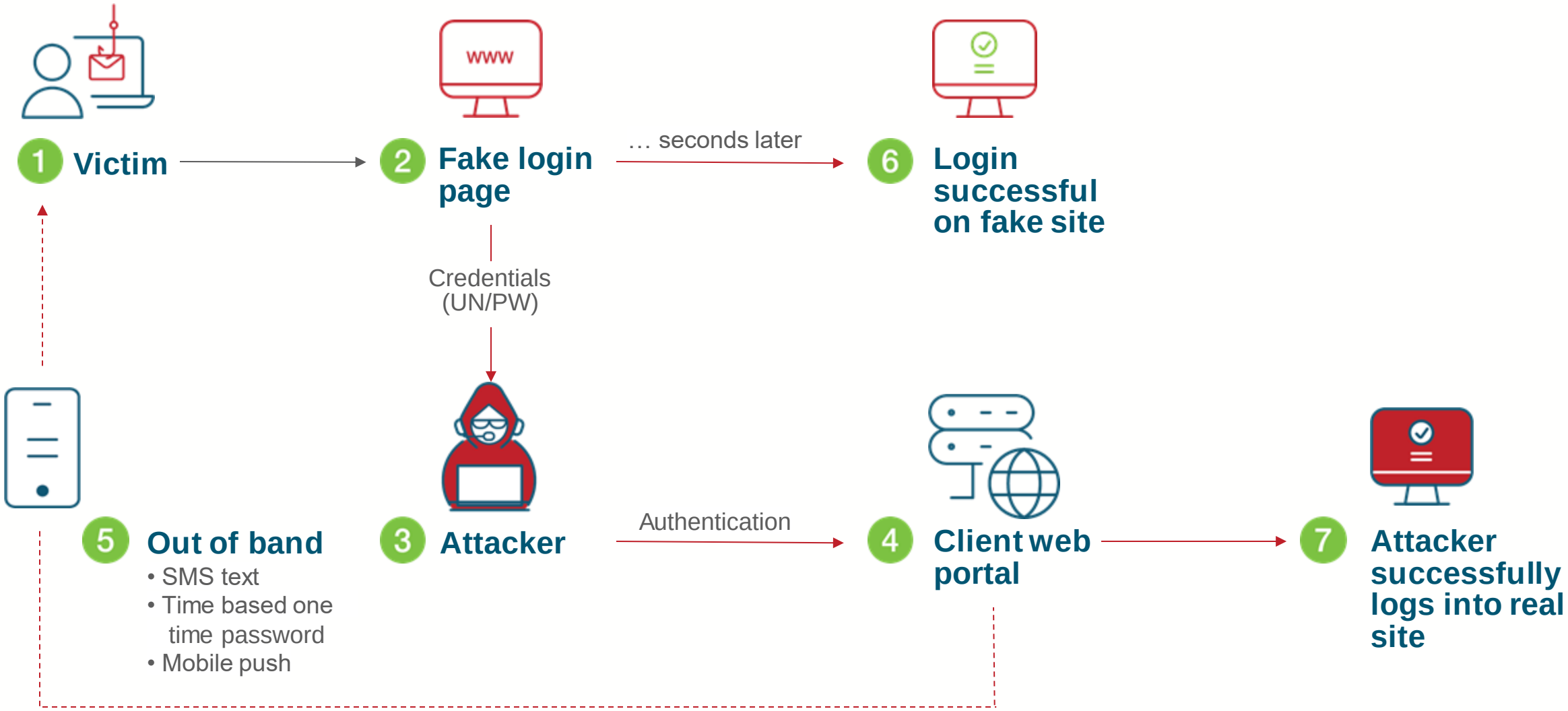
Cybercriminals launching more MFA bypass attacks

New research from Okta shows that cybercrime groups have stepped up their attacks on multifactor authentication systems in an effort to thwart account security measures.

By **Shaun Nichols**

Published: **21 Sep 2022**

How fake login page defeats legacy MFA



Today attackers don't hack in, they log in

Yahoo Announces 500 Million Users Impacted by Data Breach

Jamie White

HELSINKI TIMES

Hacked Finnish psychotherapy service provider declared bankrupt

THE DISTRICT COURT of Helsinki has confirmed it has received a declaration of bankruptcy concerning Psychotherapy Centre Vastaamo, the Finnish provider of psychotherapy services whose client database was compromised in a hacking in November 2018.

The Register

{* CYBER-CRIME *}

Now Oktapus gets access to some DoorDash customer info via phishing attack

BBC Sign in Home News Sport Reel Worklife

NEWS

Home | Queen Elizabeth II | War in Ukraine | Coronavirus | Climate | Video | World | US & Canada | UK | Bu

Tech

Holiday Inn hotels hit by cyber-attack

By Shiona McCallum
Technology reporter

6 September

TC

Twilio hackers breached over 130 organizations during months-long hacking spree

Carly Page

@carlypage_ / 1:00 am PDT • August 25, 2022

The New York Times

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking into the scope of the apparent hack.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

ADVANCED PERSISTENT THREAT —

SolarWinds hackers have a clever way to bypass multi-factor authentication

Hackers who hit SolarWinds compromised a think tank three separate times.

DAN GOODIN - 12/14/2020, 7:00 PM

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement

Home / Enforcement / Recent FTC Cases Resulting in Refunds

Equifax Data Breach Settlement

So what does stop phishing?

True phishing-resistant MFA: Smart Card or FIDO-based authentication

US Gov’t requires Phishing-resistant MFA

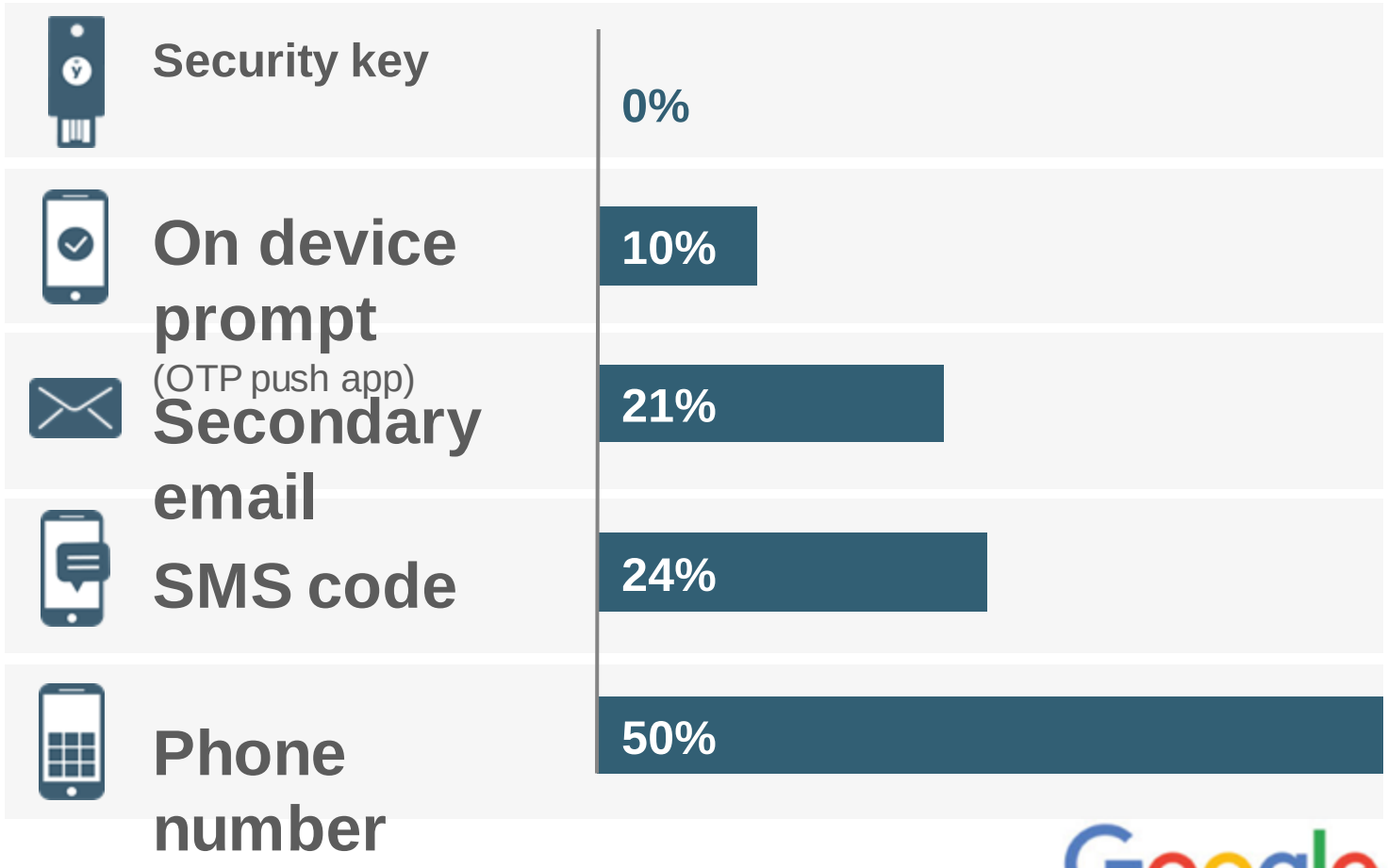
> Phishing resistance is the ability of the authentication protocol to **detect and prevent** disclosure of authentication secrets and valid authenticator outputs to an imposter relying party **without reliance on the vigilance of the subscriber**
>
> NIST 800-63B-4 December 16, 2022 (Draft)

NIST

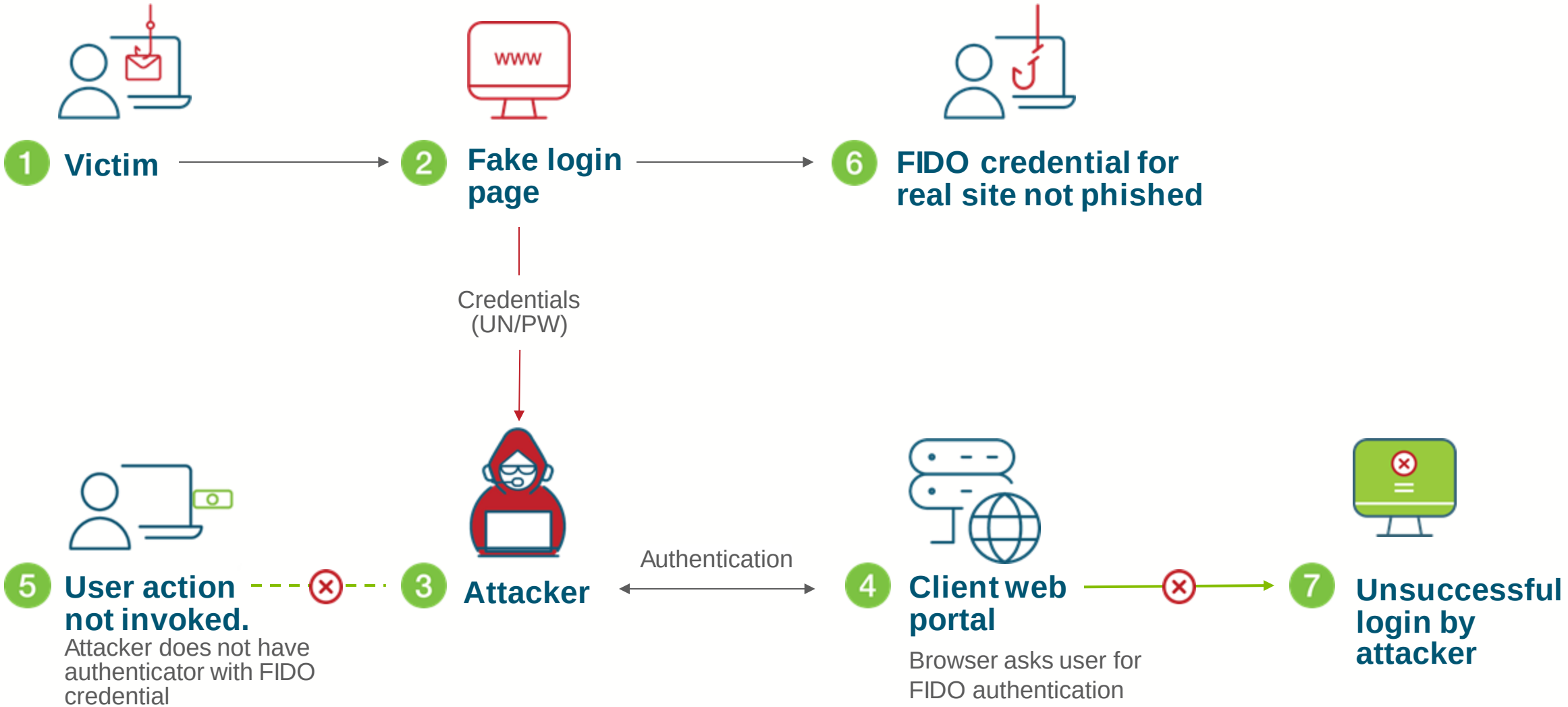
Only FIDO2 and Smart Card/PIV (PKI) are phishing-resistant

Portable hardware security keys

Stop phishing in its tracks. Zero account takeovers.



How modern MFA with FIDO stops phishing



Security Keys for Apple ID

Security keys secure iCloud accounts and Apple devices

> Security Keys strengthens Apple's two-factor authentication by requiring a hardware security key as one of the two factors. This takes our two-factor authentication even further, preventing even an advanced attacker from obtaining a user's second factor in a phishing scam."

Apple, January 2023

Modern strong authentication best practices

Consider a portable FIDO/Smart Card-based hardware security key for phishing-resistant MFA

yubico

The move to passwordless

The hidden time and cost of passwords

The average user struggles to manage passwords for a dozen or more accounts

21 hours

per person, each year, spent on password resets

20-50%

of helpdesk calls are for password resets

$45

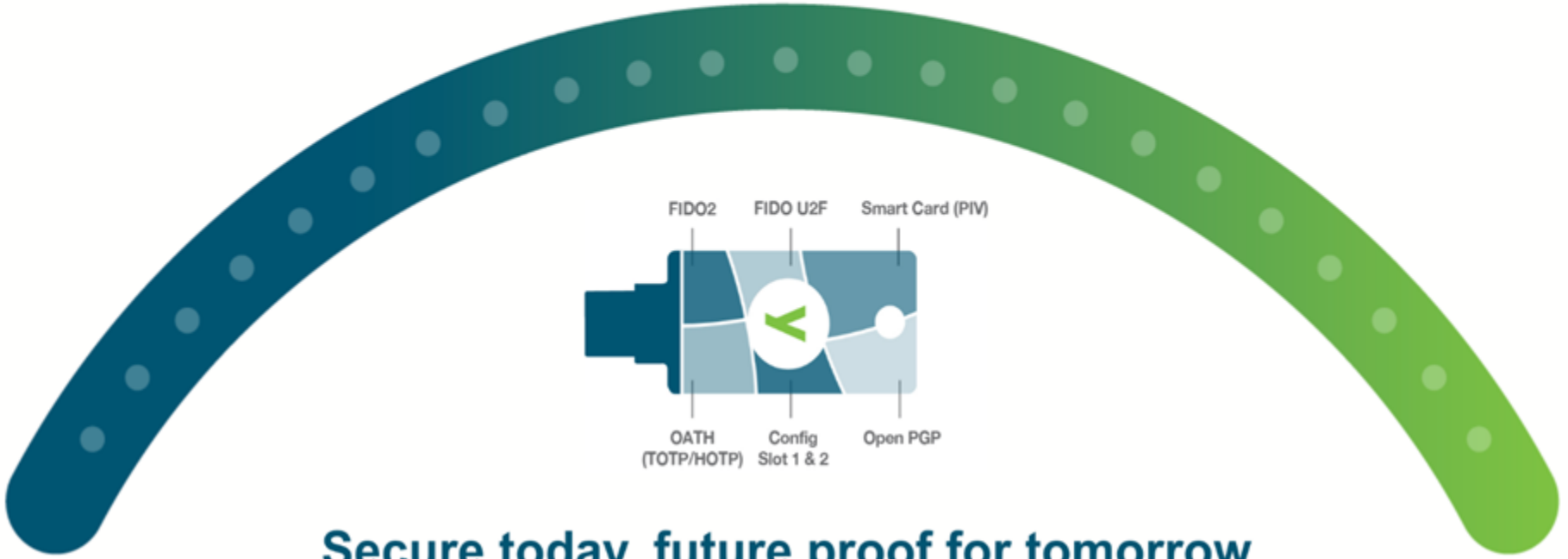
the average estimated cost of a password reset

#1

support cost is password resets

Bridge to passwordless

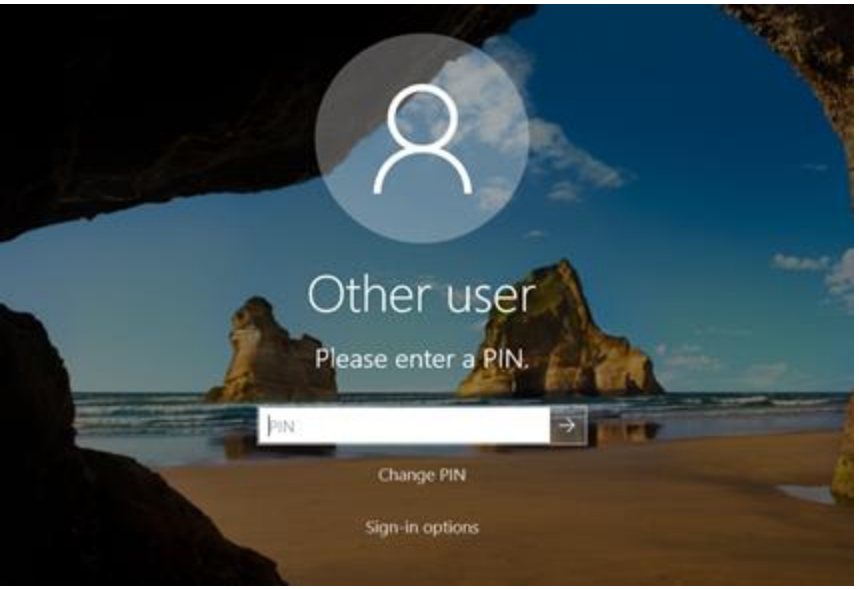
...and support zero trust initiatives



Secure today, future proof for tomorrow

What's the passwordless user experience?

Frictionless, secure account logins lead to greater productivity



Enter PIN
No password

Touch or tap the security key
Fast login / logout, e.g. shared workstations

Phishing-resistant MFA with the YubiKey

Strong security, passwordless-ready, fast and easy user experience

Strongest security with the fastest user experience for authentication

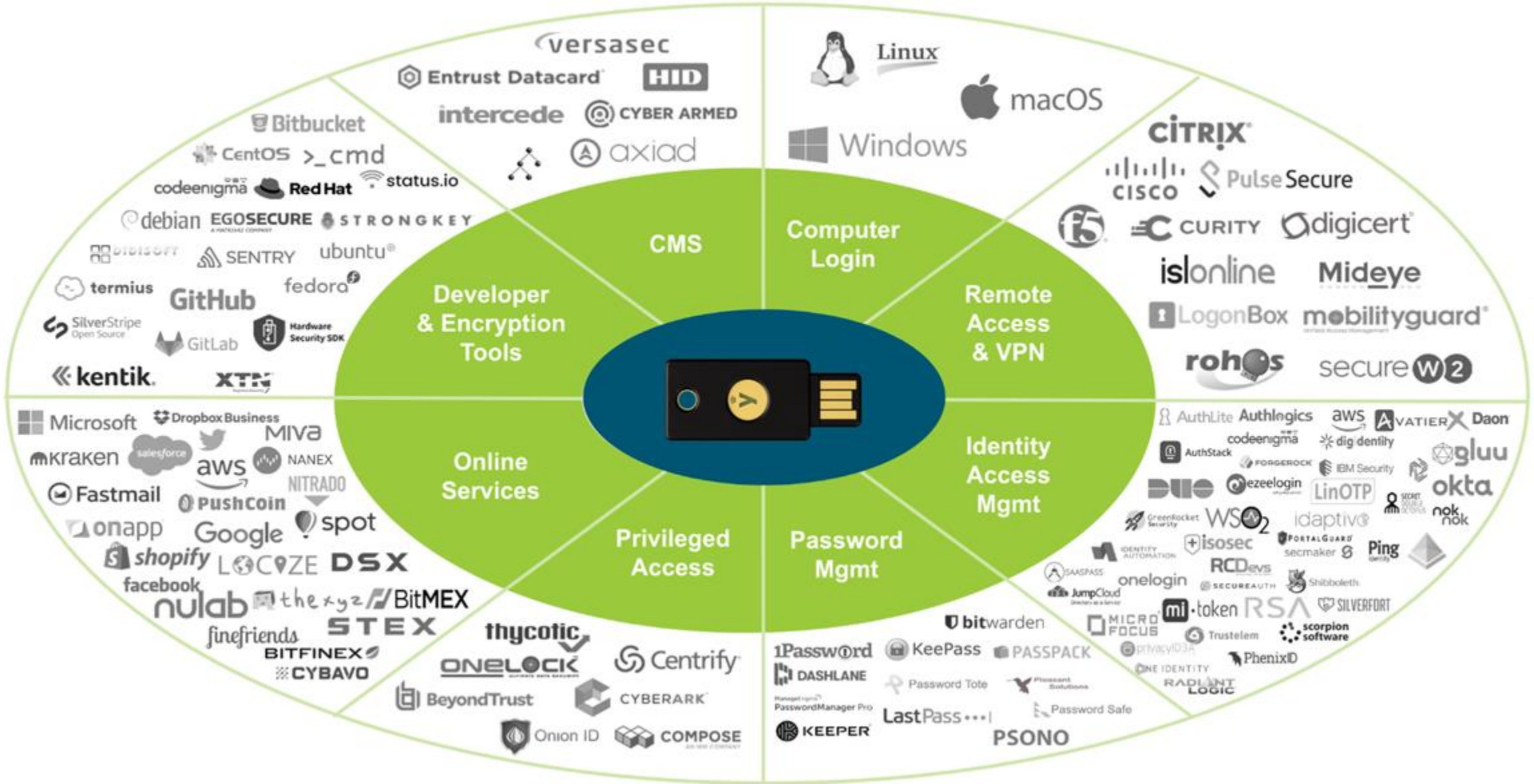
Enter PIN (or password)

Touch or tap YubiKey

Use once

Summary

Look for an MFA solution that delivers strong protection across your legacy and modern applications and services



Think past privileged users in an organization…

Remember! When a breach occurs everyone suddenly becomes a privileged user!

Privileged access

Secure privileged account users

Mobile restricted

Secure call centers for mobile restricted users

Shared workstation

Protect shared workstation users

Remote workforce

Enable remote workforce

Office workers

Improve UX and security for office workers

3rd party access

Protect corporate system access by 3rd parties

End customers

Safeguard Yubico customers end customer

Q&A

Stay safe online.

Questions?

Click to add text

NATIONAL CYBERSECURITY ALLIANCE

Website
StaySafeOnline.org

Twitter
@staysafeonline

Facebook
/staysafeonline

LinkedIn
national-cybersecurity-alliance

Email
info@staysafeonline.org