Advanced MFA passwords.

Nelson Santini
Chief Revenue Officer
BSI

2023

Biometric Signature ID

Protecting your most valuable digital assets.

MFA’s purpose…

What is MFA’s purpose?

MFA was implemented to protect corporations and users’ most valuable digital assets.

We are “IRL” but transact nearly 100% online. We are avatars…

$Billions in costs and losses

Credential sharing
Identity theft or takeover
Ransomware attacks
eCommerce fraud
Internet robot attacks
Privacy management
Regulatory enforcement

By Kelsey Sutton

May 3, 2022 · 6 min read

In my family, password-sharing is its own love language. My sister gets my Hulu password in exchange for her husband's Peacock premium login. My boyfriend's parents subsidize our HBO Max viewing; their grandchildren watch Disney+ using my credentials. My parents spent years watching Netflix courtesy of a neighbor. And one of my best friends, a television buff, accesses all those services plus Paramount+ without paying for any of them herself.

Don't tell me you don't do it, too. As streaming services proliferate, password-sharing is fast becoming one of the TV industry's costliest problems. In 2019, research firm Parks Associates estimated that piracy, which includes account-sharing, cost US video providers $9.1 billion, with nearly a third due to shared and stolen logins; by 2024, the company projects it to grow to $12.5 billion.

While the effects of synthetic identity scams cannot be felt by the dead, the living can still suffer its consequences. These victims might shoulder out-of-pocket expenses, upon discovering that their PII data have been used in a scam. Furthermore, unless the victim can successfully dispute that they were fraud victims, their credit history might get tainted and prevent them from applying for legitimate loans.

Consequently, as these fictitious identities go undetected for a long time, they can cost credit card companies and banks severe losses. Aite Group, an advisory firm, estimates that each synthetic fraud incident can cost lenders up to $15,000, while total annual losses in the United States were estimated to increase to $1.25 billion in 2020.

As synthetic identity fraud often relies on SSNs of unaware individuals, fragmented credit history files associated with varying identities can be created against a single social security number. Credit providers can take up to several years before they can clear out negative data from these files. This type of fraud not only incurs substantial costs for financial institutions but also time and effort by individuals forced at no fault of the

MEDIA

A crackdown on streaming service password-sharing is coming

s Sofalabba

By Kelsey Sutton

May 3, 2022 · 6 min read

Consumers' Trust in PayPal and Amazon to Store Credentials Grows, Putting Banks on Notice

BY PYMNTS | FEBRUARY 16, 2023

Consumers' faith in their primary banks' ability to store sensitive information safely may be slipping.

Trust and security have long been key loyalty drivers for traditional financial institutions (FIs) and may be partially behind why Americans are hesitant to break up with big banks.

- *"Uber hacked, internal systems breached and vulnerability reports stolen" - Sep '22*
- *"Equifax to pay $575M for data breach of 147M people" - Jul '19*
- *"$20B in losses to corporations in 2020" - source PYMNTS*

Let’s set the stage…

Executive order….

“This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government’s defenses against increasingly sophisticated and persistent threat campaigns.

Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.”

Executive Order
M-22-09
26JAN22

MFA

Multifactor Authentication

IS NOT

…a complete solution.

Conventional passwords and physical biometric factors are regularly:

Shared
Stolen
Replicated
Compromised

Said differently:

Today’s MFA is broken.

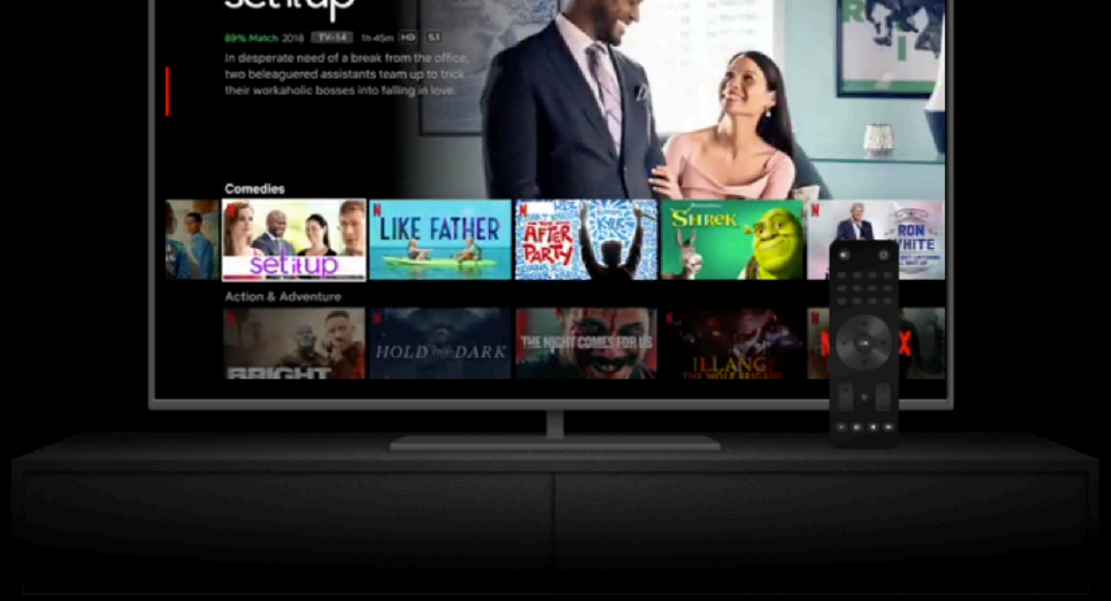
The premise…


It is *unlikely* that an unauthorized actor will have access to, or the time to reproduce multiple evidentiary factors.
MFA

How long does it take you to text a code to friend?

Enjoy on your TV.

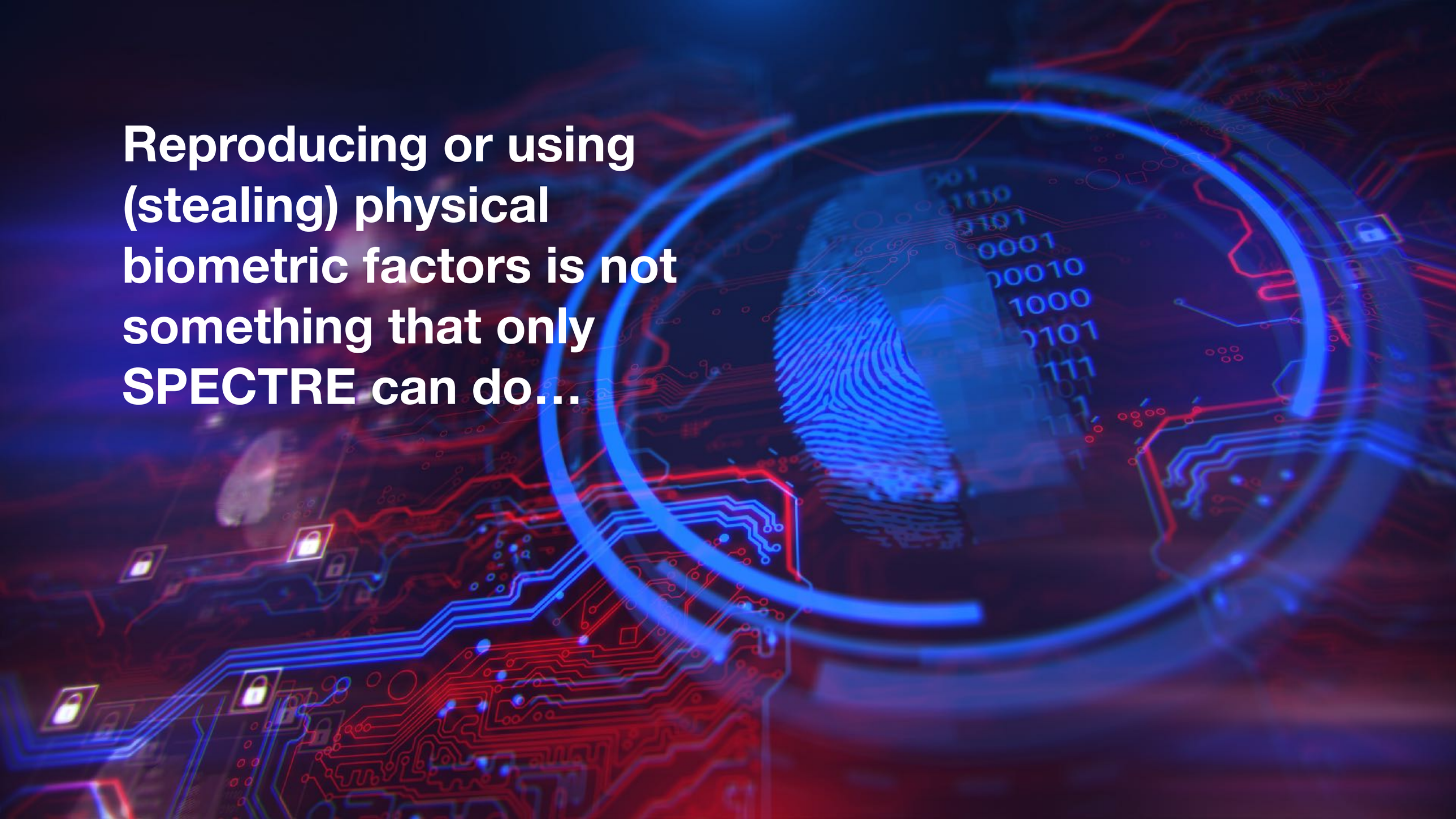
Watch on Smart TVs, Playstation, Xbox, Chromecast, Apple TV, Blu-ray players, and more.



Watch everywhere.

Stream unlimited movies and TV shows on your phone, tablet, laptop, and TV without paying more.

Can your retinal scan be used without your presence?



Reproducing or using (stealing) physical biometric factors is not something that only SPECTRE can do…

MFA

It is *unlikely* that an unauthorized actor will have access to, or the time to reproduce multiple evidentiary factors.

A flawed premise

The factors…

Key elements of MFA

Inherence
Something I am…

Possession
Something I have…

Knowledge
Something I know…

Examples here are your passwords or secret “fixed” codes like a PIN or similar limited release / distribution factor.

Key elements of MFA

Knowledge
Something I know…

Inherence
Something I am…

Possession
Something I have…

Examples here are your smartphone, or a ubi-key, dongle, or other similar device that is under the control of the user.

Key elements of MFA

Possession
Something I have…

Knowledge
Something I know…

Inherence
Something I am…

Examples here are biometrics, both physical and behavioral. These are elements that are part of who the user is.

Newer elements of MFA

Knowledge
Something I know…

Possession
Something I have…

Inherence
Something I am…

Location
This is where I am…

Ability
Something only I can do…

Randomness
Something I know just in time…

Evaluating the different factors

	Can't Share	Can't Steal	Can't Replicate
Knowledge	✗	✗	✗
Possession	✗	✗	✗
Inherence	✓	✗	✗
Ability	✓	✓	✓
Randomness	✗	✗	✓
Location	✗	✗	✗

How can we “plug” the MFA loopholes?

What alternative factors could we use to prevent credentials from being shared, stolen, or copied by human or machine?

SOLUTION

“Randomness” factors

Pros

- Harder to replicate by hackers because they are random and must be used within a finite amount of time.
- Can combine with current technology to increase permutation / commutation power.

Cons

- Require a device that can be lost.
- Eventually even the most random algorithm can be predicted and hacked.
- Introduces friction that may undesirable at times.

Inherence factors - physical

Pros

- Reduce friction in process
- No need to “recall” or remember.
- Are with you and under your control most of the time.

Cons

- Can be “stolen”
- Can be digitally recreated
- Expensive hardware
- Pilferable hardware
- False positive authentications

Inherence factors - behavioral

Pros

- Can’t be stolen
- Can’t be replicated in a timely / practical manner
- Extremely difficult to beat by human or machine
- Have built-in randomness
- Easy to learn

Cons

- Require complex algorithms
- Inject friction in the process
- May be perceived as socially awkward.

The recommendations…

Act like your MFA protocol can be hacked.

Insert randomization into the MFA equation.

Evaluate what type of biometrics you use.

Inherence ≡ biometrics

A question of “when do I use which?”

The mental state of the user is irrelevant to the outcome.

It is imperative to be right, so slowing down a bit is ok.

Moving quickly is more important than safely.

I want to manage high risk.

The physical presence of the user is not an essential.

The transactions is of low consequential value.

The transactions is of high intrinsic or consequential value.

You can’t afford a false positive.

It is critical that the user be present of body and mind.

Carrying additional hardware cost is ok.

There is low risk to worry about.

Unlikely that the user will lose a small pilfer able device.

You can afford a false negative.

Inherence = biometrics

A question of “when do I use which?”

Behavioral Biometrics

It is critical that the user be present of body and mind.

It is imperative to be right, so slowing down a bit is ok.

The transactions is of high intrinsic or consequential value.

You can’t afford a false positive.

I want to manage high risk.

Physical Biometrics

Moving quickly is more important than safely.

Carrying additional hardware cost is ok.

The physical presence of the user is not an essential.

You can afford a false negative.

The mental state of the user is irrelevant to the outcome.

Unlikely that the user will lose a small pilfer able device.

There is low risk to worry about.

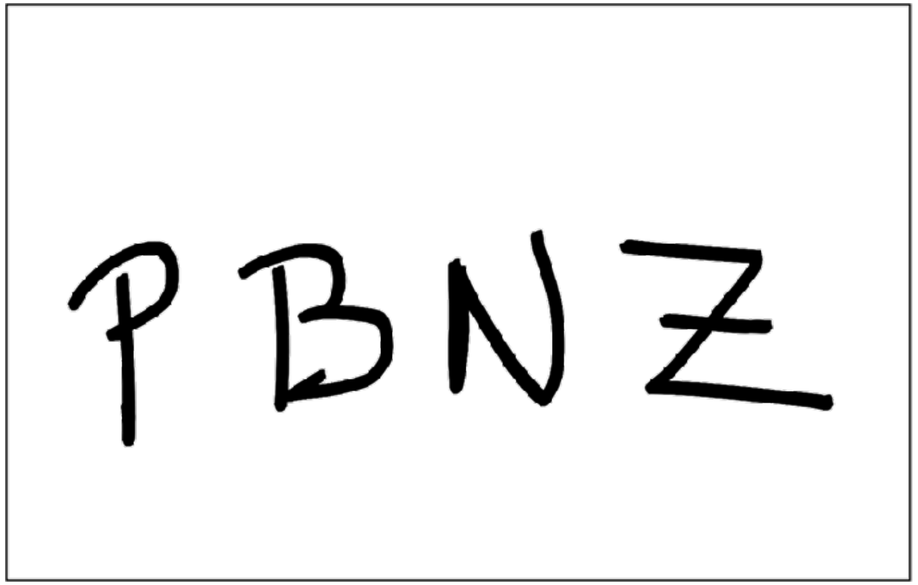
The transactions is of low consequential value.

The “written” / “drawn”…

Behavioral biometrics

About *written / drawn* passwords…

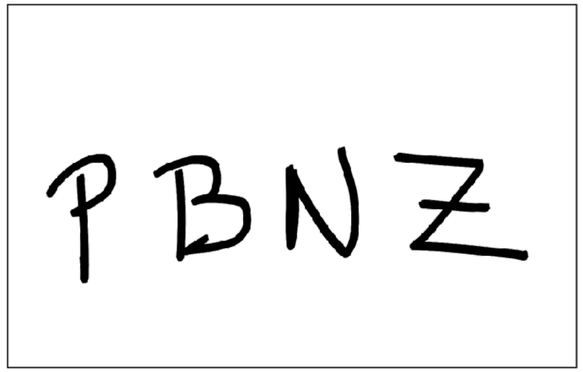
- They are not authenticated as “calligraphy”
- It’s not about “pretty” it is all about “can you repeat it”
- Mathematically, nearly impossible to beat.
- Will “trip” a robot trying to replicate.
- Inherently “random”, yet “predictable”
- Easier to memorize (eg. Your signature)
- May require mental clarity / focus
- Don’t require training. Require proficiency.



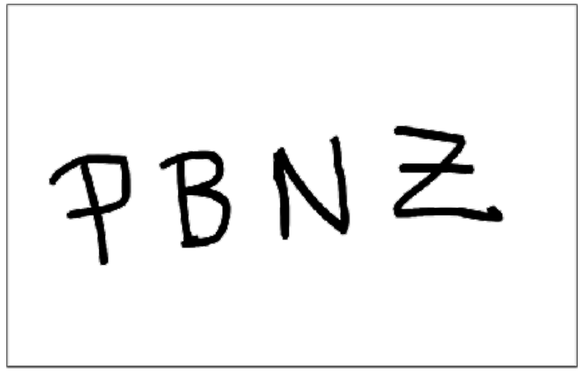
>BNs : 1 odds to hack….
Inherently random

Behavioral biometrics

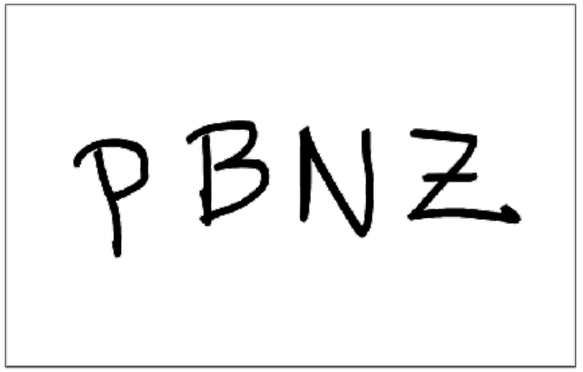
About *written / drawn* passwords…



Example 1



Example 2



Example 3

Same “code”, but not the same..

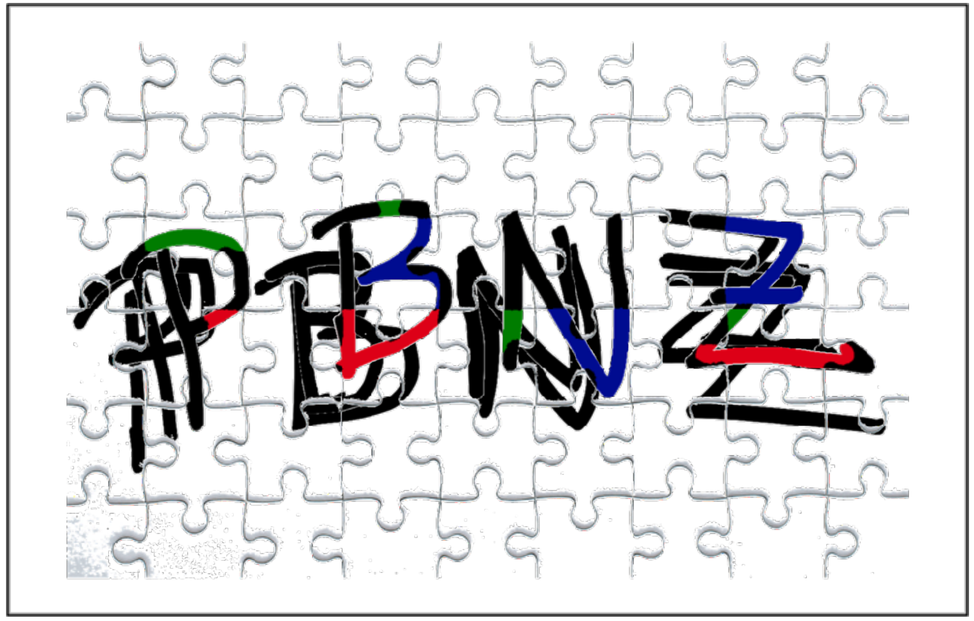
Behavioral biometrics

About *written / drawn* passwords…

It’s not about comparing pictures…

Behavioral biometrics

About *written / drawn* passwords…



- Random
- Inherent
- Ability

It’s about how only you can build the picture…

A tested version of behavioral biometrics in use…

Biometric Signature ID

Protecting your most valuable digital assets.

Advanced MFA

BSI's Behavioral Biometrics

"I am"	"I know"	"I have"	"I can do"
Awareness	Code / Password	Device	Signature

Physical Biometrics

Face, Walking, Palmprint, DNA, Veins, Retina, Palm Geometry, Fingerprints

Can be stolen, replicated, or shared.

Most products and solutions meet only one of the MFA requirements.

Code / Password

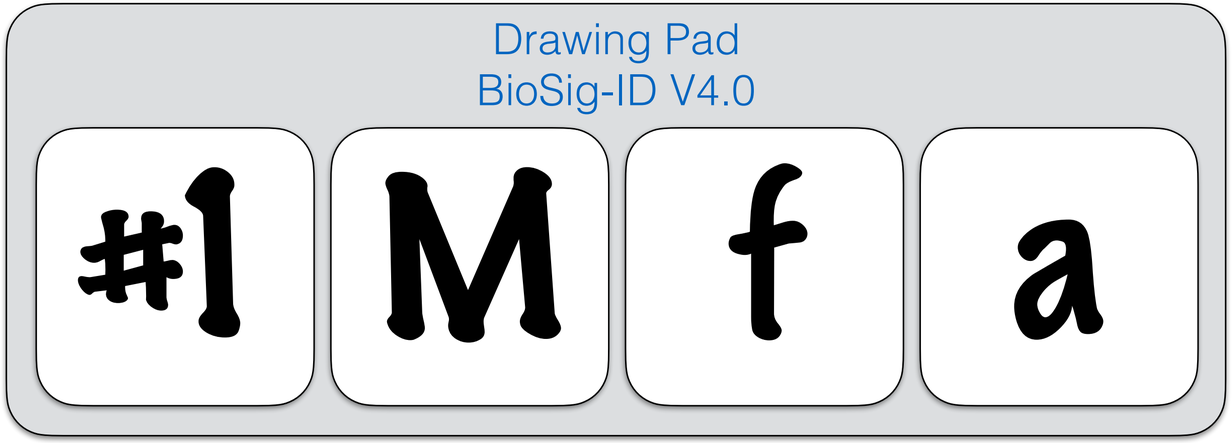
UBI Key

+

Others Tech.

Unique and robust credentials

- Needs no special hardware
- Has no private identifiable information
- 192 billion to one link to a human
- Linked to user's state of mind
- All-at-once Advanced MFA
- Patented



Behavioral biometrics close critical MFA loopholes.

Biometric Signature ID

The best cybersecurity move for today's MFA.

(We are winning. Are you in?)

Protecting your most valuable digital assets.

BSI

Biometric Signature ID

2023