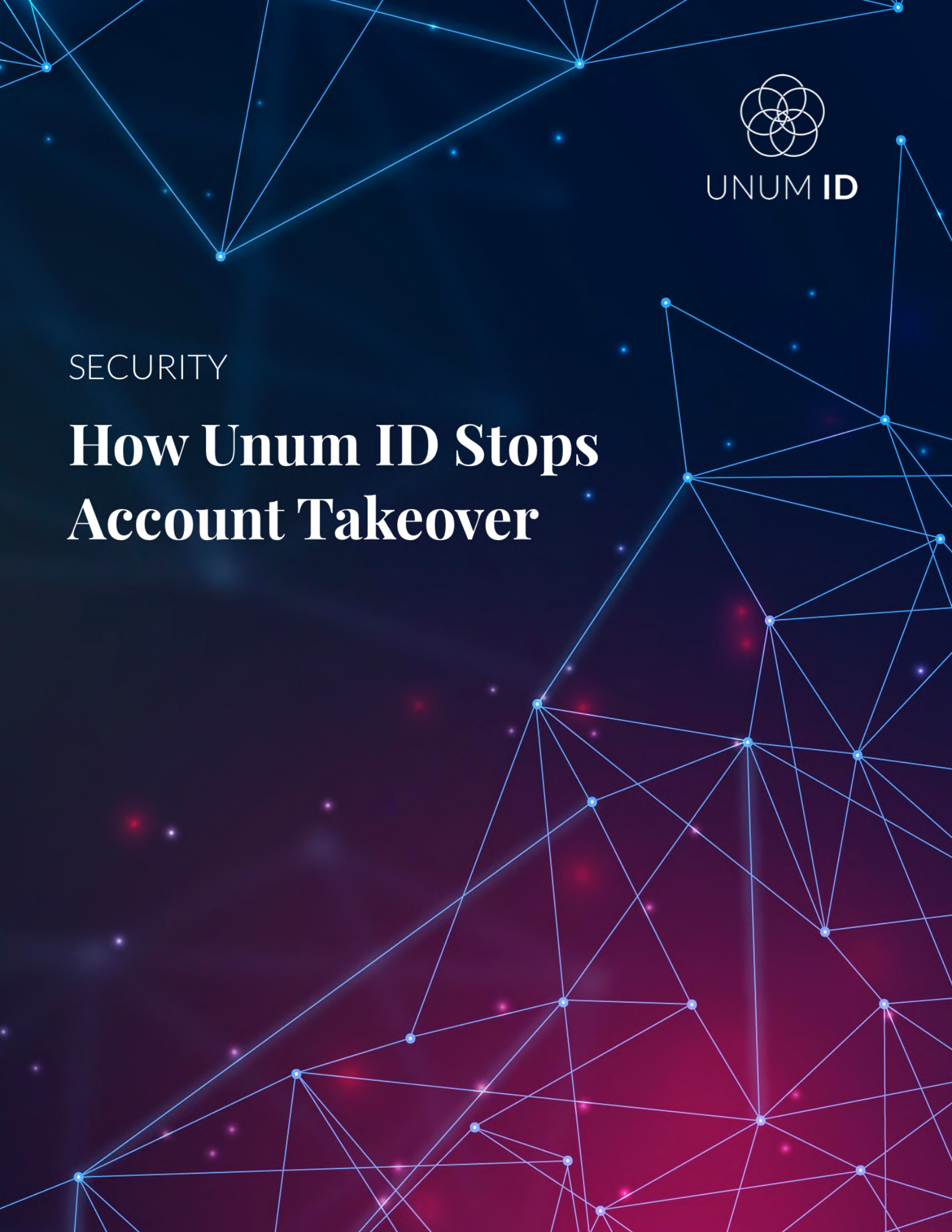

SECURITY

How Unum ID Stops Account Takeover

Table of Contents

Introduction

Account Takeover

Account takeover is perhaps the most significant cybersecurity threat facing modern enterprises. For example, Kaspersky found that in 2020 account takeover comprised over half of all fraudulent transactions in the finance industry.

The most common form of account takeover is social engineering. Attacks have moved "up the stack" from low level technology to the highest level and most vulnerable component: human beings, who are easily fooled.

Traditional authentication schemes, even those with multiple factors, fail to stop most account takeover attacks. But Unum ID does so with ease by eliminating the target: shared secrets. In this white paper, we examine three of the most common types of attack — **phishing, SIM swapping, and credential stuffing** — and explain how Unum ID protects against them.

About Unum ID

Unum ID is **the sharified identity™ network.** Companies use our technology internally for passwordless authentication and externally for sharing verified identity data with other organizations, with full user consent. *This white paper focuses on authentication specifically, but note that the security guarantees described here apply to* all *Unum ID solutions.*

Our authentication product Beyond Passwordless™ is so named because it goes beyond other "passwordless" solutions, many of which still rely on other shared secrets like one-time passcodes (OTPs) and session tokens. All such secrets are vulnerable to social engineering attacks like phishing, SIM swapping, session hijacking, and more. Unum ID relies on far stronger security, based on asymmetric cryptography with private keys stored in the secure hardware of users' mobile devices.

You can use Unum ID to replace or augment your company's existing account system. By adding Unum ID on top, you can gradually transition away from passwords without needing to eliminate them right away. To get started, contact our sales team.

Technology Overview

Fundamentally, **Unum ID eliminates shared secrets.** Whether passwords, passcodes, PINs, or otherwise, shared secrets are the cause of almost all account takeover attacks. We replace them with biometrics and asymmetric cryptography, tied to the trusted execution environment (TEE) of the user's device.

When you deploy Unum ID, you add our Mobile SDK to your app. From a security perspective, the crucial feature of this SDK is that it leverages the secure hardware element of the user's device to create, store, and use private keys, conditional on the user passing biometric checks.

The hardware element has a unique property: no one (not even the phone manufacturer) can ever access the keys stored there, but we can trigger it to generate cryptographic signatures *using* the keys and return the result. This ensures not just that there are no shared secrets but also that the private key is stored and used in an extremely secure way, on a device the user already has, in a way that requires no expertise from the user. To them, authenticating is as simple as clicking a button and passing a biometric check.

Unum ID means "one identity", and that is what our technology creates: *one identity online for each person offline.*

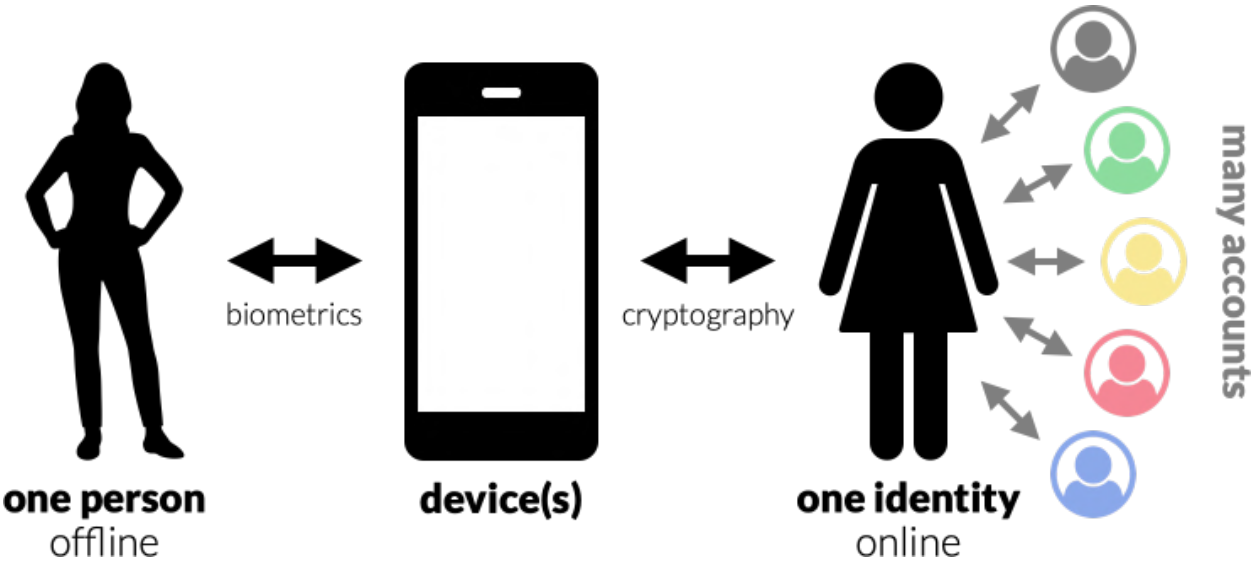

Figure I: Biometrics + Cryptography = Unum ID

Unum ID leverages biometrics and cryptography tied to the secure hardware of the user's device to establish one identity. There are zero shared secrets involved, which allows Unum ID to stop account takeover in its tracks.

FAQ

Do we have to replace our account system?

No. Unum ID integrates with your existing account system, facilitating a gradual transition away from passwords. First, you can use Beyond Passwordless™ for additional factors of authentication, on top of your current login. Later, when you're ready to eliminate passwords, you can use for a standalone multi-factor auth flow.

What if a user loses their phone?

Not a problem. The user's app is backed up, and they can remotely deactivate their lost phone, just like they can cancel a credit card. The default backup is to the user's iCloud (on iOS) or Google Drive (on Android) account, so when they get a new phone everything will work like before.

Unum ID requires that the user has a device passcode and/or biometric set up. Lost phones that have these enabled are extremely secure. (Even the FBI couldn't break into an iPhone.) But for extra protection, we provide a way for the user to remotely deactivate the app on the lost phone, making it useless even if an attacker breaks through the biometric. And for ultimate protection, the user can choose to remotely erase their device.

Does the authentication work on non-mobile devices?

Yes, it works everywhere. Unum ID transforms your app on the user's phone into a virtual ID card, and everything goes through the phone. On a desktop website, they scan a QR code. On a mobile website, they click a button. In person, they scan a QR code. On a support call, they get a push notification or SMS. (They can also make the call from within your app and be pre-authenticated.) In all cases, they can choose several alternative flows — using push notifications, links sent by SMS or email, etc.

What if a user has multiple phones?

They can use all of them and keep them synchronized.

Phishing

Phishing and its many nautical cousins (spear phishing, whaling, and more) involve luring a user into sharing a secret, like making a fish bite a hook. Unum ID prevents this by ensuring that there's no secret for the user to share and that the user never has to rely on intuition to avoid attacks.

The Attack

1. The attacker creates material that looks convincingly like the company's.
2. The user shares a secret with the attacker, believing them to be the company.
3. The attacker uses the secret to access the user's account.

Examples

- You receive an email that looks like it's from your bank but isn't.
- You get a call from someone pretending to be a customer service rep.

Fundamental Causes

- **Traditional systems use shared secrets** like passwords and one-time passcodes. Any secret a user can remember is one they can accidentally share with attackers.
- **Traditional authentication only goes one way:** The company authenticates the user, but the user has to rely on intuition to know if they're interacting with the company. *Does that logo look right? Is that the correct URL? Why did Gmail mark this as suspicious?*

How Unum ID Prevents It

- **Unum ID uses zero shared secrets.** We use private keys stored in the secure hardware of the user's device, to create cryptographic signatures. This is done behind the scenes for ease of use. There are no secrets for the user to remember or share.
- **Unum ID authentication is bidirectional.** The company authenticates the user, *and* the user authenticates the company. No data is exchanged unless both the user and company are valid. Our tech checks the company's signature on the user's behalf.

As a result, though an attacker can give the appearance that they're legitimate, a user is literally unable to share data with them. Unum ID ensures that your company's security doesn't depend on users' ability to sniff out suspicious communications.

SIM Swapping

SIM swapping has skyrocketed as more and more companies rely on one-time passcodes sent over SMS as a second factor of authentication. Although this enables a relatively convenient two-step login flow for users, it has serious security vulnerabilities — NIST deprecated it in 2016. Unum ID prevents SIM swapping by eliminating the need for one-time passcodes (or any other shared secrets) altogether.

The Attack

1. By bribing an employee at the user's phone carrier, the attacker redirects the user's phone number from the user's SIM card to the attacker's.
2. The attacker then receives the user's two-step verification code, which is an OTP (one time passcode) sent by SMS.
3. The attacker accesses the user's account.

Fundamental Causes

- **The user's identity is tied to their phone *number*, not their physical device.** The phone number can be redirected remotely. Phone numbers were never designed to be human identifiers, and they shouldn't be used in that way.
- **One-time passcodes (OTPs) over SMS rely on telcos, which aren't incentivized to stop the fraud.** The telcos could in principle stop the fraud, but they have no economic incentive to do so. It's easy for an attacker to bribe an entry level telco employee to redirect a phone number, and the cost of fraud affects your company, not the telco you're relying on for SMS functionality.

How Unum ID Prevents It

- **The user's identity is tied to the secure hardware of their physical phone.** This cannot be accessed remotely or without passing a biometric check. (Even the phone manufacturer cannot access it.)
- **The authentication process is internal to your company — it doesn't involve telcos or other third parties.** There's no misalignment of incentives. Your company has complete control over the authentication process.

Unum ID ensures that your company's security is dependent only on systems you control and that accounts cannot be accessed remotely, even by highly sophisticated attackers.

Credential Stuffing

Credential stuffing is a sophisticated version of a brute force attack that reveals the collective risks each company faces from breaches to other company's systems. Unum ID prevents credential stuffing by eliminating shared secrets so that no list of breached passwords will ever allow an attacker to break in.

The Attack

1. The attacker acquires secrets spilled from *other* organizations.
2. The attacker "stuffs" those secrets into the company's account login to find a match.
3. The attacker accesses the user's account.

Fundamental Causes

- **Traditional systems rely on secrets users create and remember.** No human being can remember the enormous number of passwords they have, and yet only 3 percent of people rely on a password manager, and 86 percent of people memorize passwords in their heads. As a result, people routinely reuse passwords across sites.
- **Secret based systems face a tragedy of the commons:** Because people reuse passwords across sites, a breach of *another* company's systems can compromise *your* company's accounts. Even if your company has strong security policies, that other company may be an easy target, a lowest common denominator.

How Unum ID Prevents It

- **Unum ID uses zero shared secrets.** We use private keys stored in the secure hardware of the user's device, to create cryptographic signatures. This is done behind the scenes for ease of use. There are no secrets for attackers to use for access.
- **Unum ID authentication is specific to your company.** There's no dependence on any secret the user may also use with another company, so there's no tragedy of the commons or lowest common denominator dynamic.

Unum ID protects your company against the threats posed by other companies' data breaches. As an added benefit, it removes shared secrets as the main threat to a breach of your own databases. **Unum ID ensures that your security is in your control.**

Get Started

Unum ID is the end of ●●●●●●●●●. Leave shared secrets behind. No more passwords, PINs, one-time passcodes, CAPTCHAs, knowledge based questions, magic links, or backup phrases. Shared secrets make for bad security *and* bad user experience.

Unum ID provides a better way. To get started, contact our sales team or visit our website. We look forward to working with you.

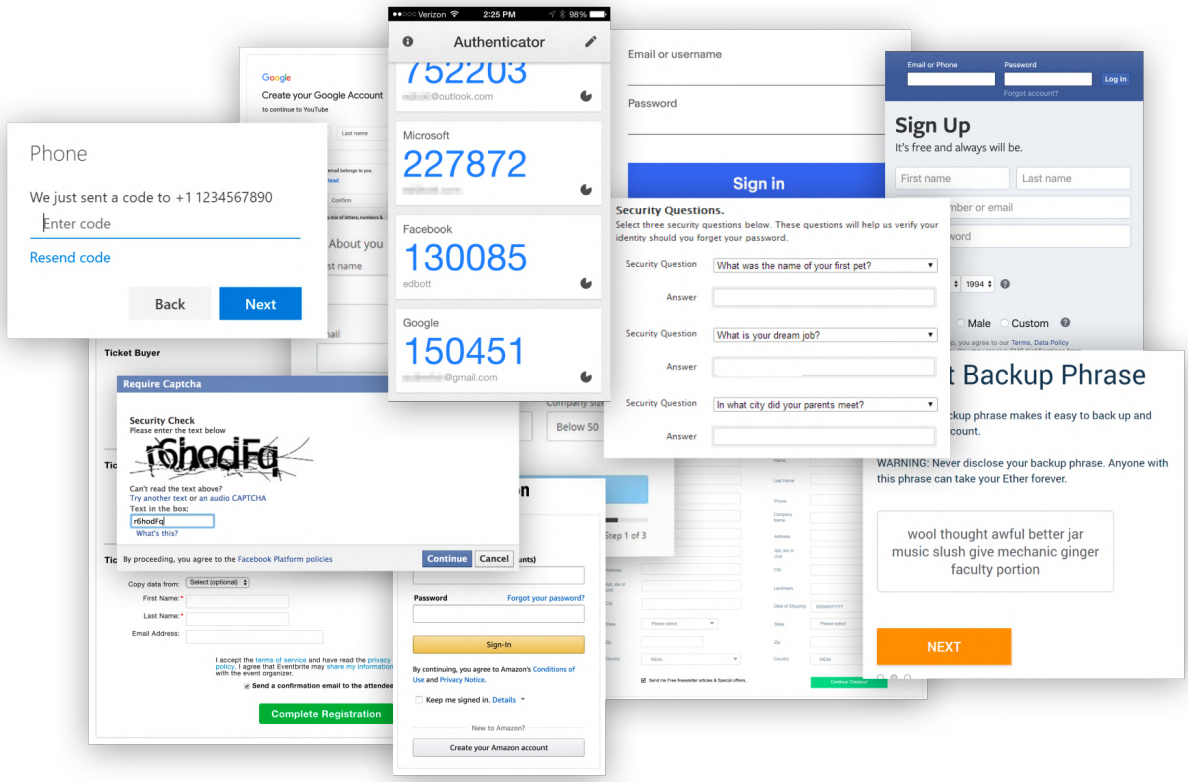

Figure II: Auth = Ouch

Legacy authentication makes for bad security and *bad user experience!*