7 THE DEADLY MISTAKES OF AUTHENTICATION

CONTENTS

EBOOK OVERVIEW

As the science of identifying and permitting entry to digital users has evolved over the years, so too have the many ways in which people with bad intentions become more effective at corrupting that science, while also becoming more elusive. Traditional methods for authenticating users at the point of login are more vulnerable than ever, and additional methods for further securing the login process, rather than make users safer, can even provide alternate avenues for bad actors to compromise the process.

To that end, both user and enterprise need to recognize the most common authentication mistakes, in both choosing and using technology. Relying on the wrong tools, engaging in risky practices, and failing to recognize the holes in an authentication scheme can lead to costly breaches and company-wide disruption. authID illustrates the "***Seven Deadly Sins of Authentication"*** to educate organizations, their employees, and their customers on how to avoid the consequences of weak tech and bad choices when it comes to safeguarding the authentication process.

ABOUT AUTHID

authID (Nasdaq: AUID) ensures enterprises "Know Who's Behind the Device" for every customer or employee interactions, through our easy-to-integrate, patented, biometric identity platform. authID quickly and accurately verifies a user's identity, to protect accounts and other digital assets. By creating a biometric root of trust for each user, authID stops fraud at onboarding, detects and stops deepfakes, eliminates password risks and costs, and provides the fastest, frictionless, and most accurate user identity experience in the industry.

AUTHENTICATION THREATS

We are all creatures of habit. We take comfort from those things we are most familiar with. Familiarity means we've mastered a thing, and find it convenient, since we know how to use it. Taking sideroads to Grandma's house, even when the highway is quicker, although scarier. TV dinners instead of fresh vegetables.

Not everything that is the same now as it always existed is necessarily bad. Musical instruments. The wheel. Calculus, Bicycles. Eyeglasses. Flush toilets. Keyboard shortcuts.

But yes, some items that have been around a long time can in fact be bad. Such as … how we log into our stuff. Those other things mentioned above won't get your data stolen, your credit card compromised, or an entire healthcare system shut down by ransomware.

"Universities, government agencies, corporate infrastructures, gaming operations and many others have been victimized by ransomware"

We all want to fly on safe planes. But we also want to get through the airport line as swiftly as possible, and so in many countries we allow for somewhat lax safeguards. Likewise, we want to get into our applications as quickly and simply as possible. And this is where all our trouble starts in the digital world.

The consequences of poor practices when it comes to authentication can be far-reaching, not just for the individual but for their larger organizations. Yes, individual accounts can result in individual losses. But when users are in positions of enhanced access, as when they can affect infrastructure or the accounts of other users, poor authentication security can spread ill effects throughout the entire institution and beyond, to customers, partners, and the general public.

How does weak authentication put all of us at risk? We'll look the consequences in detail, but in summary they manifest themselves thusly:

- Theft. Bank account get drained. Wire transfers get initiated by criminals in the name of their victims. Intellectual property gets stolen by competitors or state-sanctioned foreign criminal rings.

- Impersonation. Bad guys break into social media or other accounts, take over communications with the friends, family, or colleagues of their victims, and send out malware, requests for money, or demands for ransom to unsuspecting parties before the victims have time to alert those others.

- Data breaches. These common crimes fuel their own versions of ransom demands, and also fuel fraud committed against those whose data is exposed.

- Financials. Public companies especially guard their financial data jealously, and wish to control its release, such as at critical times like after quarterly earnings announcements.

- Ransomware. This insidious attack has targeted individuals for years, but the more lucrative path for criminals is targeting institutions. Universities, government agencies, corporate infrastructures, gaming operations, and many others have been victimized by

ransomware. The most evil ransomware occurrences have hit healthcare facilities, delaying treatments and even surgical procedures, sometimes for months at a time. Again, why hold up one victim at a time when there's a much bigger payday in forcing and entire organization to cough up ransom?

Let's examine the most common – and from a digital perspective, deadly – mistakes when it comes to accessing applications, and the data they control. These mistakes of convenience are what allow all the wrong people to access these assets for their own benefit, and at the expense of the general public.

"The most evil ransomware occurrences have hit healthcare facilities"

Why are these following authentication methods "mistakes?" Because all of us should know better than to use them, yet we use them anyway. Not everyone who uses them knows they're mistakes, but most everyone reading this article is in the business of, or has an interest in, more secure access to digital assets. So these people should absolutely recognize the mistake of falling for these convenient mistakes.

What else is convenient? Leveraging two more familiar things:

- Something we know
- Something we have

What's in our heads, and in our hands, is what we fall back on. And that's a mistake. The first of many. Let's start with the first mistake: something we know.


PASSWORD
LOCKED
ATTACK

DEADLY MISTAKE #1 - PASSWORDS

Passwords are simple. They're just a few characters. But here's the first mistake of this mistake. Because they're simple, they're inherently weak.

But the term "weak passwords" is redundant. People do indeed often employ weak passwords. This is the same as saying water is wet. They use variations of their own names, their kids' names, birthdays, series of letters or numbers. It's a cliché, but it's still a fact that a commonly used password is "password.'

But beyond the actual passwords themselves, the very ***concept*** of passwords itself is weak. Consider this progression:

1. I protect my account with a password.
2. Oh man, I used the password "password" and it got brute-forced, so my account was hacked.
3. I made my next password my nephew's name.
4. Oh man, somebody figured out my new password from my Facebook page and hacked my account again.
5. I made my next password "Th1spAssw0rd!srea11yh#rD."
6. Oh man, I clicked on a phishing link and the ensuing malware copied my keystrokes and captured my password, and I got hacked yet again.
7. I made my next password "YouJerkzc&ntsp00f-thiz1" and added one-time-PIN.
8. Oh man, a data breach exposed my latest password and the bad guys used SIM swap to steal my PIN. And hacked me again.
9. I'm now just using cash, like my ancestors did.

In the authentication universe of using what you know and what you have, the answers to security questions are things you know. And someone else can easily know them.

"The term "weak passwords" is redundant"

As we will discuss, even when more enhanced methods are employed, their root often remains a password. We reset or recover them using a password. So even when it's not the only tool in the bag, the password remains a vulnerability, since passwords are the weakest link in any authentication scheme. So in this way, the very user of passwords is a mistake.


File
Options
Import
Editing

DEADLY MISTAKE #2 - SHARING TOO MUCH ONLINE

All too often we invite our own digital misery into our own lives by giving the keys to the bad guys. While we may not be blatantly putting our passwords out there, we publish everything we need to hurt ourselves. People are inherently social animals, but the internet lets us turn sociability into, well, stupidity.

Far too many people provide far too much data about themselves, the kind of information that help bad actors determine passwords or the answers to security questions.

Social media is a treasure trove of data for bad guys who can now use AI to dig even deeper, faster.

"The internet lets us turn sociability into stupidity"

Account / password resets are the perfect opportunity for this data to be used for break-ins.

Pictures and profile info also allow bad actors to do just that, act. They can easily impersonate victims. Too often we get Facebook messages from friends saying, "Don't accept an invite from me, I've been hacked." But they haven't been hacked, they've been cloned. A fraudster grabbed their profile pic and basic information from social media and created an impersonation profile.

Why do so? To fool friends and family, maybe claim an emergency and ask for money. Or to possibly gain even more access to those friends and family members.

All this over-shared information directly feeds into the next mistake, or at least a portion of it.

DEADLY MISTAKE #3 - KBA-BASED PASSWORD RESET / ACCOUNT RECOVERY

The infrastructure required for KBA (knowledge-based authentication) is so considerable, companies that put it in place hate to move away from it, even when their customers, their admins, and the people down the block despise it. KBA entails asking questions that presumably only the targeted user knows the answers to.

KBA can take two forms. First, the user may create their own answers to security questions that typically come from a drop-down choice. Name of first pet, make of first car, the year they met their significant other, favorite book or movie, etc. These are dangerous as these answers may be discerned from the aforementioned abundance of social media data shared by people too eager to share.

There was a famous case of just such an occurrence that perfectly illustrates this. A political candidate found her email had been hacked when a prankster entered her username into a common platform and clicked “forgot password.” Her security questions were all based on things about her life that were easily Googled.

Clever users might try to thwart such pranksters (or worse people) by installing bogus answers. “The make of my first car? Blue. Favorite book? Pudding.”

But here’s the problem with that. Even when the answers are real, more than forty percent of users forget at least some of their own security question answers. So they lock themselves out.

The other method for KBA is the use of data brokers to provide more in-depth questions, such as about a user’s first mortgage, first car, the amount of that mortgage. But the problem *there* is that much of this data is available on the dark web, making the data even more accessible to fraudsters than to the users who have long forgotten those details of their own lives.

> ***“The data brokers feed the very fraud they are meant to prevent”***

In 2014, a particular government agency’s document site was breached, affecting hundreds of thousands of citizens, requiring the legitimate users to identity-proof themselves, and needing to answer ridiculously obscure questions, fueled by data brokers, about first mortgages, first cars, long-closed bank accounts, and other obscure information that might be more readily accessible to criminals using the dark web than to the real citizens.

So data brokers are used in the practice of validating identities, but when they are breached (which seems to happen with alarming regularity), the data brokers feed the very fraud they are meant to prevent. This represents a vicious cycle.

We used to jealously guard our Social Security numbers. By now, they’re all out there. And if information stored by those brokers is inaccurate or outdated, it still sits out there forever, waiting to misrepresent us. And so-called thin-files, meaning individuals without sufficient public data available, might not have enough of a profile to be proofed.

Much like the concept of passwords themselves, KBA is dreadful by default. Not only is it vulnerable through breaches, and prone to

lockouts through forgotten answers, it's just plain a lousy user experience. Just like waiting for the dreaded beep when walking through the airport metal detector, users hate having to deal with those security questions.

In the authentication universe of using what you know and what you have, the answers to security questions are things you know. And someone else can easily know them.


ON THE MOO

DEADLY MISTAKE #4 - PASSWORD REUSE

It was a very good thing when somebody invented password expiration. Keeping the same password indefinitely is an invitation to a fraudster to keep plucking away until they break into an account. Depending on the policy of any given organization, passwords have to be refreshed every sixty to ninety days. This is pretty much a de facto security stance for most companies.

But the hole in this policy, at least in some places, is allowing old passwords to be reused after a certain period, or after a certain number of passwords have rotated. The only reason for this allowance is the convenience of users who memorize a handful of passwords that they use across various applications. It's much easier to pull another of those passwords out of the bag and use it again than it is to come up with another combination of letters, numbers, upper and lower case, and special characters to satisfy rules on password complexity.

> ***"It was a very good thing when somebody invented password expiration"***

One might easily make an argument against allowing password reuse, since it gives criminals a finite number of targets to guess or steal. But it's an even worse policy for a reason that many might not think of. Data breaches have exposed user credentials from many platforms over the years, and these creds get sold on the dark web. Such files of stolen credentials live forever, just like anything else that gets published on the internet. This means these credentials circulate indefinitely. Therefore it may be years before certain credentials get used, or at least get used successfully.
So let's say a file contains your password as of right now. But by the time a bad guy gets around to combing through the many thousands of credentials and finds yours, you've been obliged to change your password at least once or twice. But just about the time he gets around to trying out that old password, it's now your new password, since you've changed it enough times that you're now allowed to go back to that old one. Everything old is new again, and the bad guy is more than happy to use it against you.

Let's consider another way that using a finite number of passwords, or password reuse, can haunt you.

DEADLY MISTAKE #5 - REUSING SAME CREDENTIALS ACROSS MULTIPLE PLATFORMS

Another symptom of user laziness is the use of the same credentials across multiple platforms, such as your email, Facebook, LinkedIn, TikTok and the rest. This approach makes it simple to log in from site to site. And now it changes things up for hackers. They may still have a large number of targets in terms of guessing or stealing passwords. But once he successfully gains that magic password, he now can unravel multiple accounts. Hack one, get the rest. This approach to account takeover is called “credentials stuffing.”

Add another slight twist to this. A massive convenience to consumer users is the ability to use social media credentials in the creation of accounts on new platforms. As in, “register with your email, or use Google or Facebook to log in.” Countless users use common social media accounts as their basis for federating their identities into new sites. But for a simple reason, this is not nearly as secure as using one’s email to create a whole new account: if a bad actor acquires those social media credentials, he can then take over all the other accounts those credentials provide access to.

It’s easier to create a new username than it is to create a new password, since username formats aren’t nearly as restrictive as password formats. In fact, usernames often allow special characters, and upper/lower characters are meaningless. Also, there are two hassles to generating new passwords to fit the rules. First, a user needs to create that password which doesn’t match the current password and fits the complexity requirements. Second, the user needs to remember that rotten password. The solution to the latter problem? Write them down.

It’s ironic that we have long been told to not write down passwords, but often crypto users are told to do just that, because storing passwords digitally, especially on our phones, makes us vulnerable to being hacked. A physical, analog record of passwords kept in a secure location can actually be safer than digital storage of those same passwords.

> ***“Countless users use common social media accounts as their basis for federating their identities”***

The other danger to storing the digitally is, this makes it more likely that users will cut and paste those passwords from their password files (such as something they keep in Notepad or the like), and this in turn encourages the practice of using the same bunch of passwords over and over.

Based on this mistake and the previous one, an observer might say, well, preventing these practices from being advantageous to hackers means users must perpetually create new, complex passwords for every platform being used that, upon expiration, must be replaced and never reused. The answer to that is, well, yep.

DEADLY MISTAKE #6 - PRIVILEGED ACCOUNT MANAGEMENT

To any given consumer, the takeover of even a single account among their many is horrifying. If it's a bank account, the consequences can be downright devastating. But that's just one person. Yes, it happens to a lot of people, but these are one-offs. Terrible one-offs, and all too common, but one-offs. The damage is awful, but compartmentalized.

But what causes these kinds of painful intrusions to operate at an industrial, criminal scale is that takeover of privileged accounts. In any given organization, plenty of people have enough access to impact many, many other people. Consider all the employees who possess enhanced access so they can manage user accounts, profiles, access rights and roles, security policies (including authentication schemes). This makes these employees powerful. And dangerous. With great power comes great responsibility, and also great risk. These employees include:

- Help desk / call center personnel
- Application administrators
- Database administrators
- Human Resources execs

Much like auto mechanics often neglect their own vehicles, IT and other privileged staff forget that they too are subject to being targeted, for their heightened access. Bad guys can do a lot of damage with the power of those accounts. The gaming industry ransomware attacks of 2023 were accomplished by the takeover of help desk accounts.

Password expirations and other policies need to be in place for these accounts at least as stringently as for regular users. Password sharing is common among such users, since they are performing batch operations.

The corruption of privileged accounts can lead not only to ransomware, but to data breaches and other system disruptions. Spear phishing attacks, targeting corporate higher-ups, have led to takeover of privileged / executive accounts resulting in the theft of highly-valued intellectual property.

> ***"The gaming industry ransomware attacks of 2023 were accomplished by the takeover of help desk accounts"***

We also need to remember service accounts. These are non-human accounts that perform background tasks, running 24x7. Quite often the passwords on these accounts never expire, since admins worry about the interruption of the services these accounts run. Such accounts have unlimited ability to affect operations. Database service accounts execute queries, and therefore often have unfettered access to data stores. Not nearly enough organizations employ policies that limit the scope of service accounts. These limits may not prevent all damage, but by segmenting access, they can keep the damage from being enterprise-wide.

Because they need to help users get or recover access, help desk / call center personnel are also super-powered. But there are many documented instances of the help desk being fooled by social engineering. The famous "hacker" Kevin Mitnick was banned from computer access as part of his probation. But he was primarily a social engineer, presenting himself physically as somebody he was not, in order to gain illicit access.

The help desk can still help. But simply resetting passwords, or unlocking accounts, by hand is not helping. It in fact propagates the mistake.

DEADLY MISTAKE #7 - TYING IDENTITY TO A DEVICE

The premise sounds, well, sound: tie your identity to your device, which presumably cannot be pried out of your hands. The device is simply an extension of the person. You might even use your face, voice, or fingerprint to unlock your phone or laptop, which in turn unlocks your access to various assets, including consumer and employer apps. At certain companies, they even containerize company assets inside the phone, to act like a separate ecosystem within the phone's desktop. How can this go wrong?

"The use of personal devices for work-related activities only exacerbates the situation"

Well, how can it not? Devices sometimes are pried out of people's hands. There are many documented instances of thieves acquiring phone passcodes, which they put to use once they physically steal the device. This allows them to bypass the biometric requirement, and then even install their own biometric into that device for further use.

The use of personal devices for work-related activities only exacerbates the situation, since an individual's personal security posture may put at risk the employer's posture.

From the standpoint of the enterprise, there is absolutely no guarantee that the person holding the device in their hand is the correct person. And once the thief has the device in their possession with full access, nothing prevents them from installing their own biometric signature.

For that matter, the thief may not even need to physically possess the device. Phones are often compromised by SIM swaps, which have plagued the telco industry for many years. Various policies and procedures have been put in place to prevent swaps, but insiders negate even those defenses. In this way, fraudsters don't even have to steal and hold your device; they can simply fake it.

So if passwords are the weak link in such a scheme, physical possession is the weak link in device-based security. And if the other aspects of identity verification can be compromised, then even the possession of a physical key or token, such as a Yubikey, is therefore rendered useless as a factor of security.

Let's talk about those tokens for a minute. For more than two decades, those tokens have been floating around, and in some cases they still have their uses. But they are difficult and expensive to provision and distribute. Organizations struggle to get them back when employees leave or when those tokens must be updated. Of course, they can be stolen.

Users make the mistake of thinking that using their face to unlock their device makes them safe. But facial id is not designed as a safeguard. It's meant as a convenience. And convenience does not equal security.

The inherent concept of device-based security is already suspect, if the whole point is to access assets on the device itself. Even biometric protection, which can be circumvented, may not put the user any further up the food chain than the device itself, which provides little value for accessing apps in the cloud.

In the authentication universe of using what you know and what you have, computers and phones and tokens are things you have. And someone else can have them, or fake having them.

BONUS 1 – EXCESSIVE FRICTION

A cartoon that came out years ago about fraud showed two IT pros discussing how to keep criminals out of their credit card system. Their answer was easy, to deny every single application. No credit cards issued, so no credit card fraud.

Yes, that works, if fraud prevention is your only use case. But keeping bad guys out of the system is only a function of actually getting in the goods. While an extremely locked-down approach may prevent fraud, it can also prevent business. This usually shows up in the form of friction.

Passwordless authentication options are typically less burdened with friction, unless they require hard tokens or authenticator apps that take up just as much time as typing in your spouse's name or your birthday.

> ***"An extremely locked-down approach may prevent fraud, it can also prevent business"***

Once again, we want to reach our plane safely, but also quickly. If it took two hours to get through the average security line, no one would fly. So we need to get people through the line both safely and securely. You can't sacrifice security for convenience, but a lack of convenience will most definitely sacrifice business.

Unless you are trying to physically access nuclear missile silos, you need to provide an experience that doesn't drive potential users away. Prospective customers for just about any online service have lots of options, and can swipe to anything else if your security requirements are so difficult that price of safety is time and/or inconvenience. The mistake is in assuming that customers are so concerned about protecting their accounts that they will jump through hoops to do business with you.

If those security requirements are for employees who have no choice ("If you want to work here, you gotta do this stuff"), there may still be an issue. Difficult identity platforms turn into lack of adoption, unsafe workarounds, and poor adherence to rules. They also result in far more calls to the help desk. So the mistake there is assuming that a captive audience will do as ordered.

BONUS 2 - TYING IDENTITY TO A DEVICE

The premise sounds, well, sound: tie your identity to your device, which presumably cannot be pried out of your hands. The device is simply an extension of the person. You might even use your face, voice, or fingerprint to unlock your phone or laptop, which in turn unlocks your access to various assets, including consumer and employer apps. At certain companies, they even containerize company assets inside the phone, to act like a separate ecosystem within the phone's desktop. How can this go wrong?

> ***"Fraudsters don't even have to steal and hold your device - they can simply fake it"***

Well, how can it not? Devices sometimes are pried out of people's hands. There are many documented instances of thieves acquiring phone passcodes, which they put to use once they physically steal the device. This allows them to bypass the biometric requirement, and then even install their own biometric into that device for further use.

The user of personal devices for work-related activities only exacerbates the situation, since an individual's personal security posture may put at risk the employer's posture.

From the standpoint of the enterprise, there is absolutely no guarantee that the person holding the device in their hand is the correct person. And once the thief has the device in their possession with full access, nothing prevents them from installing their own biometric signature.

For that matter, the thief may not even need to physically possess the device. Phones are often compromised by SIM swaps, which have plagued the telco industry for many years. Various policies and procedures have been put in place to prevent swaps, but insiders negate even those defenses. In this way, fraudsters don't even have to steal and hold your device; they can simply fake it.

So if passwords are the weak link in such a scheme, physical possession is the weak link in device-based security. And if the other aspects of identity verification can be compromised, then even the possession of a physical key or token, such as a Yubikey, is therefore rendered useless as a factor of security.

Let's talk about those tokens for a minute. For more than two decades, those tokens have been floating around, and in some cases they still have their uses. But they are difficult and expensive to provision and distribute. Organizations struggle to get them back when employees leave or when those tokens must be updated. Of course, they can be stolen.

Users make the mistake of thinking that using their face to unlock their device makes them safe. But facial id is not designed as a safeguard. It's meant as a convenience. And convenience does not equal security.

The inherent concept of device-based security is already suspect, if the whole point is to access assets on the device itself. Even biometric protection, which can be circumvented, may not put the user any further up the food chain than the device itself, which provides little value for accessing apps in the cloud.

In the authentication universe of using what you know and what you have, computers and phones and tokens are things you have. And someone else can have them, or fake having them.


HACKED

BONUS 3 – POOR USER TRAINING

It is incumbent on every organization, private or public, to provide training for their users in securely accessing their assets, digital or physical. If passwords are the weak link in the digital landscape, people are just as culpable. Once again, we desire safety, but will often personally do the bare minimum to achieve it.

Once again we invite bad actors into our very midst, with our own bad practices. And those of us who try to do better can still find ourselves the victims of our colleagues' carelessness. Bad actors steal,

How does bad user training result in intrusion by criminals and vandals? The vectors are many, and this requires IT professionals to watch every possible avenue, leveraging the lesson learned long ago by those responsible for missile defense: the defenders must be right all the time, while the attackers only have to be right once. Here are those avenues:

1. Phishing. Users must be perpetually reminded not to click on links in emails. Even if those emails appear to be from a known colleague or other party, they can still be disastrous. A colleague's email can be compromised and used for distributing malware. A common twist on this is the use of domains that resemble trusted domains. For example, a fraudster might register a domain in which a small L is exchanged for the number 1, or a zero for an O. it's easy to miss that during a cursory glance. The victim mistakes the origin for a friendly site and clicks.

   Not examining that actual origin. A seemingly harmless link might point to a hostile place. By simply hovering over the link, the recipient may be able to easily discern the actual place that link would take them. This can done with clickable links or even a sender's email address.

"Once again we invite bad actors into our very midst, with our own bad practices"

2. Reporting suspicious activity. Even when criminal attempts are caught by the recipient, they may not realize that their fellow users are also being targeted. Upon receiving illicit emails or other communications, users should immediately report them to admins, who can tighten up their defenses as well as send out alerts to the entire population to be on the lookout for such attacks.

3. Poor password construction. IT admins can put policies in place to prevent the reuse of passwords, or to prevent the use of a user's name (or variation) as part of the password. But policies won't comb Facebook or other media to see if a user has used their kid's name, pet's name, or other familiar item for that password. Yes, creating new passwords whenever the old expires is a pain. It seems like we are forever having to think up a new one. But it's a very necessary hassle, which is why organizations need to drill this into their users: don't make it easy for the crooks.

4. Password sharing. Yes, this actually happens. As in all the time. Users share their credentials so that someone else can perform a task for them. Certify other users. Book their trips for them. Perform other mundane tasks. A far more orderly approach is to empower task delegation, which is a function of several identity management tools, through which a user can grant temporary

ability for another (and presumably authorized) user to perform a task on their behalf. In the meantime, not only should password sharing be strongly discouraged, violation of such a policy should result in sanctions or reprimands.

5. Manual password resets or account unlocking. How were two multi-multi-multi-million dollar ransomware attacks accomplished in 2023 in the gaming industry? Bad actors farmed social media for enough information on privileged users to allow them to impersonate those users during calls to help desks. They then requested password resets which enabled them to install malware, take control of critical systems, and launch ransomware which encrypted those systems. One victim org paid half the ransom and got back up and running (at the cost of several million) while the other victim refused to pay, and experienced a prolonged outage resulting in over 100 million dollars in losses.

Help desks / call centers must be educated on (or even prevented from) manual resets or unlocks. Rather than hit a few keystrokes and reinstate users, they should do one of two things: either require a highly stringent identity verification, or (better yet) provide helpful links via SMS or email that allow the user to verify their own identity using factors that cannot be gleaned from social media or company website.

The general population should be subject to mandatory security training on the first day of employment of membership, and refreshed on that training on a semi-regular basis, and certainly after any incident. That training should be even more thorough for users with enhanced access. Any company or agency that fails to combat these vulnerabilities through comprehensive user training fails to nurture a culture of security and brings the consequences on themselves, on their employees and customers, and on their brand.

MOST RECENT THREATS: NOT ADDRESSING AI THREATS / DEEPFAKES

The thrill of Artificial Intelligence had barely warmed our hearts when the other side of the coin became the talking point: the threat of deepfakes. As with all human progress, AI has become an exponential presence. Chat bots have been around a long time, frustrating callers who just want to speak to a person that will fix their problem or make their reservation. But as AI has been moving toward a level of advanced progress, it has even been able to make itself better.

AI is being used for finding patterns of behavior that make spotting fraud easier. But at the same time, AI is being used for launching wider and more sophisticated attacks. Phishing, spear phishing, the generation of fake identities, and finding the softest targets can all be performed at an unprecedented scale through AI, which learns from its own mistakes and successes to perpetually sharpen its abilities. IT defenders are always playing catchup.

The most prevalent attack on the horizon, one that is constantly in the news, is deepfakes. These are phenomenally authentic-appearing replicas of humans. The deepfakes which are a product of AI have also gotten better, or, from the standpoint of their victims, worse.

Deepfakes are replicas, or impersonations, of various human traits. Fake ids have also always been around, crafted badly or sometimes not so badly for the sake of getting underage kids into bars. But now a deepfake id doesn't require an Exacto knife and a felt tip pen. Instead, anyone can tell a chatbot to make them a driver's license with a particular uploaded image, some specified data, and a barcode to match on the back. With a cheap laminator off of Amazon, that deepfake id is now perfection.

But that's the easy version of evil AI. It has quickly gotten to the point where anyone's voice can be cloned with only a few seconds of sampling, and replayed over the phone to unsuspecting acquaintances. It's already been used in horrifying fashion, to convince terrified parents that their child screaming over the line has been kidnapped and must be ransomed. Rudimentary facial recognition systems can be fooled by headshots that can be animated from 2D into moving, smiling, blinking, even speaking avatars.

"The most prevalent attack on the horizon, one that is constantly in the news, is deepfakes"

In a now infamous case, in the last several months a poor employee at a Hong Kong office was fooled on a Zoom call when all the other participants turned out to be deep-faked video avatars of colleagues, who instructed him to send millions of dollars to a nefarious recipient.

Boxers train in the ring with sparring partners to hone their skills. Deepfakes work the same way. Generative Adversarial Networks, or GANs, generate deepfakes that are immediately tested for detection. In assort of Darwinian model, the best fakes survive. By creating its own opponents, AI trains itself to be increasingly good at fooling defenses.

Deepfakes come at us in two basic vectors. The first is presentation. Simply enough, a deepfake voice, face, and/or ID is presented to a camera or sensor, trying to dupe its way in. When it looks like that initial defense can stop such an attack, fraudsters can resort to injection attacks, in which the fake is inserted behind the camera, somewhere along the network, much like a classic man-in-the-middle attack.

So the current state of deepfake defenses represent a double-whammy mistake. First, organizations make the assumption that their basic facial recognition product is sufficient to catch a deepfake. There are various signatures to a deepfake, but some of them are infuriatingly difficult to detect. When the face and voice are familiar, it can even fool an acquaintance. Only systems that are specifically trained to discern a deepfake from a legit presence will keep their hosts safe.

The second mistake is neglecting injection attacks. If you can't tell that the image, voice or other signal arriving at the back end has originated from the authorized starting point, then it's going to bypass the front-end defenses. Once again, missile defense has to be right every time, while the bad guys only have to be right once. It's almost like a workflow: if one defense holds, the fraudsters go around it.


Username
****

HEED THE CALL TO ACTION

So when it comes to authentication, we have discussed how we typically use what we know (passwords, security questions) and what we have (devices or hard tokens). Somebody else can learn what we know, and possess what we have. They can be us. It's a mistake to rely solely on traditional defenses when thieves are getting smarter, Artificial Intelligence is getting better, and our own infrastructures can't keep up.

Just as we hurt ourselves by relying on passwords and other outdated modes of self-assertion, we do ourselves a disservice by depending on defenses that struggle to keep up with an ever-evolving set of threats. Far too many companies and agencies still-still-still rely on simple username and password combination to identify users. We are practically begging for the onslaught of fraud to mow us down. Miring ourselves in these traditional approaches is the overall mistake we make. This is optimism masquerading as security.

Employing more than one factor is a good thing. But if the root of the entire chain is still something easily compromised, such as a password or the physical possession of a device, then the whole thing is a house of cards. The mistake there is building a seemingly strong structure with a weak link that threatens the entire ecosystem.

What is the solution? Making the assertion of identity something that is non-repudiable. What's better than what you know and what you have? Who you are.

Biometrics are still a great way to go, since you've always got your biometrics with you. One could say that your biometric signatures can be stolen as well, and that is accurate. Fraudsters can even take a still shot of you and animate it. So the trick is for an identity platform to ensure that upon presentation, your biometrics can be verified as being presented by you, and no one else.

"Facial biometrics are the absolute best option for deterministic verification of online identity"

As previously stated, voice is all too easy to fake. The most sophisticated deepfake voices cannot be tested for liveness, meaning market solutions aren't able to tell whether a real person is speaking. Fingerprint is no longer supported on the most ubiquitous personal device platforms available, so this option leaves out a large portion of the population, at least in terms of using personal devices.

Therefore, facial biometrics are the absolute best option for deterministic verification of online identity.

Facial biometrics can be part of a chain of authentication methods, but that chain cannot rely on a password or other weak link that can compromise this defense. In addition, the platform cannot allow biometric evaluation to be bypassed as with an injection attack, nor can it be used only as a fallback. A password cannot be used as the key to resetting a registered biometric, meaning using simple login as the path to putting in a new face.

If the help desk is contacted for a password reset or account unlock, they can send a link, via email or SMS, for a user to biometrically authenticate. But they should not manually reset or unlock anything. Instead, they are helping the user reassert themselves.

We have discussed deepfakes. That appears to be the hole in this thinking, right? The deepfake may be substituted for the real user. But the answer there is, don't use traditional facial recognition. A facial biometric solution must be trained to recognize deepfakes, up front and in the network chain.

As technology continues to evolve to help us solve our most vexing problems, it also solves problems for criminals, such as how to impersonate real people. How to enrich themselves by stealing your stuff. How to break into corporate systems. How to hold critical operations for ransom. How to make our lives more difficult.

If traditional methods for stopping these intrusions worked infallibly, rampant fraud wouldn't be all over the nightly news. Twenty-two percent of Americans would not have been affected by fraud in 2023 alone.

Onerous products that cause undue friction only add to the unhappiness that comes with using them. It's not even a guarantee that a tougher process is a safer one.

Tried and true might work when you're learning how to cook, learning calculus, learning how to play an instrument. But when you're trying to keep your digital assets safe in a world where the bad guys are working diligently to stay five steps ahead of the processes meant to detect them, tried and true must give way to forward-thinking solutions. Traditional defenses won't beat the progress of evil.

Don't make that mistake. ❖

To learn more about safeguarding your organization, contact authID for a discussion, a demo, a deep dive. We're a team of long-time identity and security experts, and happy to help.