Are we witnessing the death of the password?

December 2 2023, by Nikki Davidson, Government Technology

Credit: CC0 Public Domain

Once considered a near iron-clad weapon of defense against cyber criminals, the password has begun to fall from grace.

Effective passwords often require human efforts that many users can't or simply won't take the time to make. Many organizations have adapted

new security tools that make accounts and sensitive information harder to penetrate using emerging tech with a combination of factors.

Are passwords outdated? Government Technology surveyed a range of cybersecurity experts to find out if the password has outlived its relevance.

Do you think the password is dead?

Mark Weatherford: "If you would have asked me this question 15 years ago, I would have said, 'Yeah, passwords are on the way out.' If you would have asked me this question 10 years ago, I would have said. 'Yes, it's definitely on its last legs.' If you would have asked me this question five years ago, I would have said, 'Any day now.'

Mark Weatherford is chief strategy officer at the National Cybersecurity Center.

"But now I feel like no, passwords aren't dead. We're always going to have passwords. I think we're going to have complementary authentication systems, but in many cases the passwords are going to be there."

Omar Sandoval: "I don't think it's dead, I think it's here to stay. I think it's the most simplistic way to give end users access to the resources that they need. In that same vein, because it is simplistic, that's why it's such a danger. More and more, you're going to be asked to make more complex passwords that have different characters and all these things. I also think their time to stay alive is going to shorten.

"One of the reasons why it's dangerous but still here to stay is that it creates a simplistic way for everyone to access what they need to, but we make the mistake of using the same password for everything."

Kelly Moan: "The password is on its last legs. It's inherently insecure because it's often too weak, too short or not rotated enough."

John Evans: "It probably should be, but it's not dead yet. We still have a lot of legacy systems, systems that probably can't handle the integrations that would be needed to move toward something passwordless. ... Some of them will probably be a while until we can fully get some of those types of systems to go passwordless. Any new system that's being developed, they should probably be looking at things like passkeys or risk-based authentication and not using passwords."

Dan Lohrmann: "I think the password is dying a slow death, but it is not dead yet. There are still far too many applications out there where passwords are used. But slowly but surely, for bank accounts, financial institutions and more sensitive data, the password is going away."

Valecia Stocchetti: "Is something ever really gone? I still use my old iPhone and iPad. But I think for passwords, they provide strong user authentication, they help keep attackers out of the system. They're still used in a lot of different frameworks and standards so I think that speaks a little bit to the idea that the cybersecurity community is not ready to shift as a whole. But even the strongest password does require other protections to be in place to be the most effective."

Are there any instances where passwords will always be the most secure option?

Weatherford: "In some cases where organizations don't have a lot of resources to apply some of the more complex alternatives like biometrics or hardware tokens, passwords may be fine for that. I've seen this firsthand where we tried to increase password security on old legacy systems and it wouldn't let you create a password longer than seven

characters. So I think there are some instances where passwords are just going to continue to be a logical option. Maybe not the most secure, but a logical option."

Sandoval: "I don't think so. Even now, things like multifactor authentication (MFA) are getting bypassed because once you're able to get into a system, you're in. I could generate a device, tie it to a person's account and then I will get their authentication. The password will never be the only tool in the toolset."

Moan: "There's always going to be edge use cases that may fit for passwords being the most secure option, but largely that's dependent on their length, complexity and the use case itself."

Evans: "I can't think of anywhere that passwords are the most secure option, but they may be a necessary option. A lot of systems may not be able to handle the integrations that are needed for things like password lists, passkeys. I can't think of any instance where it's a necessary, but unlikely, most secure option."

Lohrmann: "I can't think of any instances where it's the most secure option, but there are still many instances where it's the only option. Having a password is better than having no password. If it's multifactor, even though they steal the password they can't get in because they don't have that second factor."

Stocchetti: "I think maybe not necessarily the most secure, but the most practical. There are certain instances that require dependencies on people having newer devices and that may not be accessible for all. For newer authentication methods, we require access to one or more smart devices. The challenge comes for those who maybe can't afford a smart device or don't have access to newer technologies, or the underserved who share devices with friends or family."

Will we still be using traditional passwords five years from now?

Weatherford: "Yes, we're going to continue to use traditional passwords with other compensating controls as part of that password. MFA has become fairly mainstream now and it's a perfectly logical and legitimate additional control for passwords."

Moan: "A much smaller percentage of user accounts will use traditional passwords. They'll likely be replaced with passwordless sign-on and passkeys that provide a more seamless user experience."

Sandoval: "The password is just going to continue to be the entry point, it's something that people are used to. The password is the screen door, you can open the screen door, it may or may not be locked, but then you get to the door and you're going to need the actual key. Is that the equivalent of MFA? Is that zero trust in authenticated and verified devices?"

Evans: "It depends on the person probably in a lot of cases. For many, most people, they might see a complete replacement for passwords within the next five years. But in the government space, passwords are going to hang around for a lot longer. ... For the majority of individuals, people who do mostly things like secure online transactions, like e-commerce or health care, I'd be surprised to see any of those still using passwords in five years."

Lohrmann: "Yes, I think more and more there will be options not to use passwords and people that choose not to do business with insecure accounts. Some people will, many people will not. Will we still have passwords for our Wi-Fi accounts in our homes, for example?"

Stocchetti: "I think it depends on the adoption rate of those alternative authentication methods for passwords. Major players like Microsoft, Google, Amazon Web Services, of course, are already adopting a lot of these technologies or they're planning on moving to more secure methods. But smaller companies may take longer to adapt. If there's some kind of regulatory law passed that's required at the state or federal level, then that's different. If there were some kind of regulation that came down, that would probably be the quickest adoption away from traditional passwords. It's much quicker when there's some kind of fine or legal obligation to do that, versus it's a more secure thing to do and we should just do it. Kind of like wearing a seat belt. Passwords have been around for many, many years so we're talking about a huge shift in behavior from the user perspective."

What are the most promising alternatives to the password?

Weatherford: "MFA really has helped a lot, it's changed a lot. Biometrics are getting better and better, everything from fingerprints and facial recognition, iris scans, voice recognition, even things like basic behavioral patterns like typing speed. I think biometrics can really be good, but the problem is they're very complex. There are hardware tokens and smart cards. I think we're going to see some blockchain-based authentication, blockchain has a lot of promise. There are some pretty darn good alternatives out there, where it makes sense to do it.

"For overall use, MFA stands out because now it's mature. It's getting better and better. Sometimes it's kind of annoying, you have to get a text message with a six-digit code and you have 120 seconds to put this code in to authenticate. That's pretty good, it's pretty effective."

Moan: "Passkeys, hardware tokens and software tokens."

Sandoval: "With AI, you can have a machine learning system that shows, 'Hey, this account has had so many unsuccessful attempts,' and then it'll automatically block you. I don't know that there's an end-all-be-all because the bad guys are always going to be on the leading edge, they probably have figured out a way to use AI to capture all our passwords without us even knowing it.

"Microsoft is getting ready to release AI security agents into their ecosystem. I think more and more companies are going to do that to be able to do things a little bit more real time. The speed of catching that is going to increase, which may lower the rates of compromises with passwords."

Evans: "Passkeys, physical devices or cryptographic keys that are installed and embedded in your device, and then requiring biometrics to log into that device. Risk-based authentication, I'll add that into the list of some promising alternatives. Setting it up on behalf of the organization that's managing the accounts to understand what more risky or more sensitive transactions look like. It ties into the zero-trust model.

"If you wanted to get online, look at your water bill, maybe you don't need the same level of scrutiny making sure you are who you say you are as when you're trying to access your bank account and make a $50,000 transfer. It's risk-based authentication, depending on the criticality of the systems that are attempting to be accessed, or the type of transaction that's trying to be performed. If it's a more sensitive or critical transaction, I'd probably want to have greater levels of assurance that the person is who they say they are."

Lohrmann: "MFA, or one-time passwords. A one-time password might be eight digits, it might be a mix of lowercases and you'll cut and paste that and many times it is timed as well. Biometrics, like a fingerprint scan, facial recognition, retinal scans and those kinds of things. Shared

secrets are also still very popular. People are also using all sorts of new alternatives to CAPTCHA."

Stocchetti: "One-time passwords because they reduce your need for IT support, they are harder to guess. They're easy for organizations to adapt to. Biometrics, which are fingerprint-based scans, retina scans, adaptive or behavioral authentication. Passkeys, they're similar to a one-time password where the prompt is sent to a device owned by the user, that allows them to log in using a PIN or fingerprint or face scan. The benefits of this is that they obviously reduce human error such as weak passwords or reused passwords. There's also behavioral authentication, which uses machine learning to develop those typical behavior patterns, learning over time to know when you're typically logging on, where you're logging on from, and then it can block access until identity can be verified. Users can also convert their USB stick into a password to restrict access to only those who have the USB."

What concerns do you have about those password alternatives?

Weatherford: "Probably the biggest concern I have with new password alternatives is around privacy. Certainly with biometrics we have huge privacy concerns, once you give somebody your fingerprints, iris, facial scans, that data is digitized somewhere. That data has to be protected. The cost also, the cost of doing this. Hardware tokens can be lost. MFA I don't really have any concerns, except some people think it's too much of a pain to have to do MFA. ... Generative AI can generate so much really sensitive information, just by asking the right kind of questions, so there's also going to be authentication issues associated with generative AI."

Moan: "There are always security considerations for access control and

account access. That will continue to be true in five years when alternatives likely become outdated, as technology continues to advance at a rapid pace."

Sandoval: "Accessibility and inclusivity are concerns of mine. Some may argue that MFA is the way to go, or zero trust is the way to go. That requires someone to interface with the system. The assumption is made that people have more than one device to authenticate or are willing to utilize more than one device."

Evans: "There's no security control that is a silver bullet. Everything has to be thought of and applied through the lens of security and depth strategy. Zero-trust methodology would be just one part of a framework. Using risk-based authentication, you'll have to make sure that you're looking at the right attributes and tuning your systems accordingly. Things like one-time passwords could be intercepted by malware.

"You can't just think of it as, 'Oh, I have the technology in place, I'm good to go.' It requires thoughtfulness and work on the behalf of the organization to make sure that everything's operating the way that it should.

"People are reluctant to change, people know their passwords, they trust their passwords. Even though password lists are more secure, it still is a change that not everyone feels comfortable with initially. So you have to be able to articulate to them why it's better.

"There's a cost for technology, in the case of this one there could be a significant cost for some, especially if you have to do things like refactor their application to make it support the passwordless option."

Lohrmann: "It's kind of an arms race. Now passwords are the low-hanging fruit, and they're easy. There's different ways cyber criminals

can defeat passwords, on the dark web there are databases full of usernames and passwords. As more and more of the sensitive accounts like bank accounts, administration accounts move to multifactor and get more sophisticated, more and more techniques will be used to defeat them. Hackers can train generative AI to do things like copy my voice, and while voice recognition is a step up from the password, it could also be potentially defeated. So with all of these alternatives, there's no perfect solution to this problem. Security issues are not going away in the next decade. When we eliminate passwords, we will have security issues with the alternatives.

"One-time passwords, if the user loses a secondary device, in that case it's hard. It becomes more difficult to reset the device and get the password you need. Biometrics track data and keep a record of your fingerprint, your facial scan and those are things that can't be changed. You can reset a password, but you can't reset your fingerprint. There's also higher-level privacy issues with it as well."

Stocchetti: "Passkeys, the drawback is you lose that secondary device, it's got the same problems as a one-time password. If you use a USB stick, if you lose the USB then what happens? ... Society is a little slower to adopt certain technologies, we are just major creatures of habit, right? They like what they like, what is comfortable to them is what they want."