When Common Authentication Methods Fail to Protect Your Identity

Recently published identity theft statistics paint a sobering picture. For instance, in the United States, identity theft rates have climbed twice as high as the global average. Every two seconds sees a new victim of identity theft, and standard authentication methods may not provide enough protection.

No One Immune to Identity Theft

Despite vigilant security habits, a small business owner recently discovered that thieves had stolen his identity. He enrolled in LifeLock but continued to experience problems that even interrupted his ability to do business effectively.

Finally, he realized that the thieves had hijacked his smartphone. As a result, authentication texts that should have gone to him actually went to the thieves instead. The multi-factor authentication (MFA) methods meant to protect him and his business proved insufficient.

Unfortunately, this scenario plays out over and over again with victims from all walks of life. Even security-savvy individuals who use MFA find themselves plagued by hackers with sophisticated technology at their disposal. To protect yourself, take a few minutes to review your cybersecurity practices and find areas for improvement.

The following authentication practices will help as you work to keep your identity and sensitive data secure from unauthorized access.

Strengthen Passwords

You already know to use a mixture of uppercase and lowercase letters for your passwords. And you know to include symbols, as well as make your passwords long, random, and unique. Consider making your passwords even more secure by using a password manager, increasing the length to 22 characters, and avoiding common symbols like exclamation marks.

Protect Phone from SIM-jacking

Hackers can hijack phones in various ways. For instance, a text message that appears to come from a trustworthy source may actually download a malicious app that gives hackers access to the device. Once they have access, they have eyes on all the one-time passcodes (OTPs) sent to your phone number. This allows them to break into social media, bank accounts and more.

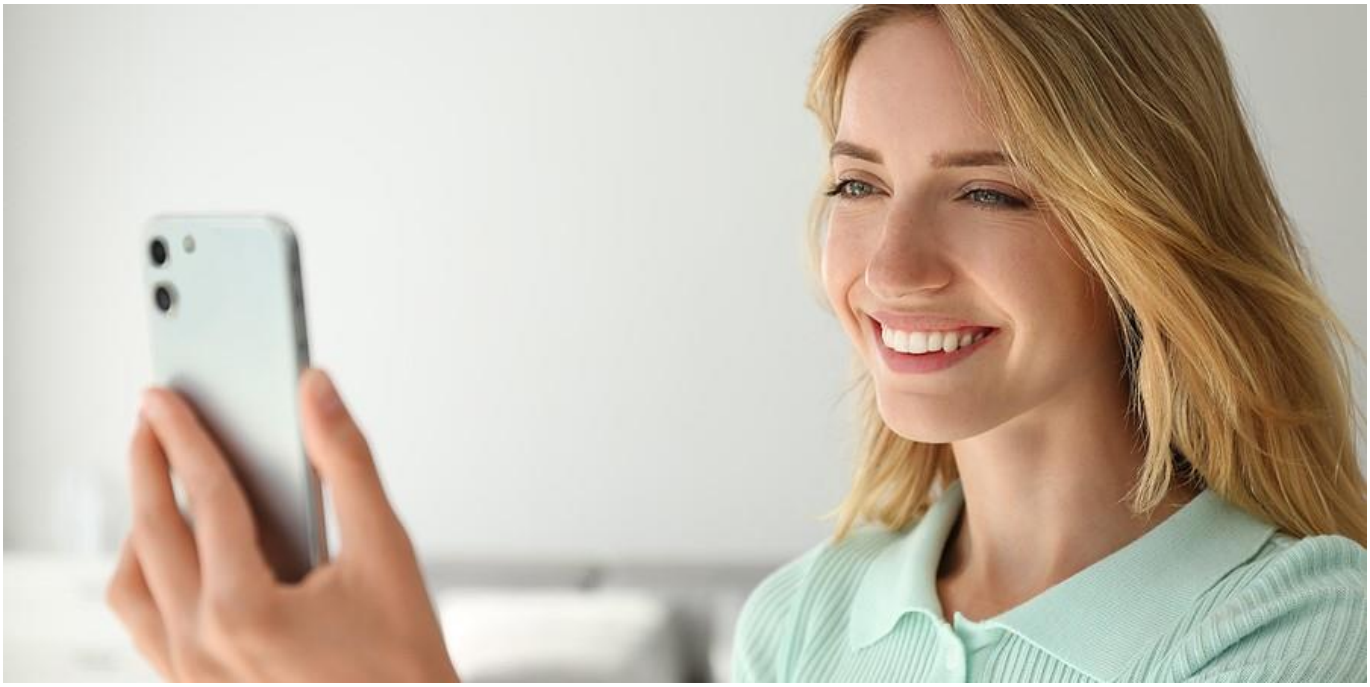
To protect yourself, avoid using texted OTPs when possible. Additionally, you can use a password manager or apply PINS to accounts that allow them. If an account has a security PIN, anyone trying to make a change to the account online will have to enter that PIN first. And, of course, use antivirus software and be careful about downloading apps or clicking links.

Use a Virtual Number

For additional protection, give your real phone number only to a few trusted individuals. Use a virtual number for everything else. Various services, such as Digits and Google Voice, allow users to set up a virtual number. The virtual number can forward directly to your phone or connect to your email.

Employ Biometrics

Biometric authentication involves verifying identity using biological characteristics. For instance, many smartphone users gain access to their phones through facial recognition or a fingerprint. Other examples include retina scans, palm scans and behavioral characteristics, such as keystrokes. MFA that includes biometrics offers exceptional security.



Use an Authentication App

Authentication apps, such as Microsoft Authenticator, allow users to bypass SMS-based MFA. Instead of a text message, users get the necessary verification code from the authentication app. These apps generate new codes every 30 seconds or so and can be used with any account that allows MFA.

Move Beyond Common Authentication Methods

Financial losses related to identity theft rose to $2.6 billion in 2019 alone. And cybercriminals have upped the ante with increasingly sophisticated attacks, including account takeovers. Furthermore, when hackers steal individual identities, those identities can potentially deliver access to corporate data.

The cybersecurity experts at Messaging Architects can help your organization build a comprehensive cybersecurity program including multiple layers of defense. From detailed risk assessments to dark web scanning, encryption, data loss prevention and more, we help you keep identities and data safe.