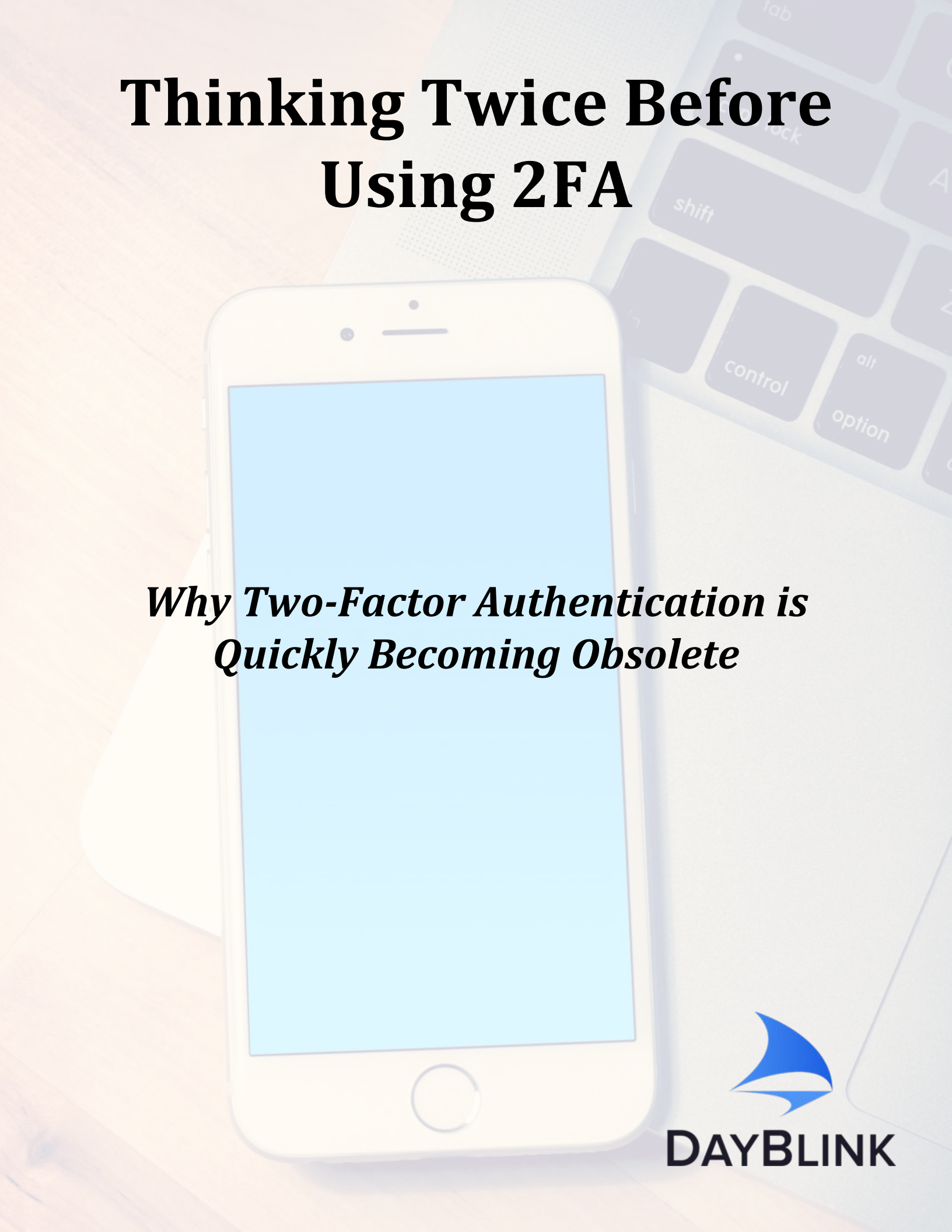
Thinking Twice Before Using 2FA



Why Two-Factor Authentication is Quickly Becoming Obsolete

DAYBLINK

What is 2 Factor Authentication?

2 Factor Authentication (2FA), a form of Multi-factor Authentication (MFA) or Multi-Step Verification, adds another layer of security, supplementing the username and password model with a code that only a specific user has access to (typically sent to something they have immediately to hand). It has quickly become one of the most valueable security practices a user can implement. This authentication method can be easily summed up as a combination of "something you have and something you know".

In 2018, MarketWatch estimated that the multifactor authentication market is roughly $6.3 Billion and is expected to reach $16.8 Billion by 2024, a CAGR of 18%*. The growth of the market is driven by various factors such as an increase in data breaches and cyber-attacks, stringent regulation, and the growing pressure of data security compliances and the growing adoption of bring your own devices (BYODs) among enterprises. Many security practitioners have viewed it as an easy panacea in solving many extremely challenging problems. However, cost and technical complexity in implementing MFA and increase in MFA use/service time are expected to inhibit the market growth for a short period of time. The continued worldwide concern with digital security will allow the market to grow, but how will security companies adapt when 2FA becomes obsolete?

In 2012, 2FA became the be-all and end-all for security by replacing the simple username and password combination. Multiple methods of 2FA became commonplace for logging into secure accounts, some more successful in securing personal information than others*.

Forms of 2 Factor Authentication

Physical Key | *App Code* | *SMS Verification* | *App Authentication* | *Email-Based* | *Recovery Code*

Sunny Day Scenario

The most secure form of 2FA is a hardware token. The most popular is Yubikey, who supplies keys for Google, Facebook, and a many of other major service providers. Thanks to the Fast ID Online (FIDO2) spec, keys can't be spoofed even if used in the incorrect computer.

Cloudy Day Scenario

If you don't want to shell out for a security key, your best bet is a dedicated app like Authy or Google Authenticator. Apps are prone to account reset issues, but they are an easy way to implement 2FA services easily.

Rainy Day Scenario

SMS has been at the center of many hacks, including breaches for common sites such as Reddit. High-security accounts are already moving away from these services, but a frightening number of enterprises maintain thes options, providing easy access to carrier hackers.

https://www.marketwatch.com/press-release/at-18-cagr-multi-factor-authentication-market-size-is-expected-to-exhibit-16800-million-usd-by-2024-2019-03-13;
https://www.digitaltrends.com/computing/why-2-factor-security-is-flawed/

What's the Problem?

2 Factor Authentication has become an archaic practice. In 2016, the National Institute of Standards and Technology (NIST) began the process of deprecating the use of SMS-based out-of-band authentication. NIST stated the following:

> *"The use of SMS to deliver one-time-codes and passwords does not meet these criteria as SMS messages can be intercepted in the network or by malware that has infected a person's mobile device. SMS is not a secure messaging system and can also not be 100% relied on in terms of delivery."*

If you can compromise the mobile carrier accounts from providers such as AT&T, Verizon or T-Mobile that support a person's phone number, you can hijack any communication, call or text, that's sent to them. In addition, SMS is not just vulnerable to interception, the codes themselves often can be seen on the lock screen of users' phones. This makes any one-time SMS code less than ideal for authentication. Some mobile apps that are tied entirely to a given phone number can provide enough information to hijack the whole account At the same time, carriers have been among the slowest to adopt two-factor, with most preferring easily bypassed PINs or even flimsier security questions. With only a few networks controlling the bulk of the market, there's been little incentive to compete on security.

What Can Go Wrong?

In February, the Cerberus baking hack was observed stealing one-time authentication passwords from the Google Authenticator App to gain access to banking user accounts. The module obtains the codes by abusing an Android device's accessibility privileges. This allows the hacker to view the content of the app while it is in operation, and exfiltrate codes to a command and control server. If a threat actor has already obtained a potential targets login credentials to the designated device or applications, the Cerberus tool would allow the intruder to gain access to an account when Google Authenticator requires a one-time password. Google Authenticator passwords expire after 30 seconds, leading experts to believe that this component of the tools is designed for automated attached with built-in target credentials.

The latest Cerberus module points to a trend of the past year: threat actors targeting 2FA messages. While there is no doubt 2FA reduces the risk for potential targets and fraudulent logins, this trend has made it clear that 2FA does not guarantee security in the login process. While the trend is relatively recent, it is preceded by a variety of tactics and attack vectors that were already being used to skirt or manipulate the 2FA process.

Recent Operations Targeting MFA Codes*

Timeline	Attack Technique	Incident Summary
Feb 2020	Stolen 2FA Codes	*Cerberus, a type of Android-based malware, was found to have stolen 2FA codes for Google Authenticator*
Dec 2019	Unauthorized Access	*A Chinese threat group generated OTPs to bypass MFA after compromising RSA SecurID systems and harvesting users' SecurID Tokens*
Jun 2019	Notification Interception	*A malicious app stole OTPs from email and SMS messages by capturing a code from a notification displayed on the infected device*
Jul 2019	Device Impersonation	*The Pegasus spyware bypassed MFA by cloning service authentication keys and impersonating devices*
Jan 2019	Credential Harvesting, SMS Interception	*The "CookieMiner" malware bypassed MFA by exfiltrating login credentials and SMS text messages*
Jan 2019	Credential Harvesting	*A security researcher created a penetration testing tool that bypassed MFA by harvesting credentials and using a reverse proxy*
Jan 2019	SMS Message Interception	*Unknown threat actors diverted and captured users' texts that contained MFA codes by exploiting flaws in the SMS SS7 protocol*

Use Case – Google Security Keys

Google has successfully avoided a phish on any of its 85,000+ employee accounts since initiating the use of security keys in 2017. Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication.

Security Key implements a form of multi-factor authentication known as Universal 2nd Factor (U2F), which allows the user to complete the login process simply by inserting the USB device and pressing a button on the device. The key works without the need for any special software drivers. Once the device is enrolled for a website, the user no longer needs to enter a password at the given site.

The U2F protocol is an open source form of authentication that currently has many high-profile sites on board such as Facebook, Github, and Dropbox. More sites soon will begin incorporating the Web Authentication API (WebAuthn) setup by the World Wide Web Consortium. The WebAuthn protocol is significant because it eliminates the need for users to constantly type in passwords, which negates the threat from common password-stealing methods like phishing and man-in-the-middle attacks.

https://resources.digitalshadows.com/digitalshadows/weekly-intelligence-summary-06-mar-2020; https://www.computerweekly.com/news/252481189/Two-factor-authentication-is-broken-What-comes-next

To heighten the bar even further, Google also offers Advanced Protection as its most secure method of account safety. Advanced Protection requires one USB-based key for desktop computers and another Bluetooth key for mobile devices without a USB port. Together they represent the fundamental security premise of Advanced Protection: that no one can log into your account without one of those two physical devices in their possession. Advanced Protection promises 3 things:

1. **Physical Security Key**: Signing into your account requires a U2F security key, preventing other people (even with access to your password) from logging into your account.
2. **Limit Data Access and Sharing**: Enabling this feature allows only Google apps to get access to your account for now, though other trusted apps will be added over time.
3. **Blocking Fraudulent Account Access**: If you lose your U2F security key, the account recovery process will involve additional steps, "including additional reviews and requests for more details about why you've lost access to your account" to prevent fraudulent account access.

How can we Improve?

It is important to note that 2FA is better than nothing, but there are certainly ways we can improve to more securely protect our data. The focus must shift to threat detection, drawing on dozens of ambient signals like device fingerprinting and on-page behavior to determine whether a given login requires extra scrutiny. A suspicious enough string of logins might trigger an account freeze or require a phone call to customer service before the subject can proceed. One-size-fits-all solutions will no longer be successful due to the advancement of complex hacks. The detection vs. prevention model is destined to be more successful in the long run.

That shift leaves users in a difficult place. “Use two-factor” is still good advice, but it’s not enough. What do you tell someone who is rightfully worried about seeing the contents of their inbox published in the next big data breach? There is no simple fix for such a threat, no one step that will keep you protected. The surprising thing is that, for a few years, it seemed like there might have been. So what is next? Here are a few methods that may be more successful in the near future.

Next Generation Authentication Methods

BROWSER AND SYSTEM FINGERPRINTING

Fingerprinting involves techniques by which a server collects info about a device's software and/or hardware configuration for the purpose of identification. Web services can mitigate insecure passwords by using server-side intelligence in the authentication process with "multidimensional" authentication.

CONTINUOUS CONTEXTUAL AUTHENTICATION

Geolocation allows access via the user's location using their mobile phone, verifying that the user is in the same physical space in which a transaction/login is being requested. In this case, there is no need for the customer to respond to a notification, creating a more transparent and frictionless authentication experience.

CONTINUOUS BEHAVIORAL AUTHENTICATION

By tracking actions such as keystroke patterns (e.g. how long it takes to find the right key or how long keys are held) and building a unique behavior-based profile, the technology can automatically and continuously check to see if a device is overtaken. If the pattern is irregular, the non-authenticated user will get locked out of the device or Web application.

PASSWORDLESS ACCESS

With a known device, users can log into a platform by simply scanning a code with their phone's camera, avoiding the need to input a password. In addition to providing an enhanced user experience, this has the potential to reduce successful phishing attacks. As passwords become less relevant to authentication, phishers will no longer significantly benefit from obtaining end-user credentials.

BIOMETRIC INTEGRATION

Combines the unique factors of biometric security (iris scan, fingerprint, facial detection, voice recognition, etc.) with the secondary pin login of 2FA to ensure advanced protection of personal data.

ABOUT THE AUTHORS

Harry Baker, is a Senior Consultant within DayBlink's Cybersecurity Center of Excellence

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence and is based in Boston, Massachusetts

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cybersecurity@dayblink.com
Call: 1 (866) 281-4403