TRUTHSIFT ANALYSIS

BEST AUTHENTICATION METHOD FOR SECURITY

Analyse which authentication method is best for security. We provide a breakup of different met hods, where each method can be discussed through its own graph.

EACH LIKELY SKILL REPRESENTED BY A TRUTHSIFT GRAPH

1. Password-Only - 8 nodes
2. Time-Based One-Time Password (TOTP) MFA - 10 nodes
3. Passkeys - 10 nodes

PARTICIPANTS

There were 16 participants

PROBABILITY LIKELIHOOD

Scoring Parameter(s):

1. Security
2. Ease of Use
3. Setup Complexity
4. Device Compatibility
5. Recovery Options

GRAPH	SCORE
1. Password-Only	75%
2. Time-Based One-Time Password (TOTP) MFA	70%
3. Passkeys	68%

GRAPH SNAPSHOT

Password-Only

https://app.truthsift.com/spectate/placeholder/494/17

Please generate a print from the graph page

GRAPH SNAPSHOT

Time-Based One-Time Password (TOTP) MFA

https://app.truthsift.com/spectate/placeholder/495/17

Please generate a print from the graph page

GRAPH SNAPSHOT

Passkeys

https://app.truthsift.com/spectate/placeholder/496/17

Please generate a print from the graph page

OVERALL VERDICT

"Biometric Authentication - 80%
Security Questions - 60%
SMS-based MFA - 65%

Based on the scores, we can analyze the design skills that are most likely to be taken over by AI.

1. Password-Only: With a high security score of 75%, this method is relatively secure but lacks ease of use and recovery options. AI could potentially streamline the password management process, making it easier for users to create and manage passwords.

2. Time-Based One-Time Password (TOTP) MFA: Scoring 70% in security, TOTP is a step up from password-only methods. However, it still requires user interaction, which could be automated by AI to enhance user experience and reduce friction.

3. Passkeys: With a security score of 68%, passkeys are a modern approach to authentication. AI could assist in managing and generating passkeys, making the process more user-friendly and secure.

4. Biometric Authentication: Scoring the highest at 80% for security, biometric authentication is already a sophisticated method. AI can further enhance this by improving recognition algorithms and making the process faster and more reliable.

5. Security Questions: With a lower security score of 60%, security questions are less secure and more vulnerable to social engineering attacks. AI could potentially replace this method entirely with more secure alternatives.

6. SMS-based MFA: Scoring 65% in security, SMS-based MFA is better than security questions but still has vulnerabilities. AI could help in creating more secure and reliable multi-factor authentication methods that do not rely on SMS.

In conclusion, the design skills most likely to be taken over by AI are those with lower security scores and higher potential for automation. Security questions are the most likely to be replaced, followed by SMS-based MFA. Password-only methods and TOTP could also see significant improvements through AI, while biometric authentication may be enhanced but is less likely to be fully taken over due to its already high security level. AI's role will",