

User authentication levels

		Blocks Basic Phishing	Blocks SIM Swapping	Blocks MFA Fatigue	Blocks Social Engineering phishing	Blocks AiTM attacks	Is called Phishing resistant MFA ?
1	Passwords(PWD) (whatever the complexity is...)						
2	PWD + MFA (Email) OTP number						
3	PWD + MFA (sms/voice) Accept/Deny or Enter your PIN						
4	PWD + MFA (sms/voice) OTP number						
5	PWD + MFA (App) Accept/Deny or Pick the right number or Enter your PIN						
6	PWD + MFA (App) OTP number						
7	PWD + Conditional Access(CA) + MFA (sms/voice) OTP number						
8	PWD + CA + MFA (App) OTP number						
9	Passwordless with Authenticator Phone Sign In						
10	PWD + CA including Managed Device(MD) + any MFA (App OTP preferred (AOTPP))						
11	PWD + CA including trusted Ips(TIP) + any MFA (AOTPP)						
12	PWD + CA including "Token Binding"(CAE) + any MFA (AOTPP)						
13	CA including MD or TIP or CAE + Passwordless with Authenticator Phone Sign In						
14	Passwordless with Fido 2 (Fingerprint, PIN)						
15	Passwordless with Certificate based Authentication(CBA based on X509)						
16	Passwordless with Windows Hello for Business (WH4B based on TPM)						

Legend:

Nope, you are at risk with these attacks.

Yes, you are protected from those attacks.

Yes, these can be called and accepted as **Phishing Resistant MFA under conditions**: search for: "Memo 22-09 multifactor authentication requirements overview - Microsoft [Entra](#) | Microsoft [Learn](#)" as an example.