Phishable vs Unphishable MFA Factors

The US government is now pushing all organizations to use phishing-resistant multi-factor authentication (MFA). And for good reason! As phishing attacks continue to grow, finding a MFA solution that is unphishable is growing in importance.

Given the increasing complexity of phishing attacks, it can be hard to keep up with what factors are phishable and which are not. Luckily, we put together a helpful chart. The main takeaway is that anything that is stored outside the device (a password) or ever is in transit (like a text message) can be phished, whereas things that never leave the device (cryptographic keys) or your body (biometrics) can not.

Review the table to learn what factors used in MFA will protect you from a phishing attack and what factors leave your systems and applications vulnerable.

Phishable Factors	Unphishable factors
Time-based one-time passwords	Biometrics
SMS text messages	Cryptographic security keys
Push notifications	Device-level security checks
Magic links	Hardware security keys
Passwords	
Security questions	

Beyond Identity provides passwordless, unphishable MFA that not only protects you from phishing attacks but from all password-based attacks. Our MFA only uses secure, phishing-resistant factors that protects your critical data and resources from threats.

GET A DEMO

beyondidentity.com | info@beyondidentity.com