# Winning the fight against cybercriminals in State, Local, Tribal and Territorial Government

Phishing-resistant MFA is key to defeating modern cyber threats and ensuring compliance to cyber insurance

## Cyber pressure keeps growing

With a combination of new federal regulations and tougher scrutiny from cyber insurance providers, state, local, tribal and territorial government agencies face massive pressure to create and execute the most modern cybersecurity strategies. At the same time, agencies are under constant cyber attack with phishing and ransomware on the rise.

**69%** the rate of ransomware attacks in state and local government increased from 58% to 69% year over year
Source

**30%** due to compromised credentials, one of the two most common root causes
Source

**25%** quarter of attacks were initiated via email-based attacks (malicious emails or phishing)
Source

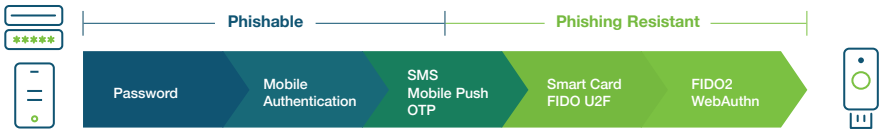
## Not all MFA is created equal

### Legacy authentication is not phishing resistant

While any MFA is better than a username and password alone, not all forms of multi-factor authentication (MFA) are created equal. Legacy mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to phishing attacks, malware, SIM swaps,and attacker-in-the-middle attacks. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and the modern FIDO2/ WebAuthn authentication standard.

### Legacy authentication creates MFA security gaps and is costly

Mobile-based authenticators create high-risk security gaps in an agency's MFA strategy, when users can't, don't, or won't use mobile authentication due to union restrictions, personal preferences, mobile-restricted locations, financial reasons and more. Additionally, employers may be required to reimburse employees for using personal cell phones for business purposes. Or alternately, are required to purchase and provide work phones and telecom services for employees, both of which can be expensive. Legacy MFA may also increase cyber insurance premiums or reduce payouts.




yubico

# Phishing-resistant MFA is key to an ever-changing cyber landscape

Modern, hardware security keys such as the YubiKey, are the only technology that offer phishing-resistant multi-factor and passwordless authentication that stops phishing attacks, account takeovers, and ransomware attacks initiated by compromised credentials, helping agencies stay protected and ensure compliance to cyber insurance MFA requirements. YubiKeys are highly suitable for users that can't, don't, won't use mobile authenticators and for mobile-restricted use cases.

### The YubiKey:

- Helps Reduce risk by 99.9% and stops account takeovers with strongest phishing resistance
  Source
- Is FIPS 140-2 validated (Overall Level 1 and Level 2) and CJIS compliant, and meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B
- Reduces help desk costs by up to 75% with self-service password resets
  Source
- Helps lower cyber insurance premiums by 30%
  Source
- Helps bridge to modern FIDO passwordless authentication with multiple authentication protocols on a single key—Smart Card (PIV/CAC), FIDO2/WebAuthn, FIDO U2F, OTP, OpenPGP
- Acts as a portable root of trust that is ideal for shared workstations and devices, and users on the move such as first responders
- Offers 203% Return on Investment (ROI) over three years through flexible YubiKey procurement and deployment options with YubiEnterprise Subscription
  Source

> "Our mission is our citizens. From the vendors to the citizens that deal with us, we're built for that—a fortress wall between threat actors and their data. I had to think of how would I break into there? How can I make it more difficult? People are looking at the state federal compliance from FBI CJIS and compliance standards like PCI DSS. So I look at it from the bad guys perspective to protect not just our people and our city, but our infrastructure. We're a lot further along in securing our future by using the YubiKey."

**Jason Rucker**
Director of Information Technology | City of Southgate, Michigan

**Contact us**
yubi.co/contact

**Learn more in our white paper:**
Modernizing authentication across state, local, tribal and territorial governments

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries.

For more information, visit: www.yubico.com 

yubico