

The 101: Multi-factor Authentication. Unpacked.



A close-up portrait of Mark LaVigne, PhD, a man with a goatee and a friendly smile, wearing a dark suit jacket and a light blue shirt. The background is a blurred outdoor setting with greenery.

Mark LaVigne, PhD
Deputy Director
NYSAC

Today's Presenter



Kimberly Biddings

VP of Product

BIO-key International

- +10 years in cybersecurity
- Helped hundreds of customers understand & implement MFA
- Presented at:
 - NYSAC Legislative Conference – Cybersecurity Workshop
 - NACo CIO Forum & Annual Conference
 - NACo Tech Exchange webinars



LAWRENCE COUNTY
SOUTH DAKOTA

"Where Beauty and Adventure Meet"



Why are we talking about MFA?





The cybersecurity landscape

- **Every 39 seconds** there is a new cyberattack somewhere on the web
- **Over 4,000 ransomware attacks** take place around the world daily
- **A 300% increase in cybercrime reports** since the COVID pandemic was noted by the FBI
- **The average cyber insurance premium rose 25%** since 2021, with some policyholders paying over an 80% higher rate in 2022

Attacks on counties of all sizes

- NJ county hit by ransomware – marks the 22nd US state or local government hit by ransomware in 2022
~340,000 population
- Hackers accessed/acquired resident's personal information from NY county services – residents told to check their credit reports closely
~1.5m population
- Services limited for 3 weeks, and county employee & resident data compromised after ransomware attack in CO county
~49,000 population
- In 2016, one of first ransomware attacks on TN county 911 call center had staff using pencil & paper for 3 days
~32,000 population

NACo CYBER SECURITY PRIORITIES AND BEST PRACTICES

NATIONAL ASSOCIATION OF COUNTIES | NACo | COUNTY TECH XCHANGE

Fighting cyberattacks in local government has become even more difficult in recent months due to attacks such as the SolarWinds breach and Microsoft Exchange (email) exploit, as well as the current pandemic environment and resulting increases in cloud adoption and remote work. These recent events coupled with the rise in ransomware, IoT devices and user credential harvesting, are raising the security bar for what counties need to implement and what they should be doing with end users as it pertains to cyber security. The National Association of Counties through the NACo Telecommunications and Technology Policy Steering Committee established the following priorities:

- Funding assistance in any form deemed necessary to provide for the information technology resources required to adequately provide security at all levels;
- Funding assistance for basic security awareness training of employees and advanced security training for information technology professionals within local government including assistance in the completion of advance certification and degree programs;
- Cooperative efforts in information sharing among all federal, state, and local governments in addition to private sector organizations regarding breaches, potential threats, threat levels, and any techniques that would assist in the prevention or mitigation of cyber related threats;
- Collaborative efforts in the form of committees or task forces that are inclusive of local government membership with federal agencies such as the Department of Homeland Security and subprograms such as NCC, US-CERT, and ICS-CERT;
- Creation of programs and initiatives that designate local government Cybersecurity liaisons and/or representatives that serve in conjunction with federal agencies such as the Department of Homeland Security

Further, in working with the NACo Tech Xchange, as well as national resources and other county IT leadership, it has become apparent how important funding and related resources are needed by counties. This is especially evident in the small to mid-size counties, who face the greatest challenges with implementing and maintaining cyber best practices. Specifically, the following are best practices that are the most important for county cyber needs that exist today to address the increasing onslaught of Cyber Attacks.

Cost **Cyber Defense Impact** **Workload Effort**

The icons represent the percentage of cost, impact on cyber defenses and workload effort needed to implement the priority. The more complete the outer circle of the icon is, the higher the percentage of cost, impact or workload, but also is dependent on current county circumstances.

MFA (Multi-Factor Authentication)

It is a proven fact that multi-factor authentication significantly decreases the amount of successful cyber-attacks on a county. Depending on the main technology platform that a county has implemented for end user authentication, will determine the cost, as well as time and resources needed. And let us not forget the education with end users. MFA solutions alone can run into hundreds of thousands of dollars, depending on the size of the county.

[NACo Cybersecurity Priorities and Best Practices](#)

Required for DHS Cybersecurity Grant Program

On September 16, 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country.

Current closing date for applications: Nov 15, 2022

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.

The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible from the Internet;

POLL QUESTION

Do you have MFA in place today?

We have MFA in place for:

- A. All access
- B. Some access
- C. We do not have MFA
- D. I'm not sure

MFA can prevent up to 90% of cyberattacks.

What is MFA?







Log in to your account

Username

Password

Login

Can't log in?

[Privacy policy](#) [Terms of use](#)



noun: **identity** ; plural noun: **identities**

1. the fact of being who or what a person or thing is.

noun: **authentication** ; plural noun: **authentications**

1. the process or action of proving or showing something to be true, genuine, or valid.



MULTI-FACTOR AUTHENTICATION

Using multiple authentication methods to prove you are who you say you are.



Two-Factor Authentication
E.g., PIN and Face

01
Something You ARE
Fingerprint, Face, Palm

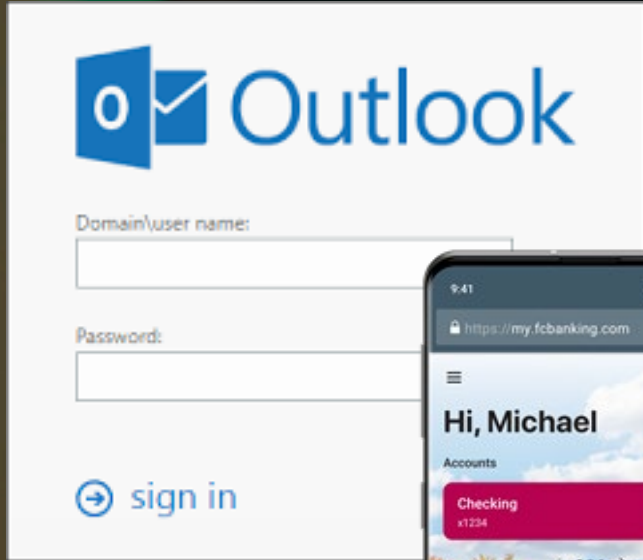
Multi -Factor Authentication
E.g., PIN, Face, & ID Badge

03
Something You KNOW
Password, PIN, Security Questions

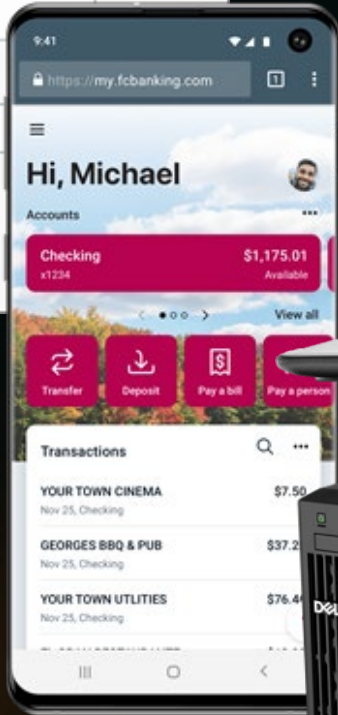
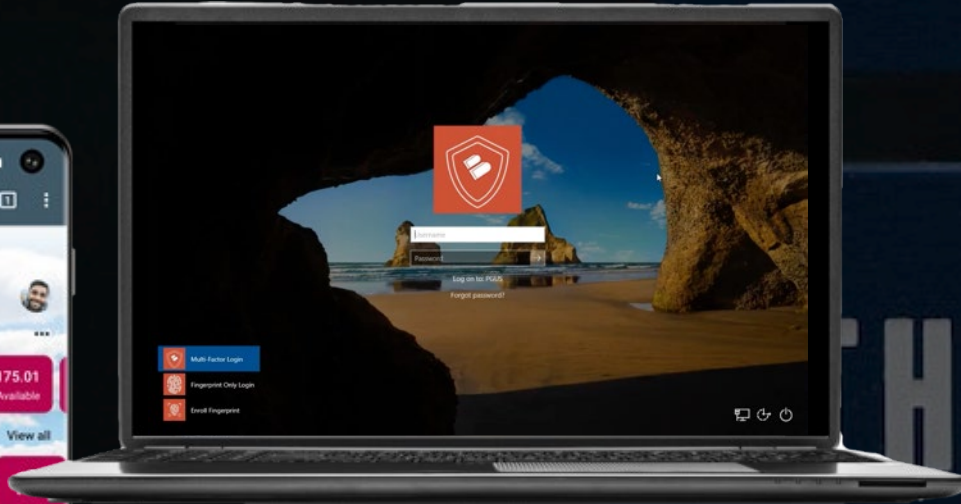
02
Something You HAVE
Smart Card, USB Token, RFID Badge, USB Dongle, Phone, PC



APPLICATIONS



DESKTOPS



SERVERS



HERE

HERE

EVERYWHERE

How do you implement MFA?



5 critical steps to implementing MFA



How do you know what authentication you should use?

THE PERSON



HOW THEY WORK



WHAT'S REQUIRED



WHAT THEY ACCESS

USABILITY

Ease of use increases



SECURITY

Security increases



Analyzed each method for:

- ✓ Security
- ✓ Convenience / Ease of Use
- ✓ Total Cost
- ✓ Effort of Implementation
- ✓ Ongoing Maintenance
- ✓ Phone-based or Not

Your cybersecurity policy outlines your guidelines and provisions for preserving the security of your county's data and technology infrastructure

V6.5.1.6: Security Policy - marketing department Edit Form In Raw Mode

Actions - Login

Information

Actions ▾

- Login
- Password Change
- RADIUS / VPN
- Desktop 2FA
- Account Unlock
- Password Reset
- Password Recovery
- Authentication Methods >
- Rules >
- Groups >
- Groups >

How will users login Two-factor (2FA) ▾

Allow End-user 2FA Opt-In

OTPMETHODS

Change Requires Password Re-Entry

Accepted OTP Methods

Phone Mobile App Web-key BIO-key PalmPositive BIO-key FacePos

BIO-key Push Token

Default Authentication Method Phone ▾

Allow Users to Override

FIDOPASSWORDLESS

Allow Passwordless Login with FIDO2 Token

Passwordless Login Bypasses Login Enrollments

REMEMBER BROWSER

INFORMATION SECURITY POLICY INCLUSIONS


- Access control
- Identification and Authentication**
(including multi-factor authentication and passwords)
- Data classification
- Encryption
- Remote access
- Acceptable use
- Patching
- Malicious code protections
- Physical security
- Backups
- Server security
(e.g. hardening)
- Employee on/offboarding
- Change management



Communication is key – use “Cyber Champions” to lead the way.

5 Steps to Communicating Effectively



A scenic landscape featuring a winding asphalt road that curves through a valley. The terrain is covered in dense green vegetation, and the hillsides are bathed in the warm, golden light of a setting or rising sun. The sky is a clear, pale blue, and the overall atmosphere is peaceful and contemplative. The road leads the eye from the foreground into the distance, where more hills and a small structure are visible.

Cybersecurity is an ongoing journey with multiple chapters.

BIO-key PortalGuard

An award-winning platform to secure access for Employees, Citizens, & Suppliers



Multi-factor Authentication (MFA)

Wide range of authentication methods for flexible, powerful identity security



Identity-Bound Biometrics

Unique, centralized biometric identity that can be used to verify the person



Single Sign-on (SSO)

Reduce password prompts and secure access to all apps from single IdP



MobileAuth

Multi-factor authentication app that offers Identity-Bound Biometric authentication options & push tokens



Self-service Password Reset (SSPR)

Reduce password-related IT support calls by up to 95%



Hardware Devices

Offer a variety of devices including Microsoft-qualified Windows Hello USB fingerprint scanners & FIDO-keys



Learn more:

Ranking Authentication Methods eBook



Try PortalGuard & MFAOR Contact Us to
schedule a discovery call



Questions?



Thank You

Kimberly.biddings@bio-key.com

www.BIO-key.com

