CYBERSECURITY AWARENESS MONTH

DO YOUR PART. #BECYBERSMART

IN THIS PRESENTATION
• Company Overview
• Series Overview
• User Behavior Recap
• Network Security
• Summary
TRAINING SERIES OVERVIEW

- Raise awareness about cybersecurity’s importance
- Help keep data from bad actors
- Understand use of hardware/software tools
- Understand practical steps to protect your networks
- Reduce volume and impact of attacks
- No program leads to 100% success

SERIES OVERVIEW: AWARENESS & TRAINING LEVELS

- Ensure all users are made aware of security risks, applicable policies, standards and procedures
- Ensure personnel are trained to carry out their assigned security-related duties and responsibilities
- Provide security awareness training on recognizing and reporting potential indicators of insider threat
- Provide awareness training focused on recognizing and responding to threats from social engineering, etc. Update at least annually or when there are significant changes.
- Include practical exercises aligned with current threat scenarios

Intermediate Cyber Hygiene

Good Cyber Hygiene

Proactive Cyber Hygiene
IN THIS PRESENTATION
- Company Overview
- Series Overview
- User Behavior Recap
- Network Security
- Summary

USER BEHAVIOR RECAP: SOCIAL ENGINEERING

The use of human interaction, social skills and manipulation by an attacker to obtain or compromise information about an organization or its computer systems.
USER BEHAVIOR RECAP: PHISHING

*A form of social engineering using email or malicious websites to solicit personal information by posing as a trustworthy organization.*

---

USER BEHAVIOR RECAP

*This type of social engineering relies on interactions with potential victims through software to attempt to install malware.*

a) Vishing  
b) Computer-Based  
c) Tricking  
d) Human-Based

---

USER BEHAVIOR RECAP

*This type of social engineering relies on interactions with potential victims through software to attempt to install malware.*

a) Vishing  
b) Computer-Based  
c) Tricking  
d) Human-Based

---
A common indicator of a phishing attempt is:

a) Suspicious Sender’s Address
b) Generic Greeting or Signature
c) Suspicious Attachments and/or Hyperlinks
d) All of the Above

This email is an example of what type of social engineering?

a) Vishing  b) Smishing  c) Phishing  d) Wishing
This email is an example of what type of social engineering?

- a) Vishing
- b) Smishing
- c) Phishing
- d) Wishing

From January 1 – October 14, 2020, the U.S. economy lost ______ due to COVID-19-related fraud cases?

- a) $80,600,000
- b) $120,500,000
- c) $160,750,000
- d) 200,175,000
A form of phishing where fraudsters tailor attacks to a specific victim or group of victims using personal details.

a) Vishing  b) Smishing  c) Spear Phishing  d) Mass Phishing

Be wary of unsolicited attachments, even from people you know.

Trust your instincts.

Save and scan any attachments before opening them.

Disable option to automatically download attachments.
USER BEHAVIOR RECAP

- Create separate accounts on your computers
- Keep software up to date
- Do not reuse same password across accounts

IN THIS PRESENTATION

- Company Overview
- Series Overview
- User Behavior Recap
- Network Security
- Summary

NETWORK SECURITY

“Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”

- U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)
NETWORK SECURITY

Control Who Accesses Data & Information
Conduct Background Checks
Require Individual User Accounts and Authentication for Each Unique User
NETWORK SECURITY

• Create Policies & Procedures
• Develop a Disaster Recovery Plan
• Develop & Test Backup Strategy

DETECT

PROTECT

PLAN

PRESERVE

NETWORK SECURITY

• Install & Monitor Logs
• Train Your Employees
• Require Strong, Unique Passwords

DETECT

PROTECT

PLAN

PRESERVE
NETWORK SECURITY

• Install Surge Protectors & Uninterruptible Power Supplies (UPS)
• Install & Activate Software/Hardware Firewalls on All Networks
• Secure Wireless Access Point & Networks
• Install & Update Anti-Virus, Anti-Spyware, Anti-Malware Programs

NETWORK SECURITY

• Patch Operating Systems & Applications
• Make Patching Automatic
• Set Up Web & Email Filters
• Use Encryption For Sensitive Information
• Control Removable Media
• Dispose Of Old Computers & Media Safely

NETWORK SECURITY

• Know Roles & Responsibilities
• Engage Disaster Recovery Plan
• Contact Appropriate Stakeholders
• Recover Backed Up Data
• Consider Cyber Insurance
• Continuously Improve Processes, Procedures, & Technologies
**NETWORK SECURITY**

- Ensure Wi-Fi Connection is Secure
- Change the default password
- Require a password to get on network
- Segregate your network
- Enable firewall

---

**NETWORK SECURITY**

Older Installations May Not Be Secure
- Ensure Anti-Virus is Fully Running & Updated
- Ensure All Security Software is Updated
- Regularly Check Privacy Tools, Add-Ons & Patches
NETWORK SECURITY

- Establish and maintain baseline configurations
- Configure systems to provide only essential capabilities
- Control and monitor user-installed software
- Establish and enforce security configuration settings
- Track, review, approve/disapprove, and log system changes
- Analyze security impact of changes prior to implementation

- Define, document, approve and enforce access restrictions
- Restrict, disable, or prevent the use of nonessential programs
- Apply deny-by-exception to prevent use of unauthorized software
- Apply permit-by-exception to allow execution of authorized software
- Employ application whitelisting and vetting for identified systems
- Verify integrity and correctness of security critical software
SUMMARY QUIZ

These can be used to block malicious communications or browsing to inappropriate websites

a) Firesticks  b) Firewalls  c) Whitewalls  d) Spyware
SUMMARY QUIZ

These can be used to block malicious communications or browsing to inappropriate websites

a) Firesticks  b) Firewalls  c) Whitewalls  d) Spyware

SUMMARY QUIZ

These can help remove attached malware attached from entering your inbox and prevent it from being cluttered by unsolicited and undesired spam.

a) Encryption  b) Firewalls  c) Email Filters  d) Passwords

SUMMARY QUIZ

These can help remove attached malware attached from entering your inbox and prevent it from being cluttered by unsolicited and undesired spam.

a) Encryption  b) Firewalls  c) Email Filters  d) Passwords
SUMMARY QUIZ

The process of making your electronically stored information unreadable to anyone not having the correct access.

a) Encryption  b) Firewalls  c) Email Filters  d) Patches

SUMMARY QUIZ

Software vendors provide _______ and updates to their supported products to correct security concerns and improve functionality

a) Downloads  b) Protocols  c) Viruses  d) Patches
SUMMARY QUIZ

Software vendors provide _______ and updates to their supported products to correct security concerns and improve functionality

a) Downloads  b) Protocols  c) Viruses  d) Patches

SUMMARY QUIZ

Uninterruptible _______ Supplies (UPS) provide a limited amount of battery power to allow you to work through short power outages and provide enough time to save your data when the electricity goes off.

a) Preservation  b) Power  c) Planning  d) Protection
SUMMARY

- Plan, Protect, Preserve
- Assume You are a Target
- Install and Update Security Software
- Implement and Test Backups
- Physically Protect Network and Hardware

SUMMARY: CYBER SECURITY MONTH

THINK BEFORE YOU CLICK

DO YOUR PART.
#BECYBERSMART

SUMMARY: NEXT SESSION

SESSION 5: BACKUP STRATEGIES
TUESDAY, OCTOBER 27, 2020
11:30 AM
AUDIENCE

Weak authentication is a common vulnerability for information systems—it is consistently one of CISA’s top five, most frequent findings for Federal High Value Asset systems. Furthermore the 2019 Verizon Data Breach Investigations Report states that compromised passwords remain “prominent fixtures” of breaches. Implementing strong authentication methods across an organization can dramatically improve resilience against common cybersecurity threats such as phishing attacks and compromised credentials.

Although this guide references federal standards and publications, it is not mapped to nor directly associated with any agency. These recommendations are applicable to any organization seeking to better their authentication process.

PURPOSE

The purpose of this guide is to lay out the concept of authentication, recommend related security enhancements, and provide guidance to help plan and implement a strong authentication solution. Strong authentication is one of many pillars of a defense-in-depth cybersecurity strategy, but it is not the only solution to cybersecurity issues.

THE CONCEPT

Authentication is the process of verifying that a user’s identity is genuine. Most systems require a user to be authenticated prior to granting access to the system. The user does this by entering a password, inserting a smart card and entering the associated personal identification number (PIN), providing a biometric (e.g., fingerprint, voice pattern sample, retinal scan)—or a combination of these things—to prove they are who they claim to be. The credentials provided are compared to those that have previously been associated with the user. The credential match may be performed within the system being accessed or via a trusted external source. If the credentials match, the system authenticates the identity and grants access (see figure 1).

![Figure 1: Relationship between identity, authentication, and access](image-url)
Authentication Methods
Different systems may implement different authentication methods to validate the user’s identity. Authentication methods can be grouped into three factors:

- Something you know (knowledge)
  - Examples include password, passphrase, or PIN
- Something you have (possession)
  - Examples include smart card, token, look-up secrets, one-time password devices, or cryptographic devices
- Something you are (inheritance/physical traits)
  - Examples include fingerprints, iris, facial characteristics, voice pattern, or gait

Single-Factor Authentication is a common, low security method of authentication. It only requires one factor, such as a username and password, to gain access to a system. (Although it includes two pieces of information, a username and password combined is still a single factor because they both come from the same category.)

Multi-Factor Authentication (MFA) is a strong authentication method. It requires two or more factors to gain access to the system. Each factor must come from a different category above (e.g., something you know and something you have). MFA may be referred to as two-factor authentication, or 2FA, when two factors are used.

A study conducted by Google, New York University, and University of California San Diego demonstrates the significant improvement implementing MFA has on an organization’s resistance to malicious attacks. The study found that using MFA blocked 100 percent of automated bots, 99 percent of bulk phishing attacks, and 66 percent of targeted attacks on users’ Google accounts.2

Assurance Levels
Different authentication methods have different assurance levels based on the robustness of the process and the confidence that the identity is who they claim to be. Organizations may determine that it is not worth the cost of implementing higher assurance levels for systems that do not contain sensitive information and are not connected to the same network as those that contain sensitive information. For more information on assurance levels, refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 Digital Identity Guidelines3 and associated standards,4 which describe authentication assurance levels and provide a risk-based approach for selecting the strength of authentication appropriate for a given system.

THE PROBLEM
Single-Factor Authentication—Everybody Uses Passwords. Are They Really That Bad?
Single-factor authentication, which usually means a username and password, provides attackers an easy way to gain access to the system.5 Since passwords are just data, attackers have many different techniques they can use to steal a password without being physically present, including:

- Brute-force attacks
- Phishing
- Keylogging
- Social engineering
- Plaintext password storage
- Credential dumping
- Network sniffing
- Malware

---

2 New research: How effective is basic account hygiene at preventing hijacking. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html
4 Other digital identity standards include ISO/IEC 29115:2013 and the European Union’s eIDAS regulation, as well as efforts to apply digital identity to emerging needs such as ePassports (ICAO’s Digital Travel Credentials Sub-Group) and digital driver’s licenses (ISO 18013 standards). Other examples can be found through The World Bank’s ID4D Identification for Development resources at https://id4d.worldbank.org/.
5 NISTIR 7983, Report: Authentication Diary Study, surveys user behaviors for coping with the friction and burden imposed by managing their portfolios user IDs and password (https://csrc.nist.gov/publications/detail/nistir/7983/).
Weak passwords (e.g., the manufacturer’s default password or passwords that follow a pattern [see figure 2]) make it easier for an attacker to compromise a password. Other unsecure practices may compound the impact a compromised password can have on the organization.

- Password reuse allows an attacker who has compromised a password to access multiple systems, networks, or data sets. Organizations can discourage password reuse, but there is no technical control that can prevent a user from reusing a password across multiple systems. The inability to prevent password reuse leaves a compromised password available for attackers to use to gain access to other systems.

- Admin password sharing makes it more likely that a privileged (administrative) account with elevated access can be compromised; an administrative password is often written down, located in a place where multiple people have access to it, simplified to make it easier to remember, and not changed frequently—even after people leave the organization. Once it has been compromised, an administrative password grants the attacker elevated access across the network and/or across multiple systems.

Adding another authentication factor (i.e., something you have or something you are) dramatically increases the difficulty of compromising an account, because a compromise now requires either the physical presence of the user or possession of a physical object such as a smart card.6

An asset with the weakest method of authentication becomes a potential path to bypass stronger authentication for a system that it is connected to. A concrete and steel building with reinforced doors and sophisticated locks can still easily be entered by intruders if there are large open windows.

To receive the full benefit of an MFA capability, organizations should be sure to implement it across all systems, applications, and resources. Requiring multi-factor authentication to gain initial access to an organization’s network (usually the user’s workstation) is a good first step; however, this provides only limited protection to other systems and data within the organization that are protected with only single-factor authentication. Threat actors may

---

6 While there are types of attacks that can compromise MFA, particularly for “something you have” authenticators, they require deceiving the user to take an affirmative act to allow access to the account and are thus not easily automated or commonly used.
seek to exploit the less protected systems and then move to other systems and continue their malicious actions.\(^7\) Network segmentation may also reduce the attacker’s ability to move throughout the network, but accounts relying on single factor authentication are still susceptible to compromise and represent the weakest link.

**WHAT CAN YOU DO?**

**Planning Phase**

**Strategic Planning**

Implementing MFA on all systems, applications, and resources can be challenging and expensive; when approached individually each requires its own, specific method of verifying a user’s identity (e.g., multiple credentials must be issued, managed, and revoked). For this reason, organizations will be most effective in implementing authentication by taking an organization-wide approach and implementing the solution as an enterprise service for systems and applications across the entire organization instead of trying to implement redundant, isolated authentication solutions for each application.

An organization-wide strategy allows standardization of authentication policies and practices, including the issuance and management of necessary credentials, and reduces the cost of each application acquiring or building its own authentication solution. Organizations should examine their existing capabilities to determine if they already have a viable solution to provide MFA across the organization. Federal agencies, for example, have Personal Identity Verification (PIV)-based authentication for users. An organization whose user accounts are managed through large commercial providers may be able to leverage the MFA capabilities already available from their service provider. Organizations with no MFA capabilities currently available should procure or design an MFA solution.

When deciding on an MFA solution, organizations should consider the following.

- Initial authentication of a user to the network or system
- Additional authentication as users access other systems, applications, or new segments of infrastructure
- Authentication to externally hosted resources
- Authentication to internal resources by external entities

Once an organization decides on an enterprise MFA solution, authentication capabilities can be expanded through single sign-on (SSO) and identity federation services. SSO and identity federation securely shares authentication and identity information across organizations, systems, applications, and resources without requiring individual implementations of the MFA capability on each system. Many systems come with connectors for SSO already in place. SSO and identity federation enhance security to the organization by putting control of access to resources in the hands of a central identity management administrator, which allows the organization to rapidly and comprehensively revoke access across all its resources when the user leaves or should the account ever be compromised. These steps simplify the management of the identity lifecycle—including various credentials issued to the user—and help ensure that access across the organization is promptly revoked when a user leaves.

An additional benefit is simplifying the user experience—users no longer must keep track of dozens of credentials—while simultaneously reducing the organization’s vulnerability to weaknesses in how the users manage multiple credentials.

\(^7\) A dramatically improved approach to address these issues underlies the concept of a zero-trust architecture, which does not implicitly trust anyone but enforces continuous authentication. NIST SP 800-207 Zero Trust Architecture (currently in draft form, https://csrc.nist.gov/publications/detail/sp/800-207/draft) goes into more detail on the concept of zero trust.
Single Sign-On

SSO is an authentication method where a user authenticates once—typically using the strong MFA authentication solution selected by the organization—to the centralized SSO solution. Other systems and applications are configured to trust the centralized SSO solution to authenticate the user with no further interaction required (see figure 3). This reduces the need to repeatedly authenticate to multiple systems and services. Most importantly, when a user moves from their initial authentication to other systems through SSO, the user’s credentials for the initial system are not shared with the other system. Once a user authenticates, the SSO solution transparently and securely completes the process for all systems involved without further exposing the initial system credential. In addition, each application is not required to manage its own identity credential store but leverages a centralized store across the organization.

Note: some SSO providers may still authenticate to other systems with a username/password for that system; organizations should ensure their SSO solution is set up with strong, non-password-based protocols at each step of connecting to a resource. Multiple technical options for incorporating SSO capabilities in an organization’s infrastructure exist. When selecting an SSO solution, organizations should consider single sign-off capabilities—which terminate all open and active sessions when a user logs out—to minimize the risk of session hijacking.

Identity Federation

Although identity federation is not, in and of itself, a solution to weak authentication; it can provide substantial indirect support for improving authentication. Identity federation refers to the establishment of a trusted relationship between more than one organization that manage their own users, identities, and authentication, in order to accept each other’s users. Organizations should only federate with other organizations whose identity vetting and authentication processes they trust. Such as, two organizations manage their own users, identities, and authentication and then establish connections between their systems, to reduce the points of weak authentication for external users that expose an organization to attacks. For example, imagine that Acme Anvil Co., and Coyote Missile Co., have an overlapping mission that requires Acme Anvil to share information with Coyote Missile, but each organization already manages the identities of their employees in their own identity store. Instead of using resources to perform a new background check on the Coyote Missile employees who need access to the information, Acme Anvil could choose to establish a trusted relationship with Coyote Missiles identity store to authorize access to the Acme Anvil system, knowing that Coyote Missile has already conducted a background check on the individual and established their identity (see figure 4).

---

8 Open ID Connect, OAuth 2.0, Kerberos, and SAML 2.0 are examples of protocols that use secure, non-password-based connections for SSO. Many social media-based SSO services that consumers use are based on Open ID Connect, allowing even consumers to use SSO while focusing on strong authentication for their primary login provider.
Identity federation thus can expand an organization’s strong authentication and SSO capabilities even further to systems owned by trusted organizations that its users access and vice versa. Organizations that need to share resources with another organization’s users can use the trusted, federated user identities without duplicating the identity-proofing or identity management for those users. Without identity federation, the authentication and identity store for any resource that is shared with another organization must be configured and managed separately from its primary identity store, which increases complexity.

**Know When to Move On**

An organization may identify resources for which incorporating strong authentication will prove too expensive or technically complicated. If this occurs, the organization must decide between 1) remaining with the current system and implementing compensating controls to address the risk to the organization; or 2) migrating to a new, modernized system that allows integration with the strong authentication solution. The organization should weigh the cost and risks of each option.⁹

**Note:** although outside the scope of this document, the organization should consider the performance and security benefits in addition to strong authentication that migration to updated technology will provide when making their decision.

**Other Strategic Considerations**

Especially for large organizations, non-technical considerations regarding binding policies, responsibilities, and budgets are likely to be relevant. If information systems are not managed and controlled by a central office or chief information officer (CIO), additional engagement and coordination will be necessary with the different offices that own the systems to align with the organization’s overall strategy. Similarly, if an organization’s information technology (IT) budget is not centrally managed, then the organization may need to consider how the cost of implementing and operating components of strong authentication, SSO, or identity federation can be recovered from each element of the organization.¹⁰

---

⁹ The calculation of the cost of such compensating controls should incorporate the cost of technical implementation of compensating controls, the cost of time and organizational complexity for administering those compensating controls, and the risk introduced by relying on additional controls and security measures to support those controls.

¹⁰ Consider the incentives that the cost recovery model creates. Any pass-through of costs to business units for adoption of the organization’s authentication can be counterproductive to improving security if the business unit’s cost increases incrementally for each user or application which it transitions to the strong authentication solution.
While automated system-to-system connections are not strictly within the scope of this guidance (and MFA is not an option for a server credential), they still leave an avenue of attack open by providing a “non-person account” to access a system. As mentioned previously, when any form of weak authentication is combined with a lack of effective network segmentation this weakness can be further exploited to move around a network, thus defeating the benefits of strong authentication implemented elsewhere. Organizations can remove this path for attackers to bypass the strong user authentication to systems by securing these connections with strong credentials (Secure Socket Layer [SSL] certificates), encrypted communications, and application-specific or IP address allowlisting.

**Tactical Planning**

Tactical planning involves discovery of the current state environment, determining the to-be state, and developing a transition plan to execute cost effective methods to migrate to the target state.

To address weak authentication, there must be 1) knowledge of the “as-is” state, 2) available capabilities, and 3) understanding of what is needed to achieve the desired state. It is essential to avoid analysis paralysis when planning and undertaking these enterprise improvement efforts. Seeking 100 percent knowledge or assurance (perfection), whether for current or future state, inhibits incremental improvements based on available (good enough) information.

**Understand the “as-is” State**

1. Catalog current applications and systems.
2. Identify users and user groups that have access to the system or application, including partners and external stakeholders with whom you share data.
3. Catalog the nature of the data shared with partners, as the need to safeguard sensitive data can drive protocol and architectural considerations. Where sensitive data is being exchanged, more detailed information about users may be necessary to enforce least-privileged access. This is particularly true for systems where sensitive data is only a subset of the data in the system (and the organization does not want to incur the financial or efficiency cost of extra security on non-sensitive data).
4. Identify the authentication method for each user to each application or system.
5. Identify authentication protocols that each system or application supports.
6. Identify supporting elements of the architecture—such as automatic system-to-system connections that will also need to be secured—to ensure configuration of secondary elements does not introduce vulnerabilities.

**Identify Current Capabilities**

1. Identify existing MFA capabilities, such as PIV card authentication, within the organization.
2. Evaluate the acquisition or budget options for executing an initiative to strengthen authentication, incorporating the strategy for recovering costs that aligns with the strategy of broad adoption of strong authentication.
3. Identify existing assets or licenses for applications that could provide MFA capabilities.
4. Evaluate licensing agreements for systems or applications to be integrated with the strong authentication solution. Support for methods of strong authentication or strong SSO/federation protocols may require additional licenses or a different type of license from the application to be secured; those licenses are separate from the cost of the strong authentication solution or SSO/federation solution itself. Understanding the end-to-end cost of implementation will inform total cost of ownership and support decision-making about cost-effective risk-management.
5. Identify current personnel with experience in implementing MFA capabilities.

**Understand the “to-be” State**

1. Select the strong authentication solution that best fits your environment and regulatory requirements (e.g., certain authentication solutions may work for an on-premise architecture but may not work well for a cloud architecture).
2. Define how users will authenticate to the network, to each subsequent system and application, and to externally hosted resources; define how external users will authenticate to internal resources.
3. Determine which systems and applications will be integrated into an SSO solution.
4. Determine which organizations with which to establish a trusted identity federation.
5. Set boundaries for systems that have different strengths of authentication and ensure that connections from weaker authenticated systems or users do not allow for weakly authenticated access to a system that is secured with stronger authentication. Pay attention to system-to-system connections crossing a boundary from a less secure environment to a system in a more secure environment.
6. Design the target architecture upon full deployment of the planned strong authentication solution. Include where the authentication solution will support other organizational security practices such as network segmentation.

Transition Plan

1. Develop a transition plan and schedule to get from the “as-is” state to the defined “to-be” state.
   a. Use a risk management strategy to prioritize users and applications for onboarding to the solution.
   b. Users with elevated privileges in a system or application are most critical for onboarding, as are those systems or applications that are critical to delivering the business mission, for core organizational functionality, or that contain sensitive data.
   c. Prioritize the organization’s most critical systems and assets that have the weakest authentication.
2. If a trusted identity federation with another organization will be used, determine how these users will be transitioned without negatively impacting their current accesses.
3. Test the migration plan against representative systems.

EXECUTION PHASE

In this phase, your organization executes strong authentication using the artifacts obtained during the planning phase. During execution, schedules and other artifacts may need to adjust to “conditions on the ground” and lessons learned. As such, adjustments under consideration should undergo the same level of rigor given to the artifacts during the planning phase. The notional timelines below can be adjusted based on the size and scope of the effort.

Short-Term Actions

1. Procure or design the strong authentication solution based on the organization’s architectural analysis and risk management determination.
2. Acquire hardware, software, and licenses, including the SSO solution, necessary to implement the transition plan defined during the planning phase.
3. Identify and catalog business processes for managing users from a centralized identity governance administration point.
4. Begin implementing strong authentication for the organization’s privileged users and its highest value systems and assets as defined in the transition plan.
5. Incorporate criteria for evaluation of a system’s authentication compatibility with the organization’s strong authentication solution into the organization’s review of proposed acquisitions or new systems.

Medium-Term Actions

1. Continue migrating systems to the strong authentication system.
2. Leverage the initial implementation of the strong authentication solution to connect to an SSO solution.
3. Transition authentication from existing systems and applications to the SSO solution.
4. Evaluate new acquisitions or proposed systems to determine compatibility with the organization’s strong authentication solution prior to procuring those systems.
Long-Term Actions

1. Continue migrating systems to the strong authentication system.
2. Establish trust relationships with other organizations for identity federation.
3. Onboard non-person entities such as service accounts.
4. Enable continuous improvement through regular review and updates to requirements, policy, and reference architecture.

SUMMARY

Strong authentication via MFA is a critical and sometimes expensive investment, but should be implemented across all networks, systems, applications, and resources to adequately protect the organization. For this reason, an organization-wide approach is recommended. One method of expanding MFA capabilities across an organization is through an SSO solution. In addition to providing better security for an organization’s resources, an SSO solution improves the user experience because it removes the need to remember passwords or manage multiple credentials such as RSA tokens for each system and application. An SSO solution implemented at an enterprise level may also eliminate the need for system owners to expend resources managing their own authentication solutions. Once an SSO solution is in place, organizations can further expand strong authentication capabilities through identity federation with other organizations. By incorporating these concepts and other strategic considerations into the evaluation of their “as-is” state, an organization can define their desired “to-be” state and create a plan to get there.
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC’s COVID-19 Situation Summary.

COVID-19 Risk Profile

On March 11, the COVID-19 outbreak was characterized as a pandemic by the WHO. The virus that causes COVID-19 is infecting people and spreading easily from person-to-person. Cases have been detected in most countries worldwide and community spread is being detected in a growing number of countries.

In anticipation of a broader spread of COVID-19, globally and within the United States, organizations should plan for continued impacts to their workforce and operations.

CISA’s Role as the Nation’s Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

CISA will use its relationships with interagency and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government.

As the situation changes, the virus may affect essential operations for businesses and federal, state, local, tribal, and territorial (SLTT) government entities.

To stay current with CISA’s efforts regarding the COVID-19, visit: cisa.gov/coronavirus.

What’s in this guide:

- Actions for Infrastructure Protection
- Actions for your Supply Chain
- Cybersecurity for Organizations
- Cybersecurity Actions for your Workforce and Consumers

Additional Information:

Visit the CDC website, or contact CDC for COVID-19-related issues or to share critical and timely information by sending an email to eocjiclead2@cdc.gov and eocjictriage2@cdc.gov or by calling 1-800-232-4636.
**Actions for Infrastructure Protection**

Planning and preparedness are critical to reducing the impact of COVID-19 on the Critical Infrastructure community and CISA recommends organizations take the following precautions to prepare for possible impacts from COVID-19:

- **Designate** a response coordinator and assign team members with specific responsibilities.
- **Implement** a formal worker and workplace protection strategy.
- **Train** workers on personal and worksite protection strategies.
- **Establish** and test flexible worksite (e.g., telework) and work hour policies.
- **Identify** essential functions, goods, and services your organization requires to sustain its own operations and mission.

- **Determine** how long your organization can expect to continue providing essential functions, goods, and services in potentially reduced quantities.
- **Identify and prioritize** suppliers of critical products and services for your organization.
- **Continuously assess** ongoing preparedness activities to adjust objectives, effects, and actions based on changes in the business and greater economic and social environments.
- **Monitor** federal, state, local, tribal and territorial COVID-19 information sites for up-to-date information on containment and mitigation strategies.

**Actions for your Supply Chain**

- **Assess** your organization’s supply chain for potential impacts from disruption of transport logistics and international manufacturing slowdowns resulting from COVID-19.
- **Discuss** with those suppliers any challenges they may be facing or may expect to face due to the ongoing situation.
- **Identify** potential alternate sources of supply, substitute products, and/or conservation measures to mitigate disruptions.
- **Communicate** with key customers to keep them informed of any issues you have identified and the steps you are taking to mitigate them.

**Cybersecurity for Organizations**

As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:

- **Secure** systems that enable remote access.
  - **Ensure** Virtual Private Network and other remote access systems are fully patched.
  - **Enhance** system monitoring to receive early detection and alerts on abnormal activity.
  - **Implement** multi-factor authentication.

- **Ensure** all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.
- **Test** remote access solutions capacity or increase capacity.
- **Ensure** continuity of operations plans or business continuity plans are up to date.
- **Increase** awareness of information technology support mechanisms for employees who work remotely.
- **Update** incident response plans to consider workforce changes in a distributed environment.

**Cybersecurity Actions for your Workforce and Consumers**

Malicious cyber actors could take advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. **Phishing** attacks often use a combination of email and bogus websites to trick victims into revealing sensitive information. Disinformation campaigns can spread discord, manipulate the public conversation, influence policy development, or disrupt markets.

CISA encourages individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions:

- **Avoid** clicking on links in unsolicited emails and be wary of email attachments.
- **Do not reveal** personal or financial information in emails, and do not respond to email solicitations for this information.
- **Review** CISA’s Tip on Avoiding Social Engineering and Phishing Scams for more information on recognizing and protecting against phishing.
- **Use** trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
CISA INSIGHTS

ACTIONS TO COUNTER EMAIL-BASED ATTACKS ON ELECTION-RELATED ENTITIES

SEPTEMBER 10, 2020

THE THREAT AND HOW TO THINK ABOUT IT

Malicious cyber actors have been known to use sophisticated phishing operations to target political parties and campaigns, think tanks, civic organizations, and associated individuals. Email systems are the preferred vector for initiating malicious cyber operations. Recent reporting shows 32 percent of breaches involve phishing attacks, and 78 percent of cyber-espionage incidents are enabled by phishing.1,2

Cyber actors launching phishing attacks often seek to entice users to do one of three things.

➢ Click on a link and turn over credentials (username and password), so the cyber actor can gain access to an account.
➢ Open an attachment or click a link that delivers the cyber actor’s malware.
➢ Click a link to a website that the cyber actor monitors; this verifies that the email account is valid for subsequent targeting.

Cyber actors can also use credential-based techniques to gain access to accounts in various ways.

➢ Password spraying attacks rely on cyber attackers using a commonly used password against multiple usernames.
➢ Brute-force attacks rely on cyber attackers knowing the username and attempting several passwords.
➢ Credential stuffing attacks rely on cyber attackers using usernames and password combinations gained from data breaches against other accounts.

To protect against these attacks, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations involved in any election-related activities prioritize the protection of accounts from email-based attacks by:

➢ Using provider-offered protections, if utilizing cloud email.
➢ Securing user accounts on high value services.
➢ Implementing email authentication and other best practices.
➢ Securing email gateway capabilities.

WHEN USING CLOUD EMAIL, USE PROVIDER-OFFERED PROTECTIONS

Organizations that use cloud email providers should enable various protections their provider offers.

a. Require multi-factor authentication (MFA) for all user email accounts.

➢ Use either physical security keys (such as those following the FIDO2 standard) or authentication apps (such as those following the TOTP algorithm).

   o Physical security keys offer protection against phishing attacks by working as a second, physical factor of authentication and only authenticating when a user is on the correct

---

website. Thus, even if a user is tricked into supplying their password to a phishing website, the physical security key will still block attackers from accessing their account.

- Authentication apps work by having a user enter a code from an app. Although authentication apps can still be vulnerable to phishing attacks, they offer more protection than SMS or email-based MFA.
  - Only use SMS and email-based MFA methods if other forms of MFA are unavailable. SMS and email-based MFA methods are vulnerable to phishing and SIM swap attacks, though they still offer better protection than password-based single-factor authentication.

b. When available, enroll user accounts in advanced protection services.

- These services provide the highest level of protection against phishing and other attacks, applying robust filtering techniques, with many requiring physical security keys. For instance, Google offers an Advanced Protection service for all users, and Microsoft offers an Advanced Threat Protection service. Google also offers an Enhanced Account Protection service at no cost to at-risk election-related organizations. Note: CISA includes these references with the intention of highlighting the types of services available; doing so does not constitute endorsement of any particular company or service.

SECURE USER ACCOUNTS ON HIGH-VALUE SERVICES

Protect individual accounts on high-value services to mitigate the impact of a successful phishing attack.

a. Enroll in a password manager service for your organization and encourage employees to use it.

- Password managers protect against phishing by generating secure, random passwords and automatically filling passwords when visiting websites. Password managers will not automatically enter passwords on malicious websites, giving employees a crucial cue that they should not proceed.

b. Require MFA for user accounts on all high-value services when possible.

- If possible, deploy physical security keys for access to high-value services.
- After physical keys, authentication app-based MFA (TOTP) is the next safest option, followed by SMS and email-based MFA. Use SMS and email-based MFA only when no other MFA options are available.
- If a high-value service does not support any form of MFA, consider switching to a similar service that does offer MFA.

c. Eliminate unnecessary password composition and rotation requirements in favor of secure, human-friendly requirements.

- Recent research shows that excessive password requirements (such as including special characters or numbers) tend to cause user frustration and may reduce security.³ Consider adopting password requirements to match guidance from the National Institute of Standards and Technology (NIST) in Special Publication 800-63B, which recommends long, human-friendly, memorable passwords (e.g., sequences of several words).

d. Consider registering your organization for a password breach monitoring service.

- Password reuse is a leading cause of account compromise. Attackers often use breached credentials to attempt to access other services for which the victim may have reused credentials. In addition to encouraging use of password managers to reduce password reuse, organizations should consider monitoring password breaches for exposed employee credentials. Several vendors offer password breach monitoring services and will send notifications to an organization if employee passwords appear in a data breach.

---

IMPLEMENT EMAIL AUTHENTICATION AND OTHER BEST PRACTICES

Implement email authentication and other best practices to reduce attackers' ability to send spoofed phishing emails originating from your organization. For additional guidance, refer to CISA Binding Operational Directive (BOD) 18-01.

a. Enable STARTTLS.
   ➢ When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes on-path attacks more difficult.

b. Disable outdated protocols and ciphers.
   ➢ Ensure that outdated, insecure protocols—such as SSLv2 and SSLv3—as well as 3DES and RC4 ciphers are disabled on mailing servers.

c. Implement SPF and DKIM.4
   ➢ SPF and DKIM allow a sending domain to effectively “watermark” their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect.

d. Configure a DMARC policy of “reject”, if possible, or at minimum, “p=none”.5
   ➢ When an email is received that does not pass an organization’s posted SPF/DKIM rules, DMARC tells the recipient what the domain owner would like done with the message.
   ➢ Setting a DMARC policy of “reject” provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an organization to be made aware of the source of an apparent forgery—information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

SECURE EMAIL GATEWAY CAPABILITIES

Organizations operating their own email gateways should secure email gateways, appliances, and services to intercept phishing emails.

a. Deploy an email filter solution that screens based on headers and malicious content (e.g., infected attachments), categorizes email, inspects Uniform Resource Locators (URLs) against reputation feeds, and has customizable rule-based filters.

b. Strip and/or block emails containing active content (e.g., ActiveX, Java, Visual Basic for Applications [VBA]), or macros) by default. Administrators should allowlist such content only for legitimate reasons.

c. Consider reformatting hyperlinks in the body of email messages by rewriting URLs as plaintext.

d. Deploy sandboxing or detonation chambers to safely isolate malicious links.

e. Ensure detection signatures and blocklists are up to date.

f. Block email beyond a certain size and/or containing attachments that exceed a certain size.
   ➢ Consider legitimate needs to receive large file sizes and limit file size to suit organizational need.

g. Block certain file extensions—including unknown or unused attachments that should not typically be transmitted over email—to prevent vectors such as .scr, .exe, .pif, and .cpl.

---

➢ To the extent feasible, filter out mislabeled file extensions, for example, an executable (.exe) file labeled as a document (.doc) file.

h. Open and analyze compressed and encrypted formats, such as .zip and .rar, that attackers may use to conceal malicious attachments in obfuscated files or information. If unable to open and analyze such content, consider blocking encrypted .zip and other files. However, blocking attachments might keep legitimate files from reaching recipients, which may hinder business functions. Consider using workarounds, such as allowlisting (e.g., trusted senders), to limit negative impacts to operations.

➢ Consider removing the encrypted content from the message and putting it in an out-of-band delivery solution (e.g., web-based portal), replacing the content with a token/link in the original message.

i. Ensure all email gateways, appliances, or services are configured to use only approved Domain Name System (DNS) resolvers and forwarders.

j. Consider implementing warning banners to alert users about emails (particularly those with links and attachments) that originate from outside the organization (place trusted domains on your allowlist to reduce unnecessary implementation).
Creating a strong password is an essential step to protecting yourself online. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime. No citizen is immune to cyber risk, but #BeCyberSmart and you can minimize your chances of an incident.

**SIMPLE TIPS:**

Creating a strong password is easier than you think. Follow these simple tips to shake up your password protocol:

- **Use a long passphrase.** According to NIST guidance, you should consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.

- **Don’t make passwords easy to guess.** Do not include personal information in your password such as your name or pets’ names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

- **Avoid using common words in your passwords.** Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter “A” and an exclamation point (!) can replace the letters “I” or “L.”

- **Get creative.** Use phonetic replacements, such as “PH” instead of “F.” Or make deliberate, but obvious misspellings, such as “enjin” instead of “engine.”

- **Keep your passwords on the down-low.** Don’t tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.

- **Unique account, unique password.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It’s important to mix things up—find easy-to remember ways to customize your standard password for different sites.

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

- **Utilize a password manager to remember all your long passwords.** The most secure way to store all of your unique passwords is by using a password manager. With just one master password, a computer can generate and retrieve passwords for every account that you have— protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions, and more.
NATIONAL CYBERSECURITY AWARENESS MONTH

5 STEPS TO PROTECTING YOUR DIGITAL HOME

More and more of our home devices—including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital home.

SIMPLE TIPS

• **Secure your Wi-Fi Network.** Your home’s wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. For more information about protecting your home network, check out the National Security Agency’s Cybersecurity Information page.

• **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

• **If you connect, you must protect.** Whether it’s your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you’re putting something into your device, such as a USB for an external hard drive, make sure your device’s security software scans for viruses and malware. Finally, protect your devices with antivirus software and be sure to periodically back up any data that cannot be recreated such as photos or personal documents.

• **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the “rule of least privilege” to delete what you don’t need or no longer use. Learn to just say “no” to privilege requests that don’t make sense. Only download apps from trusted vendors and sources.

• **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don’t realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are— and where you aren’t—at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.

For more information about how you can Do Your Part. #BeCyberSmart, visit www.cisa.gov/ncsam