North Star
Small Business Data/Cyber Protection Awareness

Basic Cybersecurity Awareness

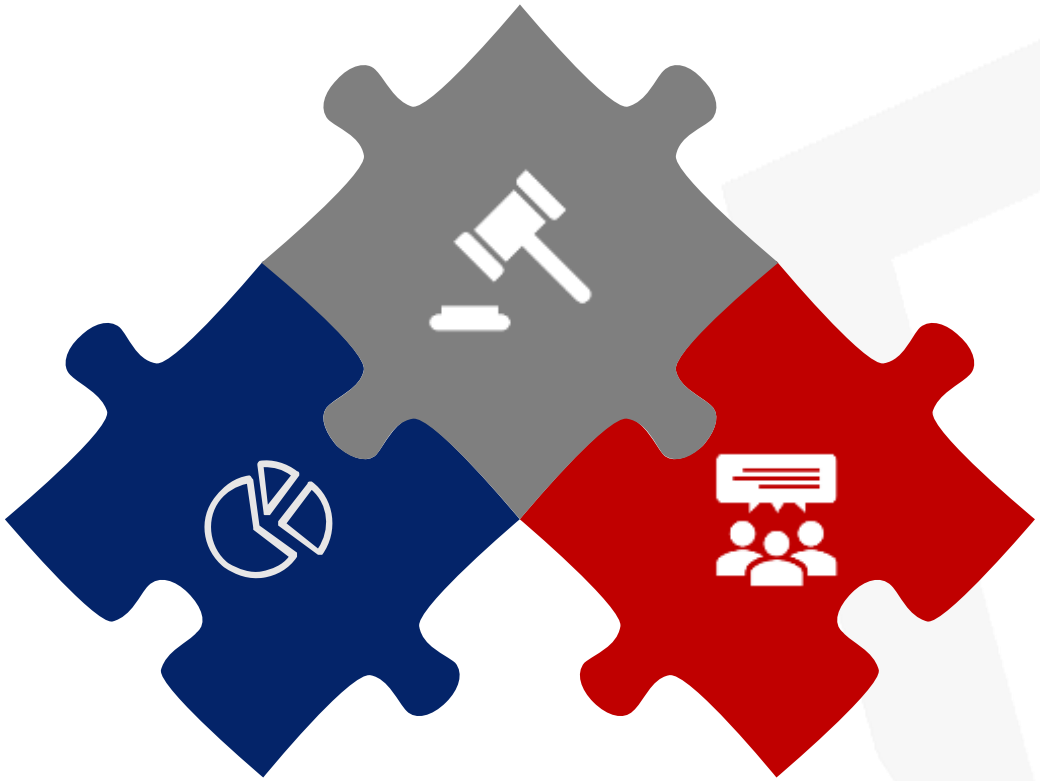
AMERICA'S SBDC

For More information email us at cmmc@AmericasSBDC.org
Or call (703) Nine Eight Nine, Eight Seven Seven Seven

Protecting Critical Confidential Information

All businesses have critical confidential information

- Your own personal info
- Employees
- Clients
- Partners



Why It's Important

- Protect business value
- Creating a competitive advantage
- Reputation protection
- Regulatory requirements

Culture Change

Process implementation, mostly no/low-cost adjustments for basic awareness (CMMC Level 1)

The North Star CMM

Cybersecurity Maturity Model Certification (CMMC)

800-171 NIST

- Core programing built from Cybersecurity Maturity Model (CMMC) while also mapping from other frameworks
- Utilizes the collection of existing frameworks and standards
- Consists of 6 domains

- Access Control
- ID & Authentication
- Media Protection
- Systems & Information Integrity
- System & Communication
- Physical Protection

Primary Considerations

Identify

What information to protect

Protect

Systems and data

Detect

Problems

Respond & Recover

Have a plan ready

Critical Confidential Information

- What is Critical Information?
  - Who, What, When, Where, & How
- Types of Data Classification
  - Restricted, Private, & Public
- Critical Information Example
  - PII – Personal Identity Information
  - CUI – Controlled Unclassified Information
  - FCI – Federal Contract Information
  - HIPPA – Medical Records and Related Data
  - PCI DSS – Credit Card Transaction Data

Critical Confidential Information

What is Critical Information?

Limit the data you collect and only keep it as long as you need it

PII – Personal Identity Information

CUI – Controlled Unclassified Information

FCI – Federal Contract Information

HIPPA – Medical Records and Related Data

PCI DSS – Credit Card Transaction Data

North Star
Small Business Data/Cyber Protection Awareness

Vulnerability

Malicious code is programming that purposefully creates an unauthorized function or process to negatively impact data confidentiality, integrity, or the availability of an information system.

Viruses

Programs designed to damage, steal information, change data, send email, show messages, or any combination of these

Spyware

Programs designed to gather a user's information unknowingly and is usually installed without the user's knowledge.

Trojan Horse

Type of malware made to look like legitimate/real software and used by cyber criminals to get access to your systems.

North Star
Small Business Data/Cyber Protection Awareness

Common Threats

- EMPLOYEES
- RANSOMWARE
- PHISHING
- SOCIAL ENGINEERING
- EMAIL SPOOFING
- BRUTE FORCE

AMERICA'S SBDC

North Star
Small Business Data/Cyber Protection Awareness

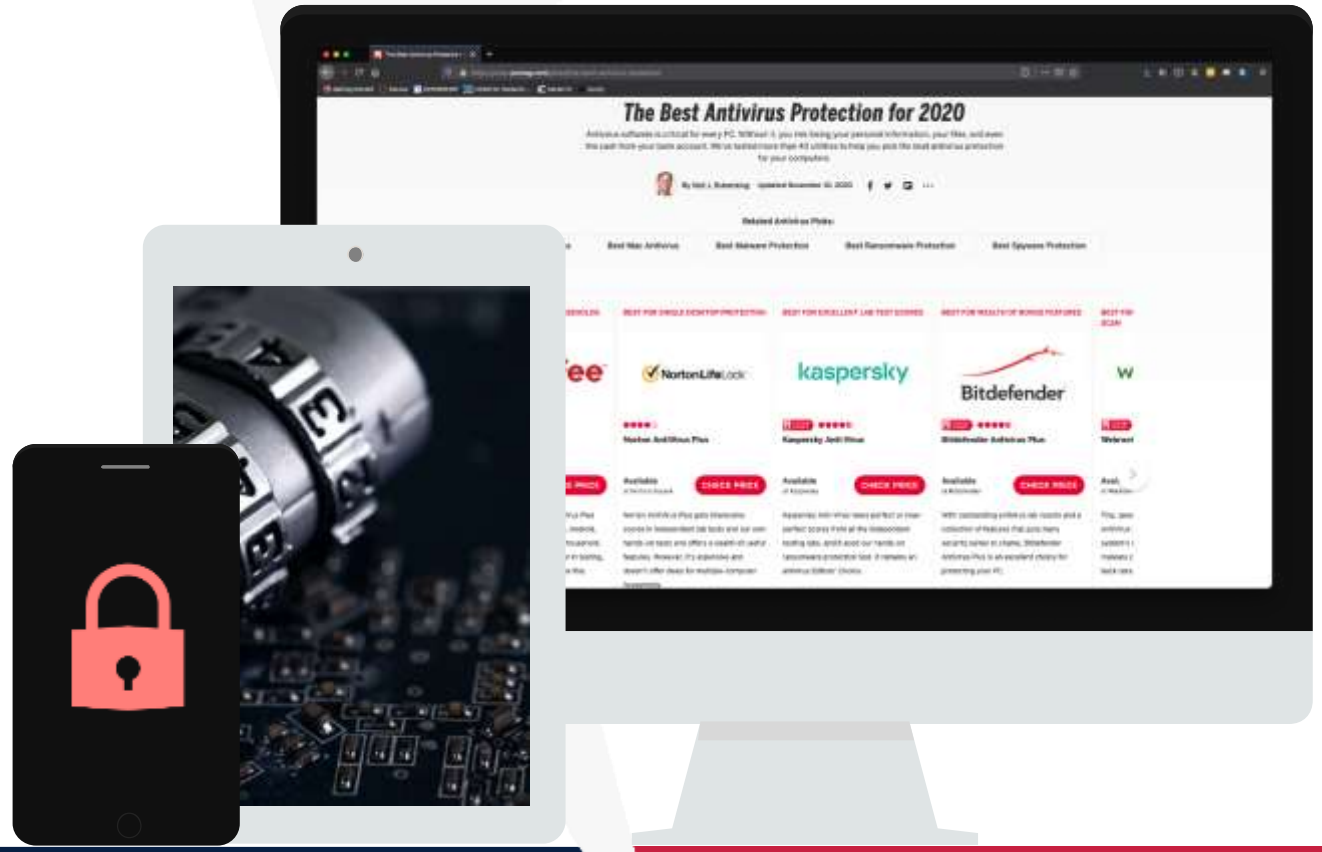
Access Control

AMERICA'S SBDC

North Star
Small Business Data/Cyber Protection Awareness

Access Control

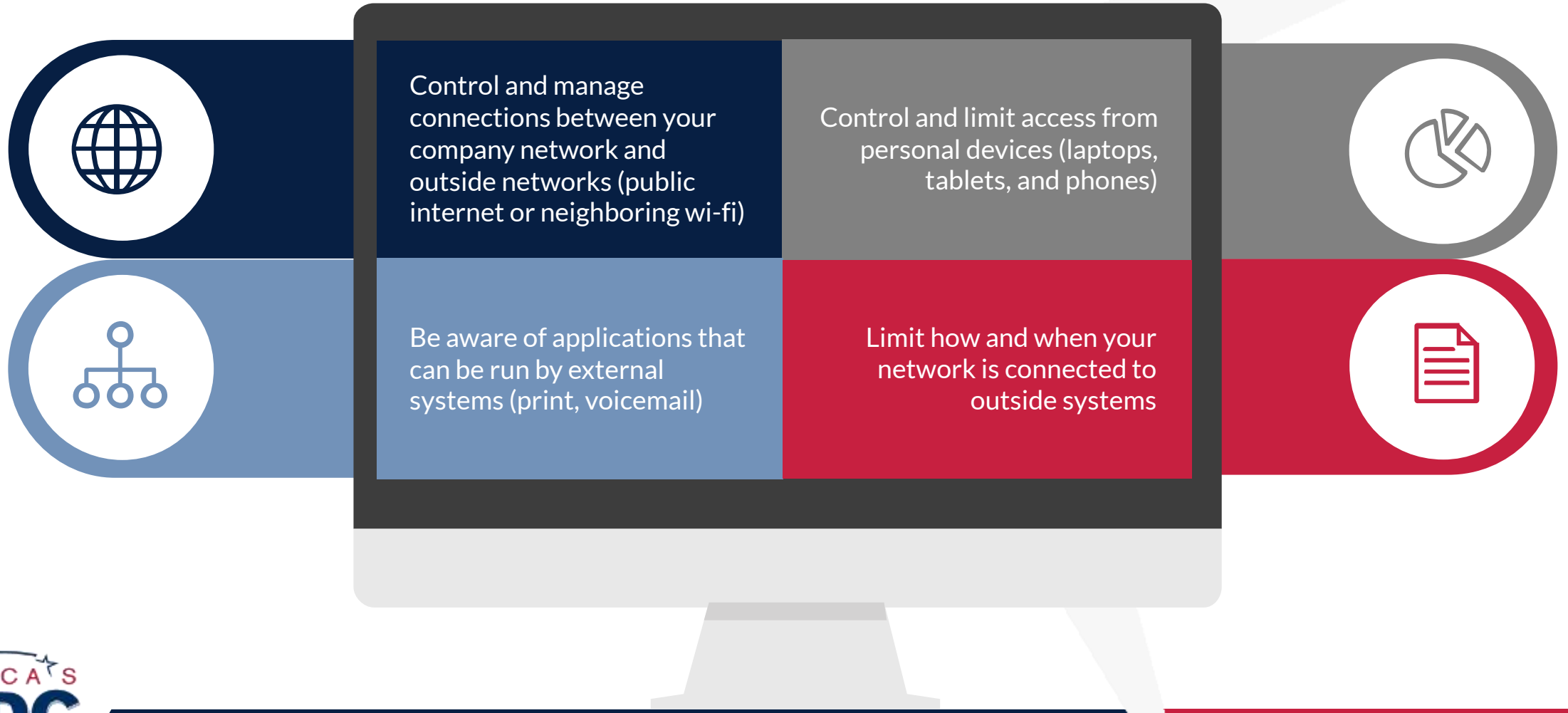
- Establish system access requirements
- Control internal system access
- Control remote system access
- Limit data access to authorized users and process



CONTROL ACCESS TO COMPUTER RESORUCES

- **Control who can use company computers** and who can log on to the company network (internal/external).
- **Limit the services and devices,** like printers, that can be accessed by company computers.
- Set up your systems so **unauthorized users and devices cannot get on the company network.**
- Make sure **to limit users/employees to only the systems, roles, or applications they are permitted to use** and that are needed for their jobs.

Control and Manage Connections



Safeguard Sensitive Information

It is important to **know which users/employees are allowed to publish information** on publicly accessible systems, like a business website.

Limit and control information posted on the company's web properties that can be accessed by the public.

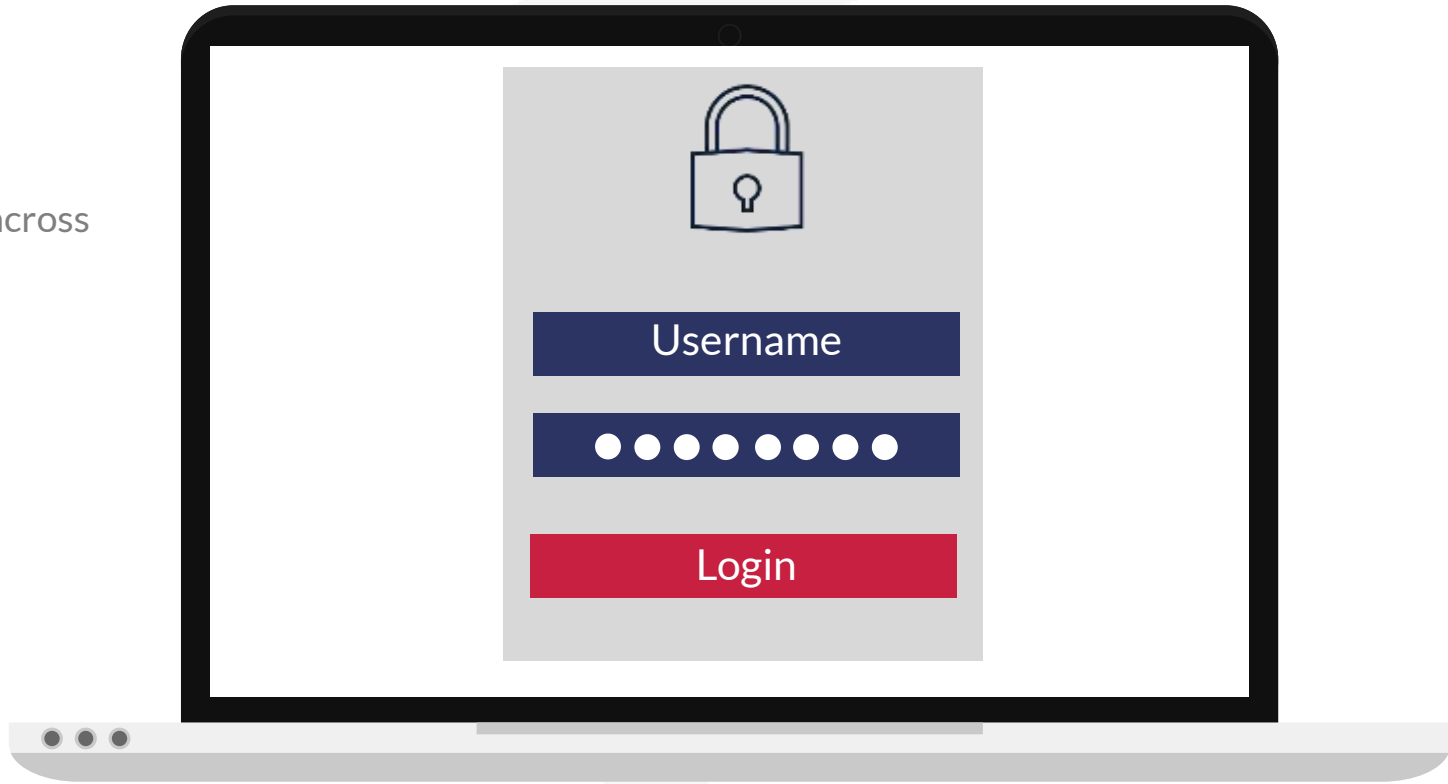
North Star
Small Business Data/Cyber Protection Awareness

Identification & Authentication

AMERICA'S SBDC

Identification & Authentication

- Identify all users on all systems
- Create ability to track users' access across network and devices
- Proper authentication is done when granting a user access to a system
- Use multi-factor authentication wherever possible.



Authenticate

- Authentication helps you to know **who is using or viewing your system**
- Make sure to **assign individual, unique identifiers**, like usernames, to all employees/users who access Company systems
- **Confirm the identities** of users, processes, or devices before allowing them access to the Company's information system-usually done through passwords

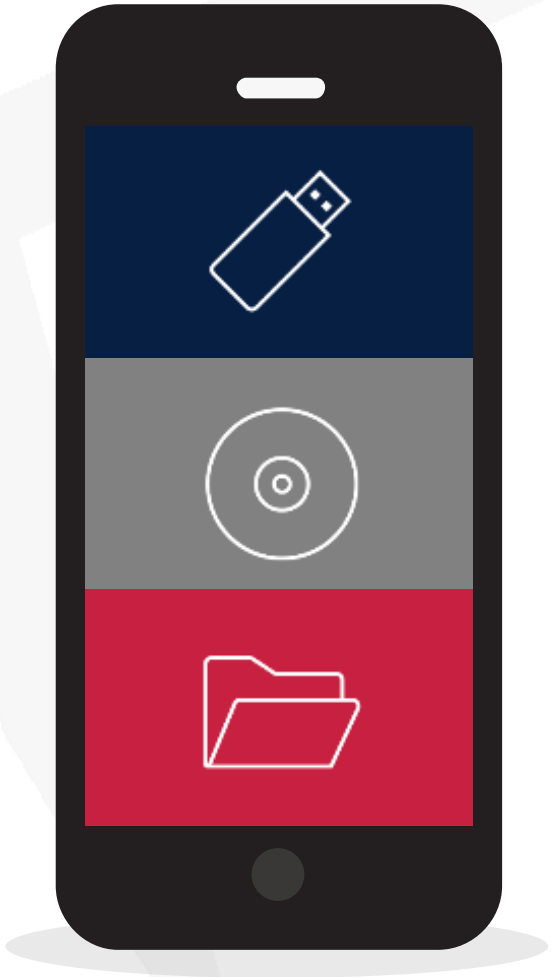
North Star
Small Business Data/Cyber Protection Awareness

Media Protection

AMERICA'S SBDC

Media Protection

- Protect access to all media, both digital and non-digital
- Media includes internal/external hard drives, flash drives, disks, film, paper – anything containing PII
- All media is properly sanitized or disposed of
- Media should be tracked from user to user



North Star
Small Business Data/Cyber Protection Awareness

Physical Protection

AMERICA'S SBDC

Physical Protection

- Protect physical access to all critical information systems
- Controls range from simple door locks to complex redundant infrastructures with guarded access.
- Facilities needing protection include, buildings, rooms, datacenters, offices, and file cabinets

North Star
Small Business Data/Cyber Protection Awareness

CONTROL WHO HAS FACILITY ACCESS

- Do not allow visitors, even those people you know well, to walk around your facility without an escort.
- Make sure that all non-employees wear special visitor badges and/or are always escorted by an employee while on your property.
- Make sure you have a record of who is accessing both your facility (office, plant, factory, etc.) and your equipment.
- Have employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility.

Physical Access Devices

Controlling physical access devices like locks, badging, key cards, etc. is just as important as monitoring and limiting who can physically access certain equipment.

Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.

North Star
Small Business Data/Cyber Protection Awareness

System & Communication

AMERICA'S SBDC

System & Communication

- Involves Physical and virtual controls protecting stored data and data in transit.
- Physically separate data from exposure to external networks.
- Data in transit can be encrypted and transmitted over virtual private networks
- Creating boundaries with firewalls and restricted, monitored network access points

North Star
Small Business Data/Cyber Protection Awareness

System & Communications Protection

Web Proxy

When an employee uses a company computer to go to a website, a web proxy makes the request on the user's behalf, looks at the web request, and decides if it should let the employee go to the website.

Firewall

A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company's network. A firewall stops unwanted traffic on the internet from passing through an outside "fence" to the company's networks and information systems.

Separate Publicly Accessible Systems

- Separate publicly accessible systems from internal systems that need to be protected. Don't place internal systems on the same network as publicly accessible systems.
  - Demilitarized Zones (DMZ) - A DMZ is part of a network put in a "neutral zone" between an organization's internal network (the protected side) and a larger network, like the internet.
    - Boundary Control Devices separate networks (i.e., routers, gateways, firewalls). This can also be done on a separated cloud network
      - Physical separation might involve a separate network infrastructure, dedicated network equipment with separate LAN segments and a firewall between the internal network and the external network.

North Star
Small Business Data/Cyber Protection Awareness

System & Information Integrity

AMERICA'S SBDC

North Star
Small Business Data/Cyber Protection Awareness

Systems & Information Integrity

- Continuous monitoring for unusual activity, malware, and active attacks.
- Antivirus software, network monitoring services and regularly updating software and hardware
- Includes detecting and removing data abnormalities and responding in an appropriate and timely manner
- Reporting and correcting shortfalls within the security infrastructure

AMERICA'S SBDC

Use Anti-Malware Software

Use anti-malware software to scan and identify viruses in your computer systems. Have a plan for how often scans are conducted.

Real-time scans will look at the system whenever new files are downloaded, opened, and saved.

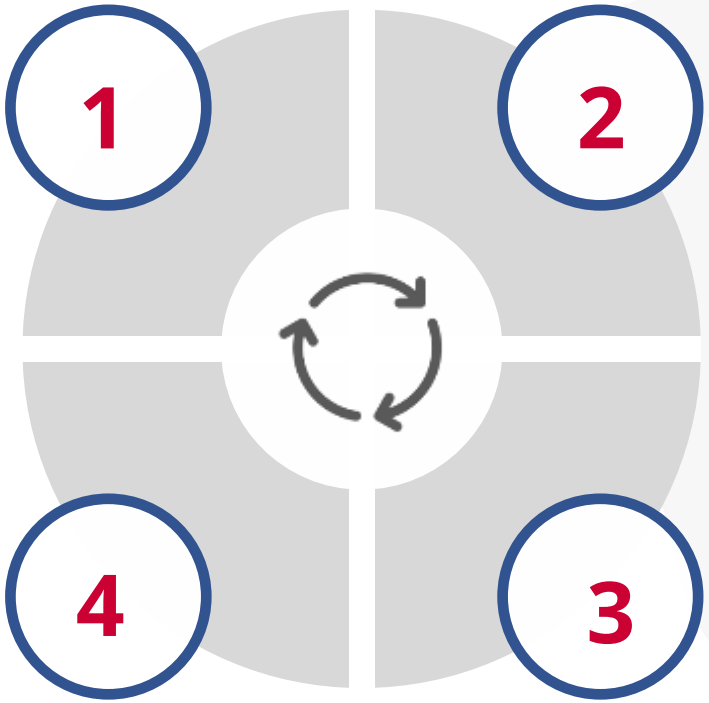
Periodic scans check previously saved files against updated malware information.

Update

- Protect a business by staying up to date on new security releases that stop malicious code and monitor the system regularly.
- Malicious code is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.

Update/Patch Management

All software and firmware have potential flaws. Many vendors work to reduce those flaws by releasing **vulnerability information and updates to their software and firmware**



Have a process to review relevant vendor newsletters with updates about common problems or weaknesses.

After reviewing the information, **execute a process called patch management** that allows for systems to be updated without adversely affecting the organization.

Purchase support from vendors to ensure timely access to updates.

Closing & Review

For More information email us at cmmc@AmericasSBDC.org
Or call (703) Nine Eight Nine, Eight Seven Seven Seven