AMERICA'S SBDC
IN PARTNERSHIP WITH SBA

# Protecting Critical Confidential Information

North Star CMM
Small Business
Data / Cyber Protection

North Star CMM
Small Business
Data / Cyber Protection

# Protecting Critical Confidential Information

The purpose of this document is to help you understand **what needs to be done** to protect critical confidential information so you can better understand how to protect it with help of others.

**All businesses have critical confidential information;** your own, your employees, clients, and partners.

This document follows the model of the CMMC (Cybersecurity Maturity Model) to help understand what needs to be done by utilizing a publicly available **collection of frameworks and standards to protect critical information.** It was created by the Department of Defense for this purpose.

The following slides provide clarifications of **Basic Cyber Hygiene, Level 1.**

North Star CMM
Small Business
Data / Cyber Protection

# OVERARCHING CONSIDERATIONS

Maintain the Confidentiality, Integrity, and Availability of information

- Identify where were and what information you have;
- Protect your systems and data;
- Detect problems;
- Have Response and Recovery plans ready before a breach occurs

While Reading through this deck, please take the time to write down some examples associated with each page that mean something to you.

Tell us what business type you are representing with the example!  Send them to us!

North Star CMM
Small Business
Data / Cyber Protection

# CONTROL ACCESS TO COMPUTER RESOURCES

- **Control who can use company computers** and who can log on to the company network.
- Set up your system so that **unauthorized users and devices cannot get on the Company network**
- **Limit the services and devices,** like printers, that can be accessed by company computers.
- 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

North Star CMM
Small Business
Data / Cyber Protection

- Make sure to **control and manage connections between your company network and outside networks**, such as the public internet or one not belonging to your company.
- Be aware of applications that can be run by external systems.
- **Control and limit personal devices like** laptops, tablets, and phones from accessing your networks and information.
- **Limit how and when your network is connected to outside systems** and/or decide that only certain employees can connect to outside systems from network resources.

North Star CMM
Small Business
Data / Cyber Protection

# DO NOT ALLOW SENSITIVE INFORMATION TO BECOME PUBLIC

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

**Limit and control information posted on your Company's website**(s) that can be accessed by the public.

North Star CMM
Small Business
Data / Cyber Protection

# AUTHENTICATE!

IA.2.076 B-89 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 CMM
Small Business
Data / Cyber Protection

# GRANTING ACCESS

Before you let a person or a device have access to your system, you need to verify that the user or device is who or what it claims to be.

**This verification is called authentication**. The most common way to verify identity is using a username and a hard-to-guess password

Some devices ship with default usernames and passwords. For example, some devices ship so that when you first logon to the device, the username is “admin” and the password is “admin””.

When you have devices with this type of default username and password, **you need to change the default password** to a unique password you create. Default passwords are well known to the public, and easily found in a search.

So, these default passwords would be easy for an unauthorized person to guess and use to gain access to your system.

North Star CMM
Small Business
Data / Cyber Protection

# SANITIZE MEDIA BEFORE DISPOSING OR REUSE

Media can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones.

It is important to see what information is on these types of media.

If there is client contract information your Company got doing work for a client that is not shared publicly, you or someone in your Company should do one of two things before throwing the media away:

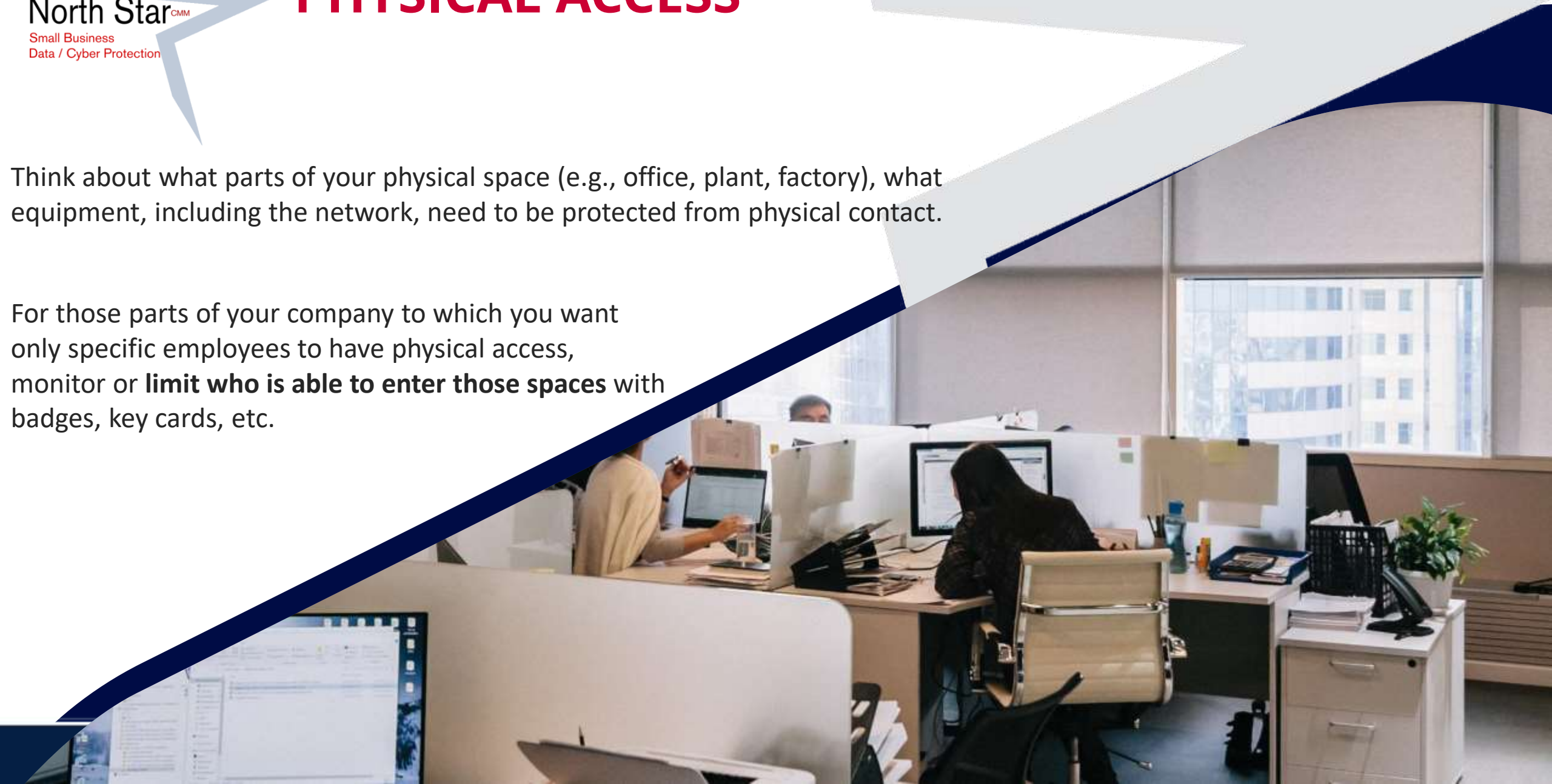
**Clean or purge the information,** if you want to reuse the device, or **shred or destroy the device** so it cannot be read.

North Star CMM
Small Business
Data / Cyber Protection

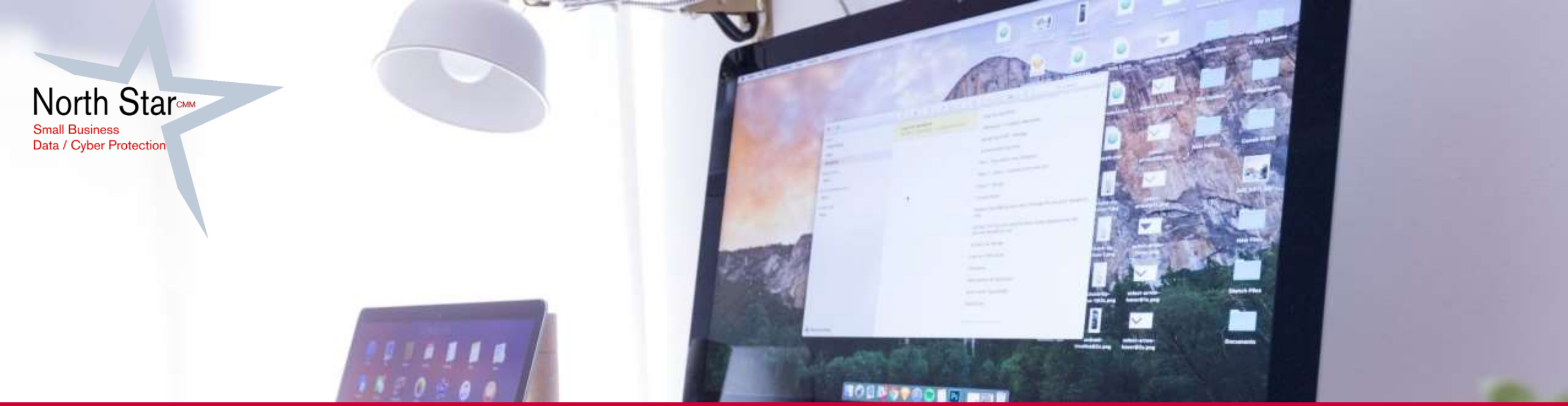
# PHYSICAL ACCESS

Think about what parts of your physical space (e.g., office, plant, factory), what equipment, including the network, need to be protected from physical contact.

For those parts of your company to which you want only specific employees to have physical access, monitor or **limit who is able to enter those spaces** with badges, key cards, etc.



North Star CMM
Small Business
Data / Cyber Protection



# CONTROL WHO HAS ACCESS TO FACILITY

- **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.
- You can do this in writing by having 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 CMM
Small Business
Data / Cyber Protection

North Star CMM
Small Business
Data / Cyber Protection

# SYSTEM and COMMUNICATIONS PROTECTION

Just as your business has fences and locks for protection from the outside and uses badges and keycards to keep non-employees out, your Company's IT network or system has boundaries that must be protected.

**Many companies use a web proxy and a firewall.**

## 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.

If your Company is large enough, monitor, control, or protect one part of the Company enterprise/network from the other. This can also be done with a firewall. Do this to stop adversaries, hackers, or disgruntled employees from entering your network and causing damage.

# 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 the publicly accessible systems.

A network or part of a network that is separated (sometimes physically) from an internal network is called a demilitarized zone (DMZ). A DMZ is a host or 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.

To separate a subnetwork physically, your business may **put in boundary control devices** (i.e., routers, gateways, firewalls). This can also be done on a cloud network that can be separated from the rest of the network.

A DMZ can add an extra layer of security to your business's LAN, because an external network node can reach only what is permitted to be accessed in the DMZ.

Physical separation **might involve a separate network infrastructure, dedicated network equipment with separate LAN segments and a firewall between the internal network** and the DMZ segment and a firewall between the DMZ segment and the internet. A logical separation might involve VLAN separation for the DMZ supporting a separate subnet with routing and access controls between subnets.

North Star CMM
Small Business
Data / Cyber Protection

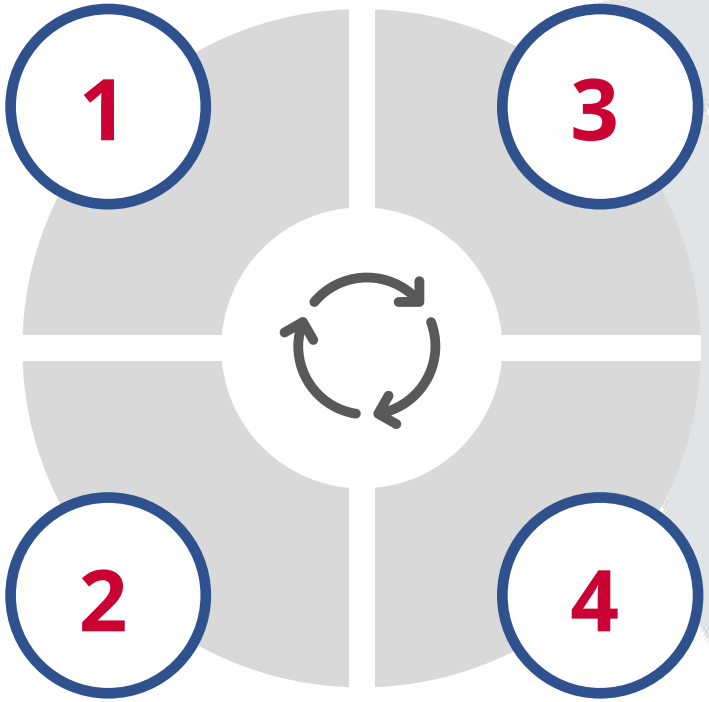
# PATCH MANAGEMENT

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**

1

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

2



3

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

4

**Purchase support from their vendors** to ensure timely access to updates.

North Star CMM
Small Business
Data / Cyber Protection

# VULNERABILITY

Protect your valuable IT system by stopping malicious code at designated locations in your system.

Malicious code is program code that **purposefully creates an unauthorized function or process that will have a negative impact** on the confidentiality, integrity, or availability of an information system.

A designated location may be your network device or your computer.

**Malicious code includes the following**, which can be hidden in email, email attachments, web access:

- **Viruses, programs designed to damage**, steal information, change data, send email, show messages, or any combination of these things.
- **Spyware, a program designed to gather information about a person's activity** in secret and is usually installed without the person knowing when they click on a link.
- A Trojan Horse, **a type of malware made to look like legitimate/real software** and used by cyber criminals to get access to a business's systems.

By using anti-malware tools, you can stop or lessen the impact of malicious code.

# UPDATE

Protect your business **by staying up to date on new security releases t**hat stop malicious code and monitoring the system regularly.

Malicious code is program code that is always changing, so it is important to **always have up-to-date protections, such as anti-malware tools.**

North Star CMM
Small Business
Data / Cyber Protection

# 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.

North Star CMM
Small Business
Data / Cyber Protection

North Star CMM
Small Business
Data / Cyber Protection

AMERICA'S SBDC
IN PARTNERSHIP WITH SBA

www.AmericasSBDC.org

charlie.tupitza@AmericasSBDC.org 703 989-8777