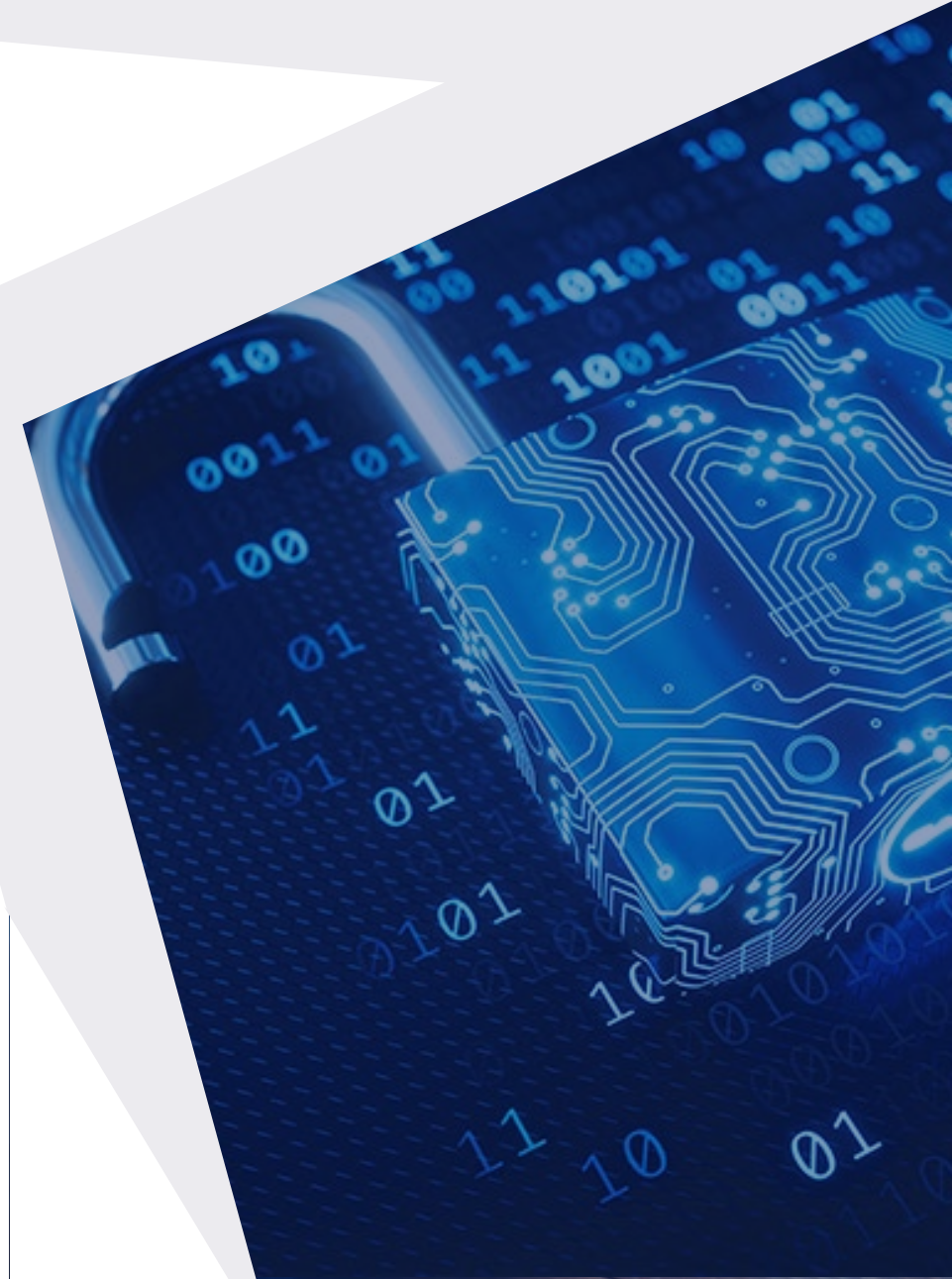


Spring Into Cybersecurity & Data Protection Awareness



Learning Objectives

- 01 Understanding Cyber Threats
- 02 Developing a Cybersecurity Plan
- 03 Implementing Effective Security Measures
- 04 Training Employee's and Meeting Requirements



Data Protection for A Secure Business



Common Threats To Small Businesses



Data Breaches



Phishing Attacks



Malware & Ransomware



Insider Threats



Social Engineering

Top 4 Cybersecurity Topics



Encryption



Password Management



Two-Factor Authentication



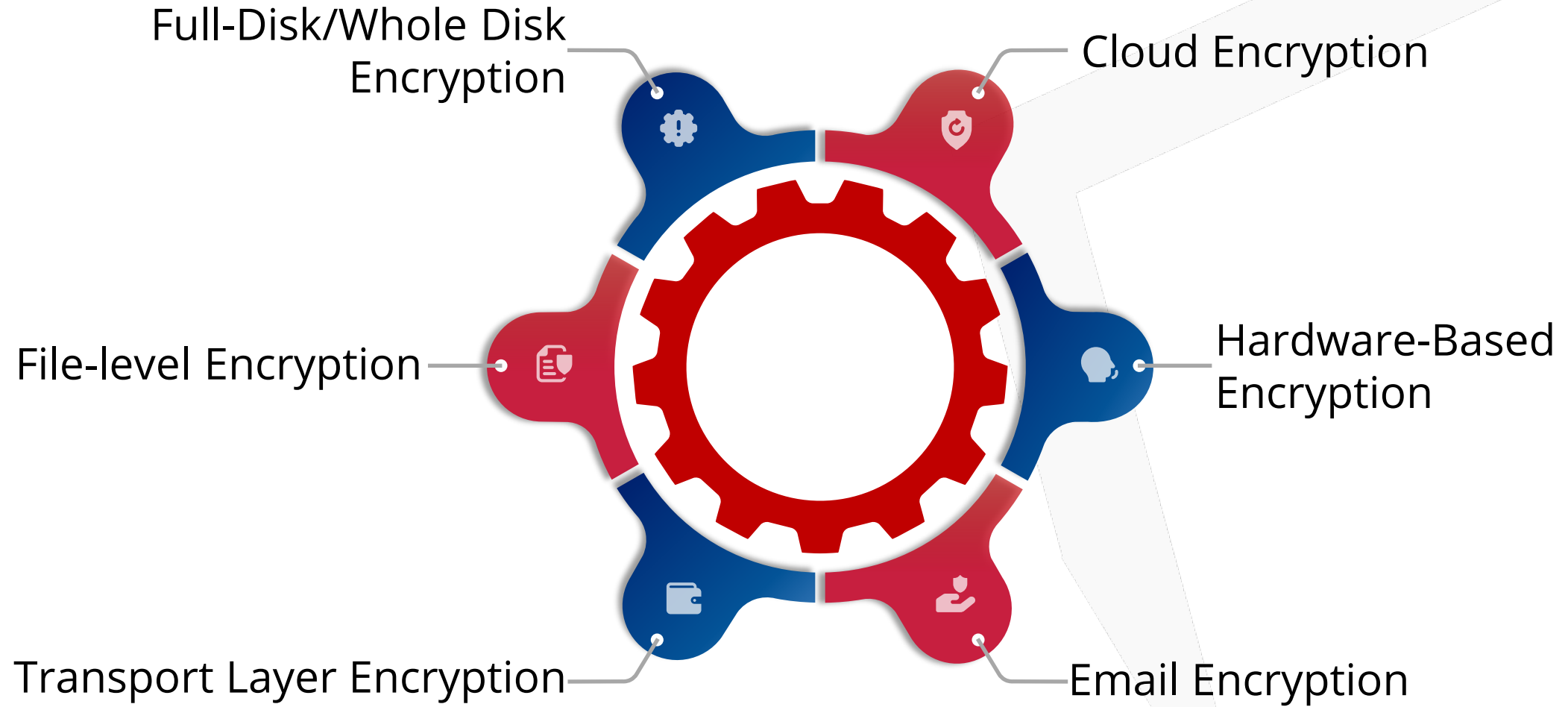
Threat Detection



What is Data Encryption

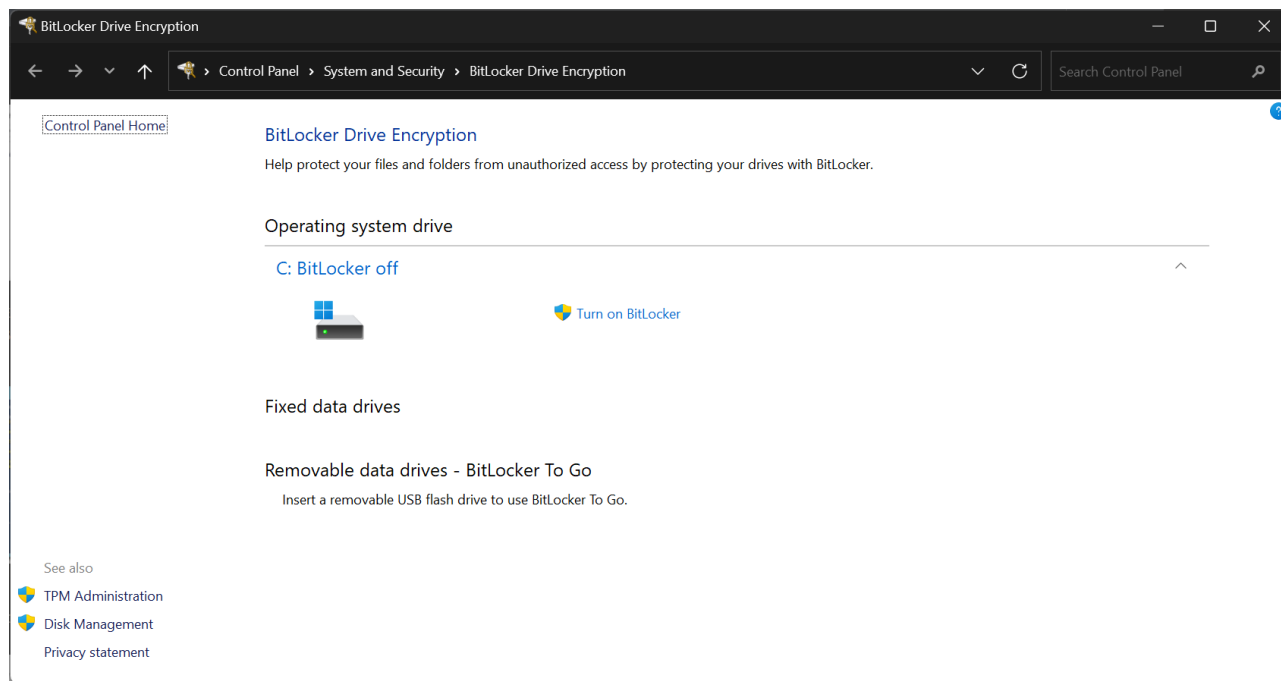


Encryption By Application

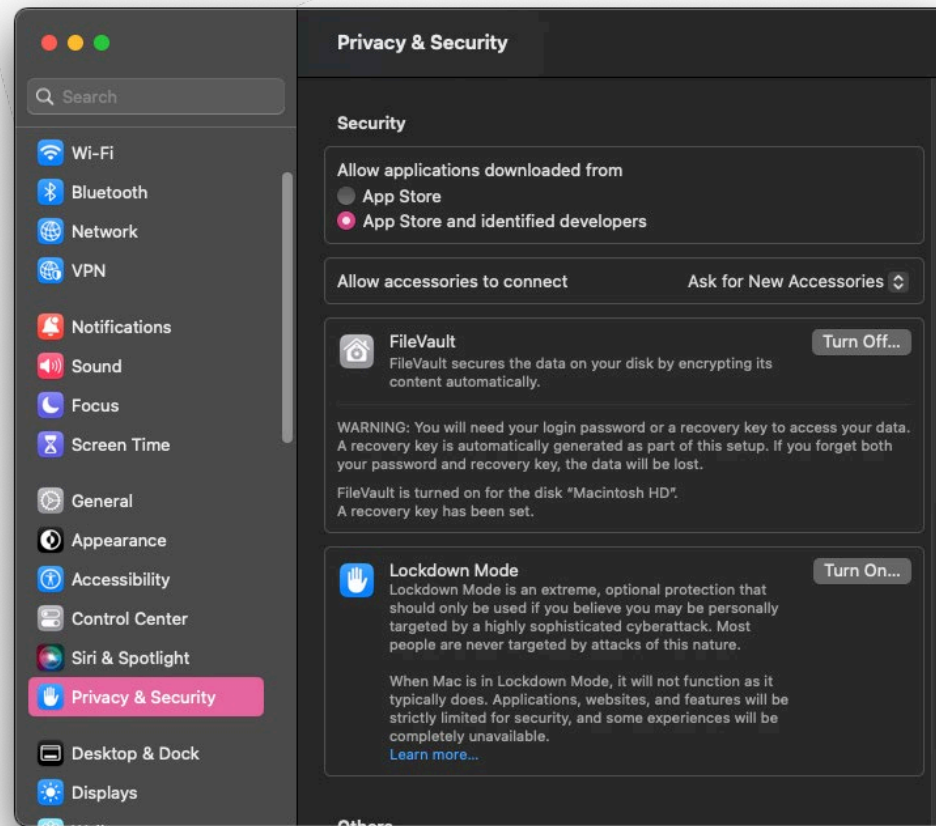


Encryption Samples

Windows



macOS



Encryption Resources

Full-Disk:

- ✓ BitLocker for Windows
- ✓ FileVault for macOS

File-Level:

- ✓ VeraCrypt
- ✓ Encrypting File System (EFS) in Windows

Hardware-Based:

- ✓ TPM Chip
- ✓ Self-Encrypting Drives
- ✓ Secure USB Devices
- ✓ Apple Silicon

Why Do Password Managers Matter?





Characteristics of Strong Passwords

Most Commonly used Passwords:

- "123456"
- "admin"
- "12345678"
- "password"

Uniqueness:
Different Passwords Per Account

Unpredictability:
Avoid Common Words

Length:
At least 12 Characters

Complexity:
Upper, Lower, Numbers, Symbols

96% of the most common passwords can be cracked in less than one second

Password Managers

A Password Manager is designed to securely store and encrypt user passwords. They allow users to create and manage unique, strong passwords for different accounts without the need to remember each one.



Benefits of Password Managers:

- Enhanced Security
- Encryption
- Auto-Fill
- Synchronization
- Regular Updates





Knowledge
Factor



Possession
Factor



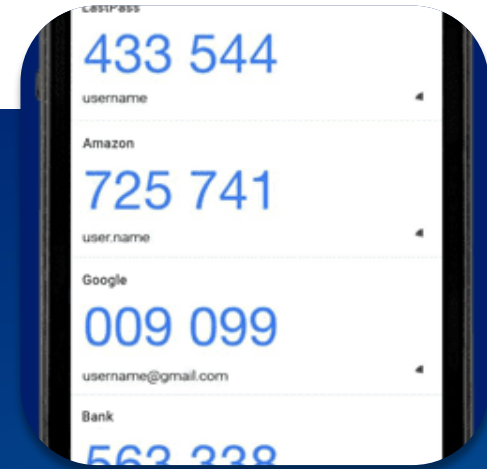
Inherence
Factor

Multi-Factor Authentication

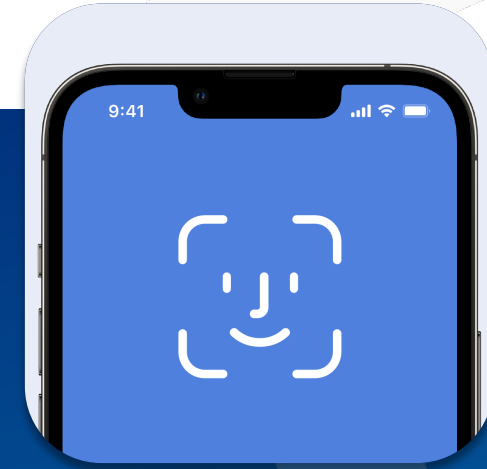
Types of Multi-Factor Authentication (MFA)



SMS-Based MFA



App-Based MFA



Biometric MFA



Hardware Token

Multi-Factor Authentication Samples



Google

Allow 2-Step Verification

1. Open your [Google Account](#) .
2. In the navigation panel, select **Security**.
3. Under “How you sign in to Google,” select **2-Step Verification** > **Get started**.
4. Follow the on-screen steps.

Facebook

Turn on or manage two-factor authentication

1. Click on your profile picture in the top right, then click  **Settings and privacy**.
2. Click  **Settings**.
3. Click **Accounts Center**, then click **Password and security**.
4. Click **Two-factor authentication**, then click on the account that you'd like to update.
5. Choose the security method you want to add and follow the on-screen instructions.

When you set up two-factor authentication on Facebook, you'll be asked to choose one of three security methods:

- Tapping your [security key](#) on a compatible device.
- Login codes from a [third party authentication app](#).
- [Text message \(SMS\) codes](#) from your mobile phone.

Once you've turned on two-factor authentication, you can get 10 recovery login codes to use when you're unable to use your phone. Learn how to [set up recovery codes](#).

Password Resources

- ✓ [CISA - Strengthen Passwords with Three Simple Tips \(infographic\)](#)
- ✓ [CISA - Stop Online Crime with Strong Passwords \(video\)](#)
- ✓ [Multi-Factor Authentication \(NIST\)](#)
- ✓ [CISA - Secure Our World MFA Tip Sheet](#)
- ✓ [CISA - Require Strong Passwords](#)
- ✓ [Cyber Readiness Institute: Poster-Use-Better-Passwords](#)
- ✓ [GCA Toolkit: Beyond Simple Passwords - MFA \(video\)](#)

Password Management

- ✓ [Bitwarden](#)
- ✓ [Keeper](#)
- ✓ [1Password](#)

- ✓ [Dashlane](#)



What is Antivirus



Choosing the Right Antivirus Software

Comprehensive
Protection

Ease of Use

Performance
Impact

Customer
Support

Compare
Functionality

Best Practices for Using Antivirus Software



Regular Updates & Patches



Scheduled Scans



Combine with other Security Measures



Monitoring & Managing

Ransomware & Antivirus Resources

- ✓ [America's SBDC - Ransomware Overview](#)
- ✓ [NIST - Getting Started with Cybersecurity Risk Management: Ransomware Quick Start Guide](#)
- ✓ [NIST - Small Business Cybersecurity Corner: Ransomware](#)
- ✓ [Microsoft - Vulnerability Management](#)
- ✓ [FTC - Cybersecurity/ransomware](#)
- ✓ [FBI - IC3 Ransomware Fact Sheet.pdf](#)
- ✓ [Nessus Vulnerability Scanner](#)
- ✓ [Qualys Vulnerability Management](#)

✓ [CrowdStrike](#)

✓ [Bitdefender](#)

✓ [Norton Small Business](#)

✓ [Trend Micro Business](#)

Thank You!

