# Cyber Security

## For Small Businesses

**Identify Protect Detect Respond Recover**

**1. Identify**

- ✓ **What needs protection in your business**
- ✓ **Common cyber attacks that may be used against your business**
- ✓ **The risks and costs of not being prepared for a cyber attack**

**2. Protect**

- ✓ **Train your employees to make smart decisions on electronic devices**
- ✓ **Use firewalls, encryption and strong passwords**
- ✓ **Actively assess and manage cyber risk**

**3. Detect**

- ✓ **Implement company policies**
- ✓ **Buy and regularly update antivirus software**
- ✓ **Teach employees to recognize cyber attacks**

**4. Respond**

- ✓ **Develop an Incident Response Plan**
- ✓ **Do a simple and low cost risk assessment for your business**
- ✓ **Actively manage your business's security risks**

**5. Recover**

- ✓ **Learn how to limit the time and money spent on the recovery process**
- ✓ **Get rid of all traces of malicious code and make sure systems are secure**

✓ **Contact the proper authorities**

U.S. Small Business Administration

# 14 Tips to Protect Your Business from Ransomware Attacks

Ransomware attacks are the fastest growing malware threats. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Ransomware, a type of malicious software that infects and restricts access to a computer until a ransom is paid, affects businesses of all sizes. The good news is that there are best practices you can adopt to protect your business.

1. **Implement an awareness and training program**. Because end users are targets, employees should be aware of the threat of ransomware and how it is delivered.
2. **Enable strong spam filters to prevent phishing emails** (an attempt to obtain sensitive information electronically) from reaching employees and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
3. **Scan all incoming and outgoing emails** to detect threats and filter executable files (used to perform computer functions) from reaching employees.
4. **Configure firewalls to block access** to known malicious IP addresses.
5. **Patch operating systems, software, and firmware on devices**. Consider using a centralized patch management system.
6. **Set anti-virus and anti-malware programs to conduct regular scans automatically**.
7. **Manage the use of privileged accounts** based on the principle of least privilege: no employees should be assigned administrative access unless absolutely needed and those with a need for administrator accounts should only use them when necessary.
8. **Configure access controls**—including file, directory, and network share permissions— with least privilege in mind. If an employee only needs to read specific files, the employee should not have write access to those files, directories, or shares.
9. **Disable macro scripts** (tool bar buttons and keyboard shortcut) from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
10. **Implement Software Restriction Policies** (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
11. **Consider disabling Remote Desktop protocol** (RDP) if it is not being used.
12. **Use application whitelisting**, which only allows systems to execute programs known and permitted by security policy.
13. **Execute operating system environments** or specific programs in a virtualized environment.

14. **Categorize data** based on organizational value and implement physical and logical separation of networks and data for different organizational units.