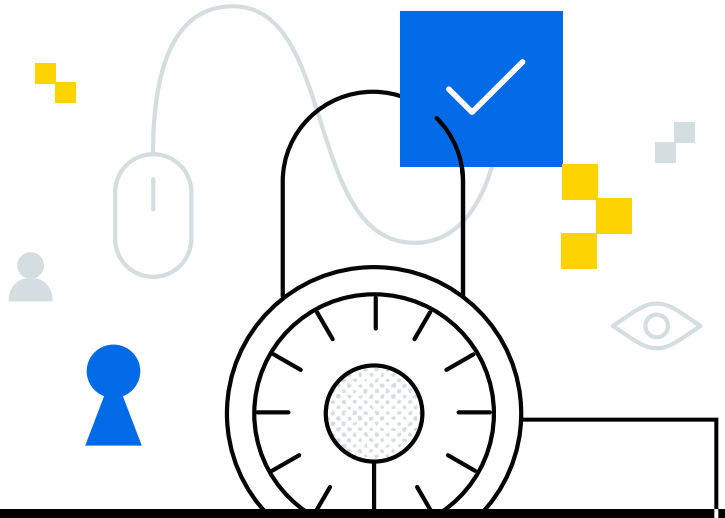
# Cybersecurity Checklist



Every password we set, service we use, and network we access leaves us exposed and vulnerable to cyber threats. We worked closely with our in-house security experts to put together a checklist of simple (low-cost and free) steps you can take to secure your business.

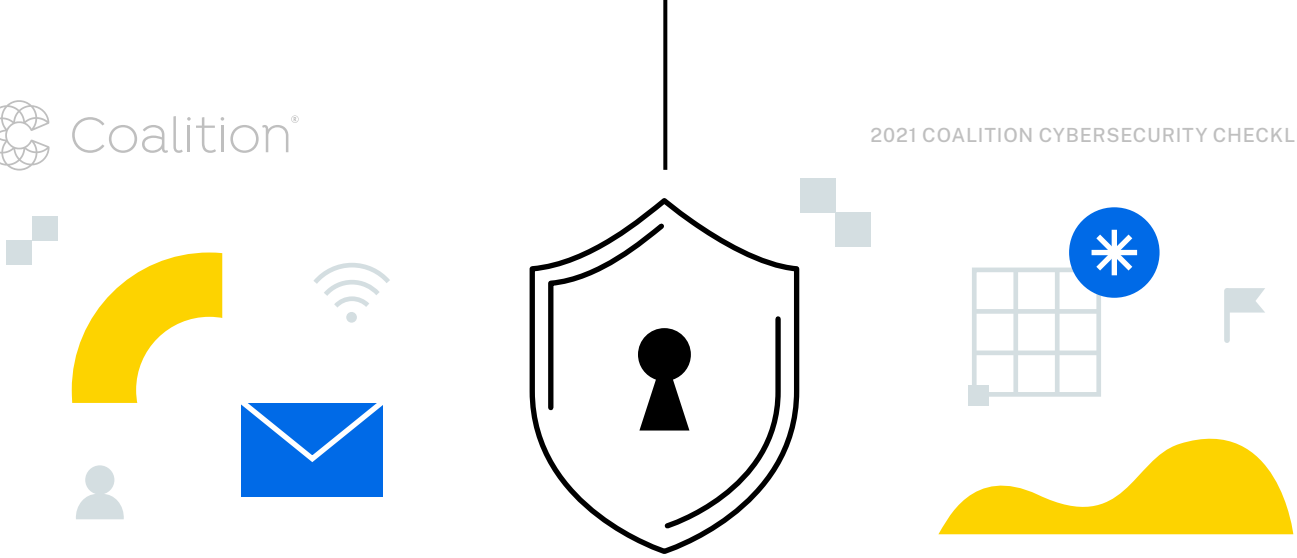
Use this checklist to think critically about cybersecurity and explore new ways to keep your business safe.

**Ransomware attacks**
A bad actor encrypts and disables access to business-critical systems and data until a ransom payment is made. Data may also be exfiltrated and exposed if the ransom isn't paid.

**Funds transfer fraud**
A bad actor uses social engineering, sometimes in concert with phishing attacks, to divert funds to the attacker instead of the proper recipient.

**Business email compromise**
Email intrusion resulting from spoofing, phishing, or spear phishing can result in a data breach, funds transfer loss, or escalate to ransomware and other attacks.

Implementing the tips in this checklist can help you prevent most claims. Phishing, remote access, and social engineering attacks accounted for 89% of all known attack techniques Coalition saw in the first half of 2020.



## 01. Increase email security

Despite popular belief, email is not a secure form of communication, and every organization should use caution when sending or verifying sensitive information by email.

- [ ] Turn on **Multi-factor Authentication (MFA)** for email access. Approximately 80% of email intrusion incidents happen because of weak or stolen passwords.
- [ ] Implement protocols to protect the integrity of your email, including Sender Policy Framework (**SPF**), DomainKeys Identified Mail (**DKIM**), and Domain-based Message Authentication, Reporting, and Conformance (**DMARC**).

## 02. Implement Multi-factor Authentication (MFA)

MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application. Start with your email, then apply MFA everywhere it's available.

- [ ] Select an MFA app or solution that meets your business needs and turn on MFA for existing tools and devices that offer it. **Note:** MFA services that use SMS (text messages) are less secure than proper mobile applications or token generators. In this case, you should also set up MFA with your mobile carrier.
- [ ] Turn on MFA through the Google Suite Admin console (called 2-Step Verification) or Microsoft Office 365 portal.

## 03. Maintain full data backups

A full data backup can mean the difference between a complete loss and a complete recovery after a ransomware attack. You'll need to develop a strategy tailored to your business.

- [ ] Maintain backups both **on and off-site** for critical business data. 'Off-site' means on a network (or totally offline) where a malicious actor can not gain access.
- [ ] Test your backups by trying a full recovery to make sure you have what you need if an incident occurs.

## 04. Enable secure remote access

Remote work is more necessary than ever before, which means workers are no longer in controlled work environments. Instead, they are often given access to company resources remotely. When remote access is allowed, your organization takes on additional risks.

- [ ] If your business has moved to cloud-based resources like Microsoft 365 (formerly Office 365), Google Apps, and Salesforce, ensure that access is secured with MFA, strong passwords, and the highest level of encryption supported (HTTPS and TLS 1.1 or above).
- [ ] If your business has on-site (on-prem) infrastructure, ensure that access is secured with MFA and strong passwords. Additionally, it is a best practice to provide access to information systems using a VPN rather than exposing them to direct Internet access.
- [ ] If possible, require remote users to use company-provided hardware that has been secured to your company standards.
- [ ] Limit authorization and review authorizations for remote access regularly.

## 05. Update your software regularly

All software presents at least some risk to your organization. Cybercriminals look for vulnerabilities, which you can easily locate and prevent through regular software updates.

- [ ] Consistently update your operating system, software, servers, and applications.



## 06. Use a password manager

Password managers help keep track of multiple passwords and generate new ones at random. They are essentially an encrypted vault for storing passwords that are protected by one master password. These master passwords act as ‘keys to the kingdom’ and should be heavily protected.

- [ ] Select a password manager solution that meets your budgetary and usage needs
- [ ] Introduce the tool to your company and train them on password best practices
- [ ] Create a password policy in writing that is easy to understand and access

## 07. Scan for malicious software

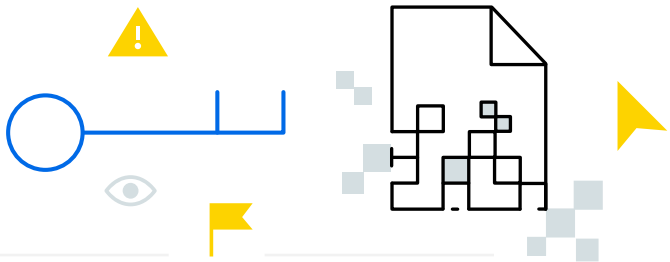
Endpoint detection and response (EDR) tools (including traditional antivirus and anti-malware software) readily identify, detect, and prevent advanced cyber threats.

- [ ] Implement an EDR tool that is active 100% of the time and pushes notifications when threats are detected. Turn on alerts for when EDR has been disabled, which is a common tactic for attackers.

## 08. Encrypt your data

Encryption is a process that renders data inaccessible to bad actors who manage to steal it unless they possess the key required to access it. If your data is not encrypted and you lose a device, your organization may face a data breach and all of the legal, regulatory, and notification costs that come with it.

- [ ] Encrypt data on all business-related devices (mobile phones, computers, etc.)



## 09. Set up a security awareness training program

We've found that 60% of claims are the result of *human error*. This can be avoided by creating a culture of cyber risk awareness that holds everyone accountable.

- [ ] Create or select a cybersecurity awareness training program that includes hands-on activities, presentations, and documentation that is easy to understand and access.



## 10. Purchase cyber insurance

Organizations can never be 100 percent secure, and if the worst happens, you want to make sure your organization is prepared to recover.

- [ ] Sign up for a Coalition Risk Assessment to understand your specific risks.
- [ ] Buy a cyber insurance policy that meets your unique business needs.

For more detailed explanations of each section of this checklist, including vetted vendor recommendations, download the *2021 Coalition Cybersecurity Guide*. If you have any questions, feel free to reach out to our team of in-house experts. We're happy to help!