



2021 Coalition

# Cybersecurity Guide

# 2021 Coalition Cybersecurity Guide

As small and midsize businesses become increasingly dependent on services and applications connected to the internet, they also become a larger target for cyber criminals looking to exploit vulnerabilities in their systems. Every password we set, tool we use, and network we access leaves us exposed and vulnerable to cyber threats.

At Coalition, we have a unique up-close view of the attacks that impact organizations. We've seen the frequency, severity, and sophistication of cyber attacks continue to grow. From 2019 to 2020, we saw a 67% increase in the frequency of business email compromise attacks. In the first half of 2020 alone, we witnessed a 47% increase in the average ransom demand. And while many attackers exploit misconfigured security settings and software vulnerabilities, 60% of claims we saw resulted from *human error*.

This guide is designed for small businesses who want specific and actionable recommendations to protect their organization. According to the Global Cyber Alliance, more than [43% of cyber attacks](#) target small businesses, who often don't have the security and technical expertise of larger organizations. Luckily, we have a powerful team of in-house experts who are ready to share actionable steps to help prevent (or at least minimize) cyber threats.

*Addressing these areas of security will help you mitigate cyber risk, but they can't guarantee you won't be a target. All recommendations are in alphabetical order. If you're looking for more detailed cybersecurity advice, [reach out to our team](#), and they will be happy to assist.*



# Common cyber claims

**Ransomware and malware 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 cause funds to be sent to the attacker instead of the proper recipient

**Business email compromise**

Email intrusion resulting from spoofing, phishing, or spear phishing that can result in a data breach or funds transfer loss

**Data breaches**

Exposure of Personally Identifiable Information (PII) or Protected/ Personal Health Information (PHI) of your customers

**Legal and regulatory issues**

Violation of a legal or regulatory framework, such as GDPR or CCPA

**Web application compromise**

Direct compromise of a web-based product, such as an ecommerce platform, as a result of a targeted attack

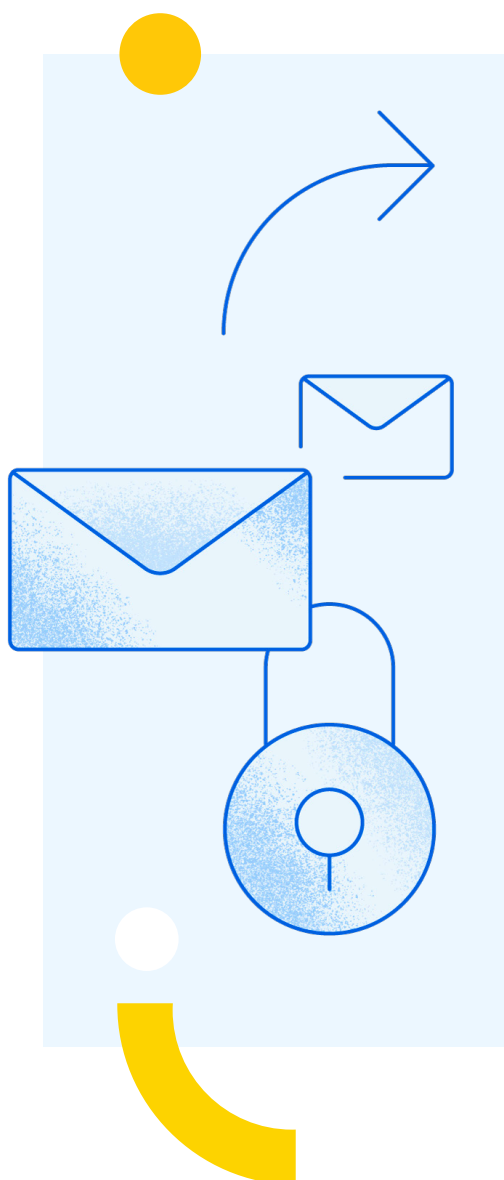
**Technology errors & omissions**

A failure in the technology product or services results in business interruption or loss on behalf of your customers

# Table of Contents

<b>5</b>	Increase email security
<b>7</b>	Implement Multi-factor Authentication (MFA)
<b>8</b>	Maintain good data backups
<b>9</b>	Enable secure remote access
<b>10</b>	Update your software
<b>11</b>	Use a password manager
<b>12</b>	Scan for malicious software
<b>13</b>	Encrypt your data
<b>14</b>	Implement a security awareness training program
<b>15</b>	Purchase cyber insurance

# Increase email security



One thing we all have in common is our use of email to communicate, both in our personal and professional lives. 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.

According to our data, an attack on your business email (also known as business email compromise, or BEC) was the initial point of entry for 54% of the claims reported to us and resulted in a wide variety of incidents, including funds transfer fraud, ransomware, and data breaches. There are a number of cybersecurity measures your company can take to protect your business and decrease the chances of experiencing a cyber attack.

## Things to consider

Our data shows that the likelihood an organization experiences a BEC is related to their email provider choice. Coalition policyholders who used Microsoft 365 were more than **three times** as likely to report a business email compromise than our policyholders that used Google Gmail. Despite the increased risk, both email providers are good options if all security protocols available are put in place.

## Vendor recommendations

### Email Hosting Provider

a platform that manages (aka “hosts”) your email

- Google Workspace (formerly G Suite)
- Microsoft 365

### Mail Proxy

a mail proxy sits in front of an ESP to filter out malicious emails

- Mimecast
- Proofpoint

## Free security measures to implement with any email provider:

### Sender Policy Framework (SPF)

SPF is a simple record you can add to your domain name system (DNS) server that specifies what mail servers are allowed to send email for your domain. SPF helps to ensure that someone cannot create an email server and send it from your domain unless you have authorized them to do so in your DNS records.

- SPF is defined in a simple TXT record. You'll want to check with your email provider for the proper settings, as well as every provider that you allow to send email on your behalf.
- You can simply create a new TXT record and add the allowed servers to the list.
- Example SPF TXT record: `v=spf1 include:spf.protection.outlook.com -all`. The first part (spf1) means you are using SPF version 1, the middle part means you allow the server 'spf.protection.outlook.com' to send email for your domain, and the last part means 'all' indicates what policy should be applied when ISPs detect a server that is not listed in your SPF record. The '-all' signifies that unauthorized servers will be rejected from sending mail.

### DomainKeys Identified Mail (DKIM)

DKIM ensures that emails sent to and from your mail server haven't been altered in transit. This prevents man-in-the-middle style attacks on your email. DKIM is configured through your mail provider and is free.

- To enable DKIM, you need to generate encryption keys and place those keys in your DNS. Your mail service provider will have precise instructions on how to do that.

### Domain-based Message Authentication, Reporting and Conformance (DMARC)

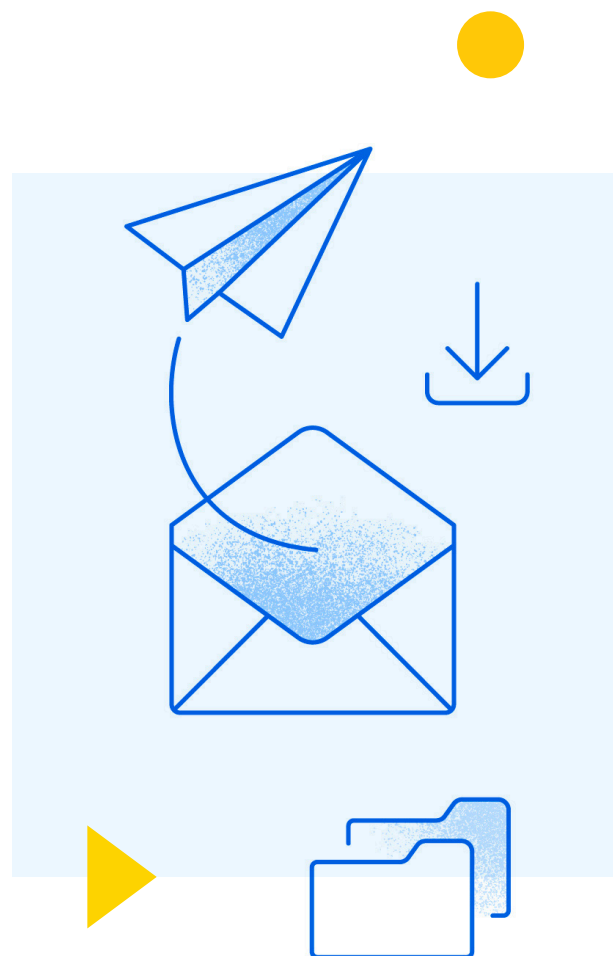
DMARC ties SPF and DKIM together with another simple DNS record that provides a policy for how SPF

and DKIM operate. DMARC also specifies an email address where delivery and forensic reports can be sent for analysis.

- To enable DMARC, you need to add a DNS TXT record with the name "\_dmarc" and the content set to appropriate values for your organization. [Learn more about enabling DMARC.](#)

### Multi-factor Authentication (MFA)

Approximately 80% of email intrusion incidents happen because of weak or stolen passwords. One of the most effective methods to mitigate the risk of an email-based cybersecurity incident is to enable Multi-factor Authentication (see next chapter).



# 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. With MFA, users must also provide a digital token or code that is provided by a secondary device (often a mobile device) in the physical possession of the user to gain access to their account. You may also see references to Two-factor Authentication or 2FA.

We recommend using MFA on all business-critical systems: corporate email accounts, internal services, and third-party services.

## Things to consider

Some MFA services use SMS (text messages) as the second factor. If this is your chosen MFA method, it's crucial that you also set up MFA with your mobile carrier. Keep in mind; text messages are less secure than a proper mobile application or token generator, but better than no second factor at all.

## How to implement MFA

### Google Suite

- Log into your Google Suite Admin console and select the "Security" icon. Keep in mind that Google refers to MFA as 2-step verification (2SV)

- In the Security settings, click "Basic Settings." Be sure that "Allow users to turn on 2-step verification" is checked. Then click "Go to advanced settings to enforce 2-step verification"
- At this point, 2SV is enabled but not enforced. That means that users can choose if they want to use 2SV or not. We recommend requiring 2SV and enabling enforcement

### Microsoft 365

- Log in to your portal as an administrator user, and navigate to the Admin panel
- Navigate to the Users --> Active Users
- Click the "Multi-factor Authentication" link
- Select all your users, then click "Enforce" on the right under "quick steps"

### Selected vendors or existing services

- Select an MFA solution that works with your existing tools and devices (see below) and figure out which services you currently use that have MFA settings you can enable (WordPress, Salesforce, Box, Dropbox, Amazon Web Services, etc.)
- Deploy MFA to your organization with customizable posters, emails, and other training materials

## Vendor recommendations

**Authentication app** - Provides an authentication token for a software/service that already has 2FA or MFA enabled

- Authy from Twilio
- Google Authenticator
- Microsoft Authenticator

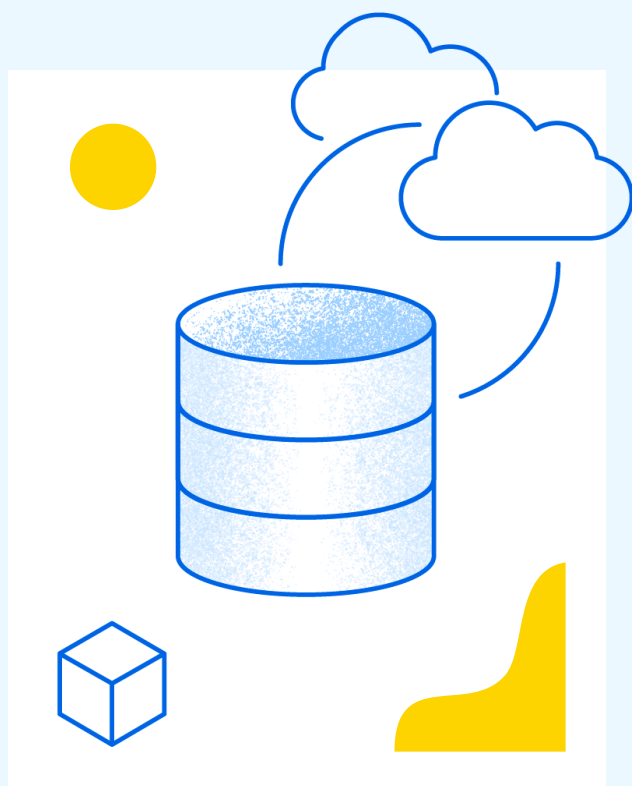
**Authentication solution** - Enables you to configure MFA or 2FA natively for any software

- Duo Security
- Okta

# Maintain good data backups

Ransomware is taking organizations hostage (literally) by encrypting and disabling access to business-critical systems and data until a ransom payment is made. The ransomware business model is arguably the most significant innovation in cybercrime in recent history, and the sophistication of criminal actors is increasing.

A good data backup can mean the difference between a full loss and a full recovery after a ransomware attack. To best protect your business, you'll need to develop a strategy tailored to your business.



## Things to consider

- Maintain backups both on and off-site for critical business data. We recommend using offline backups to store essential data completely separate from the primary network. Cloud backups with a username and password combination not associated with an organization's domain are another alternative.
- You *must* test your backups by trying a *full recovery*. It is extremely common for organizations to only test their backups when they need them, and failures are extremely high in those situations.

## Developing a backup strategy

- What data should be backed up, and where it should be stored
- How frequently data backups should occur
- How quickly you could restore your data from that system in the event of an incident and at different times (right now and years down the line)
- How you can test and iterate on your backup solution to ensure it's working as intended and accommodates changing business needs

## Vendor recommendations

- Acronis
- Backblaze
- Carbonite
- CrashPlan
- Datto
- IDrive
- Veeam Cloud



# Enable secure remote access

The global pandemic changed the work landscape dramatically in 2020. We witnessed a massive shift to remote work, which meant workers were no longer in environments controlled or directly secured by their companies. Instead, they were given access to their organization's resources outside the corporate networks, known as remote access.

When this kind of remote access is allowed, your organization takes on additional risks, and the access should be handled as securely as possible. Without the proper security solutions in place, remote connections can act as a gateway for cybercriminals to access your devices and sensitive data.


## Things to consider

- Remote access protocols (especially Remote Desktop Protocol or RDP) pose a significant risk to organizations of all sizes. Consider implementing a leading perimeterless remote access capability, such as Cloudflare Teams, that will add security to the authentication process and eliminate the external network exposures that continue to be targeted.
- Common remote access solutions such as TeamViewer, ScreenConnect, and LogMeIn are sufficient alternatives (**only** if used with Multi-factor Authentication and strong passwords). We also suggest logging and reviewing access weekly or bimonthly.

## How to safely offer remote access

- When possible, utilize an authentication proxy or identity and access management solution for all remote access
- Make sure the remote access is encrypted (SSL, IPSec, etc)
- Set up strong authentication for remote access (MFA)
- Set strong passwords that are required for remote access
- If possible, require remote users to use company-provided hardware that has been secured to your company standards. Otherwise, ensure that employees understand the safety measures they should be taking (e.g., antivirus, passwords, etc.)
- Be sure to limit authorization to those with critical business needs
- Review authorizations for remote access regularly to make sure unwanted personnel cannot gain access

## Technology recommendations

- Authentication Proxies (Twingate and Cloudflare Teams)  COALITION PARTNER
- IPSec VPN (Supported by firewalls such as Cisco, PaloAlto, Checkpoint)
- SSL VPN (Also supported by many firewall vendors)

## Alternate vendors (use *only* with MFA)

- TeamViewer
- ScreenConnect
- LogMeIn

# Update your software

Cybercriminals look for weaknesses and flaws (known as vulnerabilities) that can be used to gain access to systems or spread malicious software. These vulnerabilities can be located and patched through regular software updates.

We often think of system updates in terms of updating our computer's operating system (which is indeed essential). However, the software applications that run on your operating system, like word processors, spreadsheets, web browsers, and email clients, present their own security challenges. Software exposed to the internet, such as web servers and mail servers, pose an even greater risk because they can be more easily exploited.

All software presents at least some risk to your organization. As much as software engineers try, there are almost always security "bugs" that must be corrected in an update. Patches are created because they're necessary, which makes applying those patches necessary as well.

## Things to consider

When security updates are available for your operating system or software, you should test them before making any changes and apply them as soon as the updates are verified (or in accordance with your IT security policy). This applies to workstations, laptops, and servers alike.

## Best practices for local software updates

- Make sure that updates are applied regularly, including:
  - Operating System (Windows/OS X)
  - Microsoft 365 and other desktop applications, such as Adobe Reader
  - Web browsers and plugins
- Review updates regularly

## Vendor recommendations for internet software

- **Attack Surface Monitor (ASM):** Coalition's proprietary platform provides continuous scanning and automated security alerts, at no additional charge for Coalition policyholders.



# Use a password manager

The passwords your employees set for their business-related accounts and devices matter. Passwords grant access to the most private information your company deems critical. The reality is hackers have mastered the art of stealing password credentials using brute force attacks, where they automate every combination possible until they get it right, or through phishing attempts, where cybercriminals trick people into entering their information under false pretenses (using social engineering). Exposed passwords are also used to gain access to other accounts, potentially increasing the extent of the damage.

While it may feel daunting to worry about the length, strength, and update-frequency of your company passwords — it's necessary. Passwords need to be unique (don't reuse passwords multiple times), strong (with a mix of letters, numbers, and symbols), and updated regularly (based on a company-wide password policy).

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.

**Password managers and MFA:** Even the most secure passwords aren't 100% secure — they may be lost in a third-party breach that you can't control. We recommend using MFA in conjunction with a password manager as the most secure approach to managing your logins. Check out our MFA section for vendor recommendations.

## Things to consider

- Make sure your password manager supports each device platform your employees use
- Find a password manager with browser extensions and full mobile support
- Some password managers let your employees securely share passwords, and some automate password changes regularly

## How to implement a password manager

- Select a password manager solution that meets your budgetary and usage needs
- Work with your IT team to vet and distribute the software
- Host a company-wide training to introduce the new tool and make sure to include it in future new employee onboarding
- Create a password policy in writing that employees can easily access at any time

## Vendor recommendations

- 1Password
- Dashlane
- Keeper
- LastPass (free with limited use)



# Scan for malicious software


Every device you use (personal phone, work phone, laptop, desktop, tablet, etc.) can create an open door for hackers to target your organization. You're just one wrong click away from a cyber event, which is why it is vital to secure and protect every last device (also known as an endpoint) from exposure. The rise in the number of endpoints attached to the networks we use every day has led to an increased need for endpoint protection. The cyber attacks are getting more sophisticated, and endpoints are often viewed as easier targets for infiltrating networks.

Endpoint detection and response (EDR), a more enhanced version of antivirus software, is an emerging technology that addresses the need for continuous monitoring and response to advanced threats. EDR tools (including traditional antivirus and anti-malware software) readily identify, detect, and prevent these threats, making them a crucial part of your overall cybersecurity strategy.

## Best practices for implementing EDR

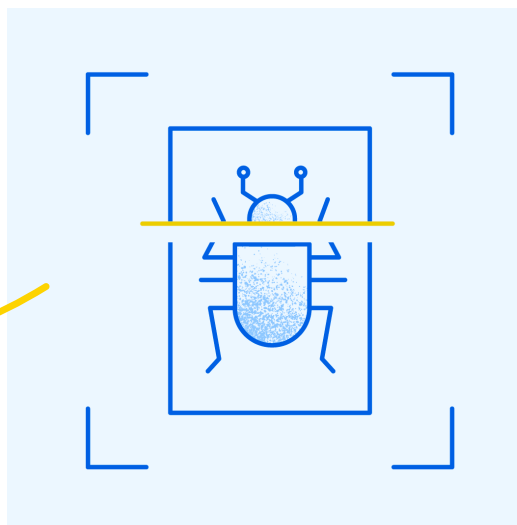
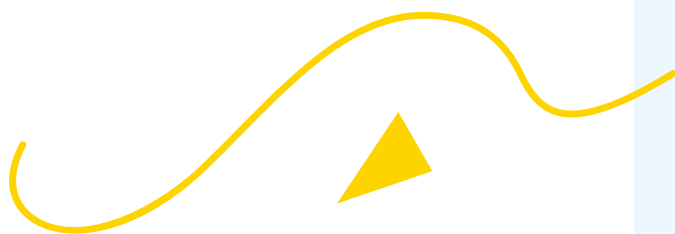
- Require that EDR be installed and active 100% of the time
- Make sure the EDR tech pushes notifications to you rather than forcing you to request updates from the software provider
- Review periodically to verify EDR is installed and updated
- Set a schedule to review EDR detections (weekly, monthly, etc.)

## Antivirus vendor recommendations

- Emsisoft
- ESET
- Malwarebytes  COALITION PARTNER
- Webroot
- Windows Defender

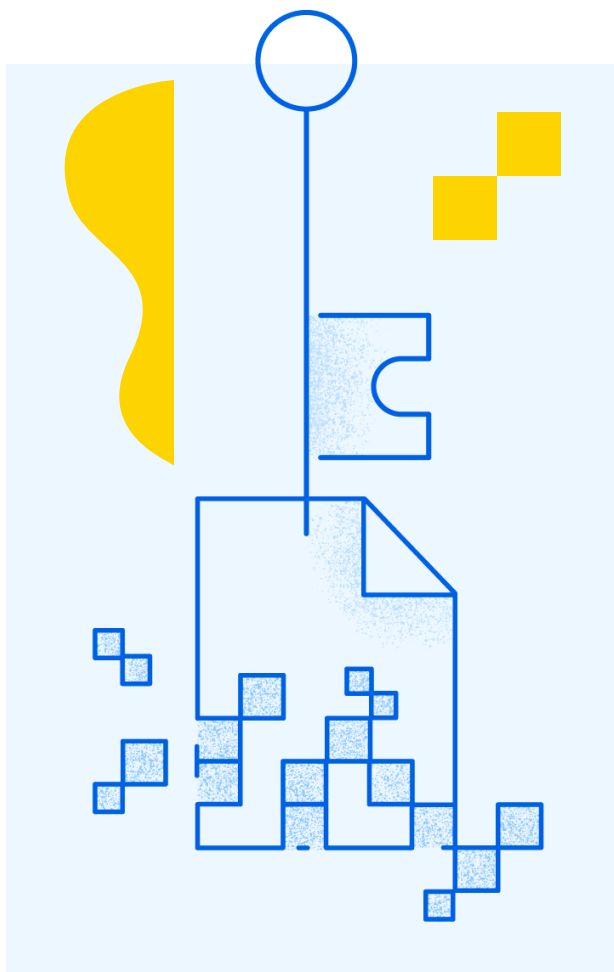
## EDR vendor recommendations

- Carbon Black
- Comodo
- Endgame
- SentinelOne



# Encrypt your data

Computers and phones are crucial for getting work done and need to be managed with security in mind. Encryption is the process through which data is encoded so that it's hidden from bad actors who manage to gain access. It helps protect private information, sensitive data, and enhances the security of communication between client apps and servers.



If you lose a device and your organization's data is protected, the expense is limited to replacing the device, not the information on it — assuming the data is backed up. 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. Physical damage and loss are far cheaper than the loss of sensitive data.

We recommend checking applicable state privacy statutes (or federal statutes) to ensure that your encryption meets the relevant standard. Individual states and other regulatory bodies may require a base level of encryption. NIST currently recommends the [Advanced Encryption Standard \(AES\)](#) as the algorithm of choice to protect electronic data.

If you have a different device, or the encryption process has been updated for your device, check with your provider. Visit our website for more information about [device encryption](#).

## Things to consider

Your organization may be subject to additional compliance requirements based on the data you store

## Mobile phone encryption best practices

- Require a passcode to unlock the phone
- Require an “auto-locking” feature to require entering a passcode after 10 minutes of inactivity
- Require mobile phones to leverage encryption when possible
- On all mobile platforms, keep your operating system software up to date from authorized vendors (e.g., Apple, Android)

# Implement a security awareness training program

If you ask any IT security professional who is responsible for cybersecurity in their organization, they will probably say ‘everyone’ — from the C-suite to contract workers and third-party vendors. Properly mitigating cyber risk isn’t accomplished by one small team. It requires a deliberate culture of cyber risk awareness that holds every individual accountable.


Cyber criminals, targeting small and large businesses alike, aren’t taking advantage of obscure technology. They rely on the manipulation of busy employees to gain access to your company’s networks and devices. Through security awareness training programs, every employee gains the knowledge they need to stay vigilant and avoid becoming the victim of a phishing attack.



## Cybersecurity tips for employees

- **Do not click links or open any attachments you are not expecting.** If you are not expecting a specific attachment, do not open it for review. Additionally, do not click links within emails if you are not expecting them. Follow up with a phone call to the sender directly; better to be safe than sorry!
- **Use proper email security.** Always verify that the emails you receive are from legitimate and trusted sources. Inspect the from addresses closely, and be wary of downloading any files that you’re not anticipating.
- **Use proper web security.** Only download files from known and trusted websites. Verify that the URL is not intentionally misspelled to confuse you into downloading malware from a malicious website.
- **Disable office macros.** Macros in Microsoft 365 are small pieces of code that run in the background — that code often downloads malware. It’s rare to see macro-enabled documents used in everyday business (DOCM and XLSX files). We recommend disabling macros on all computers to prevent ransomware infection.
- **Stay vigilant.** Hackers rely on people letting their guard down and taking action without thinking. It only takes one mistake for malware to get installed and spread through a company.

## Vendor recommendations

- Curricula  COALITION PARTNER
- KnowBe4
- Proofpoint
- SANS Security Awareness

# Purchase cyber insurance

Even with the best defenses in place, things can still go wrong, and employees make mistakes. Organizations can never be 100 percent secure, and if the worst happens, you want to make sure your organization is prepared to recover.

At Coalition, we've seen claims made by organizations of all kinds: small businesses, large businesses, for-profits, and nonprofits — across every industry, despite investments in cybersecurity. However, this is particularly problematic for small organizations that may not have the resources to respond and bounce back quickly. Cyber insurance plays a critical role in providing organizations the financial resources to recover and resume operations after a cyber attack.

## What makes Coalition unique

- Speed of response is critical to limit the damage of a cyber attack. Coalition's in-house Claims and Security and Incident Response teams are available around the clock and get to work fast to help our customers recover from cyber attacks.
- Coalition's customers experience less than **one-fourth** as many claims as the overall marketplace due to our unique approach to underwriting and risk management.
- Coalition continuously monitors its policyholders to identify and notify them of any security concerns. Monitoring is performed entirely on publicly-available data and is non-intrusive. Coalition has helped customers remedy countless vulnerabilities and avoid millions of dollars in claims. We provide these threat monitoring and proactive alerting tools, valued at \$10,000+ per year, for free to all policyholders.

## How to protect your business with Coalition

- Contact your broker. If you don't have one, [contact us](#) and we can provide a list of recommended brokers in your area.
- Sign up for a Coalition Risk Assessment to understand your specific risks.
- Customize your cyber policy to meet your unique business needs.
- Utilize Coalition's security tools, in-house experts, and educational resources to continue your cyber education.



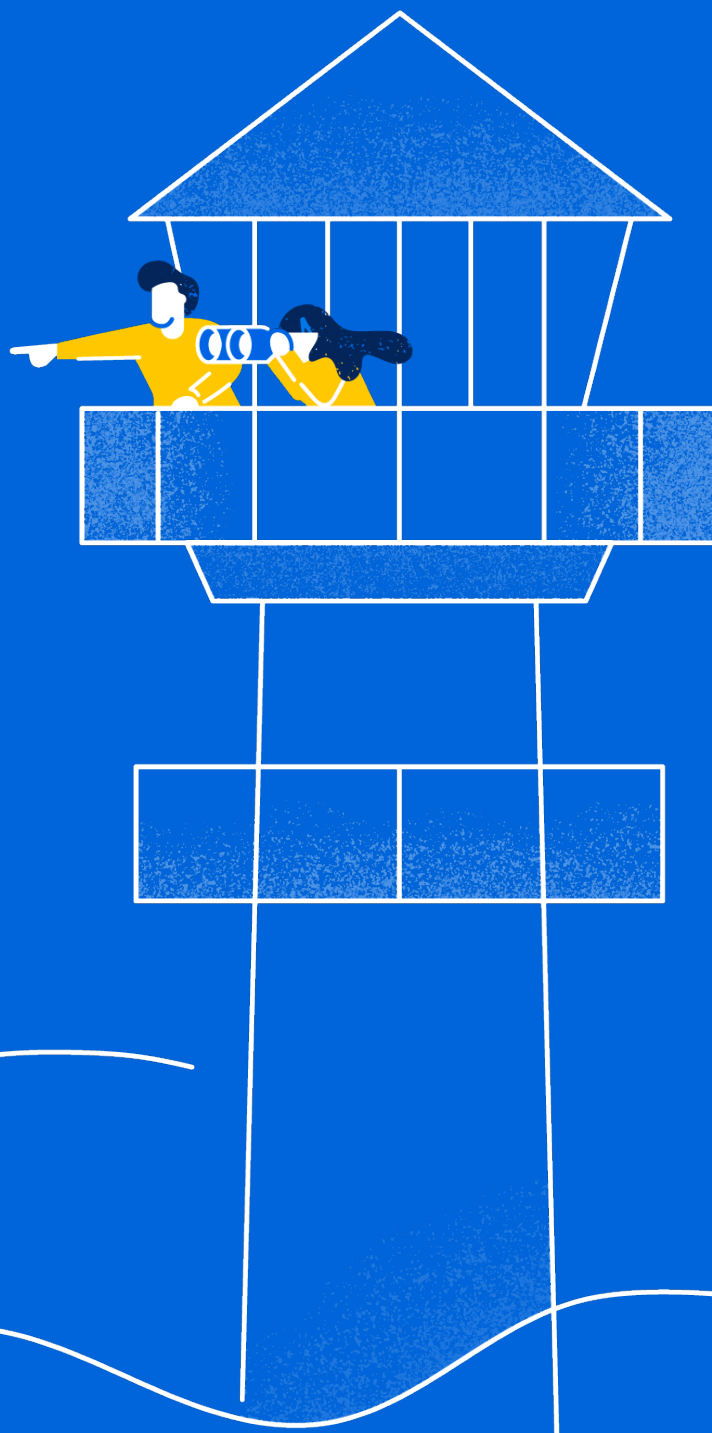


# Coalition is committed to solving cyber risk

Coalition offers more than just insurance — we provide end-to-end risk management for our policyholders. We have a dedicated team available 24/7 to help you before, during, and after a cyber incident to get you back up and running quickly.

We hope you feel more confident protecting your business from cyber threats. We encourage all policyholders to [schedule time](#) with Coalition's in-house Security and Incident Response team to discuss your security program and receive personalized advice.

Under no circumstances shall Coalition be liable for any damages or loss for your use of the recommendations provided. Any action taken upon this information is strictly at your own risk. Similarly, Coalition is not liable or responsible for any errors or omissions in the content. The information contained is provided on an "as is" basis with no guarantee of completeness, accuracy, usefulness, or timeliness.







Cyber Risk, Solved.®

[coalitioninc.com](https://coalitioninc.com)

[@SolveCyberRisk](https://twitter.com/SolveCyberRisk)

[help@coalitioninc.com](mailto:help@coalitioninc.com)

1160 Battery St. Suite 350

San Francisco, CA 94111