



Keeping Your Business Secure: A Checklist For Website Safety

Keeping Your Business Secure: A Checklist For Basic Website Safety

SOPHOS HubSpot

In March 2020, businesses everywhere underwent a change. COVID-19 changed the way consumers made purchases, moving the economy to a more online-focused marketplace than we've ever had before. With all of that new website traffic, comes a more prominent need to make sure your website and customer data is safe and secure. 56% of all internet traffic is from an automated source such as hacking tools, scrapers and spammers, impersonators, and bots—how do you make sure you're taking steps to make your website safe for you and your customers?

We worked with the security experts at [Sophos](#) to put together a security checklist all businesses should keep close-by to make sure you're taking the basic steps to keep your business safe.

Stay In The Know

Learn where your website stands in terms of security (and other pillars). [Website Grader](#) will give your website a score that'll help you learn where you stand.

Phishing

[Phishing](#) scams are some of the most common online scams around, and they're becoming more and more sophisticated. Phishing is no longer limited to an email asking for money, or an email telling you you've won something or been selected for a special opportunity. Today, phishing attacks can look like emails from your bank, your doctor, or even your own business. It's important to stay vigilant in making sure that each email you open and link you click is coming from a reputable sender.



Some quick tips for identifying phishing scams:

Try this:

- Is there a typo in the email? Does the logo of the company sending it look right? Is the branding the same as you remember? Companies take a lot of time and effort to make sure their emails look good and represent the brand well—they won't have typos or major image issues.
- Make sure the URL you are on has an HTTPS at the start and a padlock image next to it. That will tell you the website has security features.

Protecting yourself and your business against phishing attacks means staying vigilant and educating yourself and your team. 41% of IT pros report daily phishing attacks, and the number has been steadily growing. Make sure you're taking the steps you need to protect your business from phishing.

Start Here:

- Set up a time to have a team meeting around phishing attacks. Get your team together and put together a couple of examples of phishing emails ([here's a good place to start](#)). Put your team members into groups and have them work together to identify the phishing giveaway. You'll learn together and make security feel like more of a collaborative effort.



- Have a security training session each employee has to take as part of their onboarding or yearly training. HubSpot does this by creating security videos each employee has to watch in order to be able to continue with their work.

Virtual Meetings And Events

Virtual meetings have become the norm across almost all industries—since we're not able to meet in person as much as we've been used to doing, platforms like Zoom have been immensely helpful in bringing our teams together outside of our offices or physical locations. These platforms have also been vital in moving our physical conferences and events into an online space. Here are some security actions you'll want to use to ensure that your virtual meeting or event is safe and secure:

- Do not allow anonymous attendees—make sure each attendee adds their first and last name once they sign into the meeting.
- Do not allow questions to be asked anonymously—this will help keep folks accountable, and also allows you to follow up should you need to.
- Require attendees to provide their first name, last name, and email address in order to register for an event.
- Use the Zoom password feature to make sure the only folks in your event are the ones who were invited.
- Prepare a statement in advance of events that you can use if an attendee posts inappropriate content in the chat.
- If your event has 50+ registrants, try to have 2-3 moderators to help with chat & QA.



Password Management

Making sure that your passwords are safe and protected is critical to maintaining your website security. Try taking these steps for password management:

Try This:

- Encourage employees to enable two factor authentication across all of their tools. Two factor authentication will help make sure that you're the only one signing into your accounts, keeping both your own and your customer data safe. Tools like Duo make it easy.
- Use a password manager, and encourage others to do the same. Password management apps like LastPass, 1Password, and others make it easy to choose a strong and unique password for every website. You can even purchase a work subscription as an employee benefit.
- Set a quarterly reminder across your company to help folks remember to change their passwords. Keeping up on refreshing your passwords will help ensure the safety of your accounts.

Caring For Your Tools

The tools you use help you do your best job, and it's important to make sure you're staying on top of their security features. Here are a couple of steps you can take right away:

Start Here:

- Know which tools are being used across your business, and consider getting company accounts that you can manage. This will make sure that no unapproved tools are being used, and you can easily and securely remove users if need be, as well as disable potentially compromised accounts.



- Make sure you're staying on top of updates on your tools—update frequently, as sometimes, updates include important security features. Encourage employees to set up automatic updates.
- Consider implementing a cybersecurity solution like Sophos both at work and at home to protect your machine from malware, ransomware accounts, and more. In a recent survey of 5,000 IT Managers, 51% of respondents revealed that they were hit by ransomware in the last year. Check out these 7 best practices to block ransomware.
- Before approving a new tool or vendor, ask them about their security practices—this should be standard practice in evaluating a new tool for your business. Make sure to ask about which data they collect, how they keep their own systems safe, and how your customer data might interact with their systems.
- Consider whether your website is built on a secure platform that offers security features as part of its benefit, such as security monitoring and threat detection.

Cultivating A Culture of Security

If you want to set up a safe and secure online presence, you have to have a culture of security at your company. It's critical that your employees understand the importance of consistently looking back on each checkbox to make sure that both their own, and the business data is protected. Here are some steps you can take to build that culture at your workplace.

Start Here:





■ Talk early and often. Make sure security trainings are part of every employee's yearly training. You can even bundle it with annual points of interest—a first day of the quarter, an annual review, etc. Start here, at the HubSpot Academy ["Implementing Website Security Practices"](#) lesson of our Website Optimization course.

■ Make it easy for employees to point out a potential issue. How can your team members report an attempted phishing attack or remind folks to change their passwords? Consider a simple email address like `security@yourcompanyname.com`, or if you use a messaging tool such as Slack, set up a `#security` channel to make it easy for anyone to check in and keep security top of mind.

■ Create a culture of backups—make sure your employees understand why it's important to back up their projects and important data regularly. Store data in the cloud, and back up what's on your machines. Set up a recurring calendar reminder for your team.

■ Bookmark this checklist and come back to it regularly, making sure your company is staying on top of these best practices.





Start with the best possible protection, validated by independent third-party testing. Then, once you've reviewed these analyst and expert reports to select a vendor that meets your needs, take it for a test drive before you trust. Look for online demos, free trials and customer references.

Security Resources For You and Your Team

1. [A Beginner's Guide to SSL: What It is & Why It Makes Your Website More Secure](#)
2. [Keeping Your Online Data Secure: In HubSpot and Beyond](#)
3. [Best Practices Guide to Block Ransomware](#)
4. [How To Secure Home Computers](#)
5. [Endpoint Protection Buyers Guide](#)
6. [The Ultimate Guide To Cybersecurity](#)
7. [What Is Phishing?](#)
8. [Website Optimization Course](#)

Note: Any legal information in this content is not the same as legal advice, where an attorney applies the law to your specific circumstances, so we insist that you consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this as legal advice or as a recommendation of any particular legal understanding.



Learn more about HubSpot's CMS Hub

CMS Hub integrates all your website tools in one place. From website management, landing pages, security, and blog, it's delightfully simple, yet powerful.

[Learn More](#)

Staying Protected in 2020: Ransomware, Remote Working, and Beyond

Looking to take the next step? Check out Sophos Covid 19 Cybersecurity Hub for threat updates, tips and free tools to help you stay secure this year and beyond.

[Learn More](#)

This Checklist is Brought to You By

