CYBERSECURITY FOR SMALL BUSINESS

Cybersecurity Basics • NIST Cybersecurity Framework • Physical Security • Ransomware
Phishing • Business Email Imposters • Tech Support Scams • Vendor Security • Cyber Insurance
Email Authentication • Hiring a Web Host • Secure Remote Access

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

Table of contents

How to use this booklet

This booklet contains fact sheets on cybersecurity topics. Online versions are available at **FTC.gov/SmallBusiness**, as well as videos and quizzes. These materials will help you and your staff learn about cybersecurity and make it part of your business routine. Here are some ideas to get you started:

- Review the information in this booklet and watch the videos online at **FTC.gov/SmallBusiness**. Familiarize yourself with the information and consider how it applies to your business.
- Talk about cybersecurity with your employees, vendors, and others involved in your business. Share with them the information in this booklet. You can download each of the fact sheets from **FTC.gov/SmallBusiness**.
- Ask your employees to go to **FTC.gov/SmallBusiness** to watch videos about the topics in this booklet — and take the online quizzes to test their understanding of cybersecurity issues.
- Assign a staff person to guide a discussion on one of the cybersecurity topics in this booklet at your next staff meeting. Play a video for all to watch together and discuss how the information can be applied to your business.
- For more free copies of this booklet to use in your employee trainings, go to **FTC.gov/Bulkorder**.

FTC.gov/SmallBusiness

CYBERSECURITY FOR
SMALL BUSINESS

CYBERSECURITY BASICS

Cyber criminals target companies of all sizes.

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT
YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

PROTECT YOUR WIRELESS NETWORK

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take. You can find it at FTC.gov/DataBreach.

Understanding THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

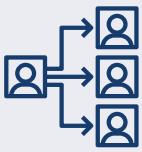
NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:



Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.

Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

3. DETECT

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

Check your network for unauthorized users or connections.

Investigate any unusual activities on your network or by your staff.

4. RESPOND

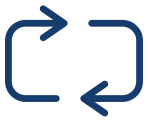
Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER

After an attack:



Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/Programs-Projects/Small-Business-Corner-SBC.

PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

Store securely

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

Limit physical access

When records or devices contain sensitive data, allow access only to those who need it.

Send reminders

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

Keep stock

Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.

HOW TO PROTECT DATA ON YOUR DEVICES

A burglary, lost laptop, stolen mobile phone, or misplaced flash drive — all can happen due to lapses in physical security. But they're less likely to result in a data breach if information on those devices is protected. Here are a few ways to do that:

Require complex passwords

Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Limit login attempts

Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.

Encrypt

Encrypt portable media, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside of the company, like to an accountant or a shipping service.

TRAIN YOUR EMPLOYEES

Include physical security in your regular employee trainings and communications. Remind employees to:

Shred documents

Always shred documents with sensitive information before throwing them away.

Erase data correctly

Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don't rely on "delete" alone. That does not actually remove the file from the computer.

Promote security practices in all locations

Maintain security practices even if working remotely from home or on business travel.

Know the response plan

All staff should know what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. Use *Data Breach Response: A Guide for Business* for help creating a response plan. You can find it at FTC.gov/DataBreach.

RANSOMWARE

Someone in your company gets an email.

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That's a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransomware can take a serious toll on your business.

HOW IT HAPPENS

Criminals can start a ransomware attack in a variety of ways.

Scam emails
with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.

Server vulnerabilities
which can be exploited by hackers.

Infected websites
that automatically download malicious software onto your computer.

Online ads
that contain malicious code — even on websites you know and trust.

HOW TO PROTECT YOUR BUSINESS

Have a plan

How would your business stay up and running after a ransomware attack? Put this plan in writing and share it with everyone who needs to know.

Back up your data

Regularly save important files to a drive or server that's not connected to your network. Make data backup part of your routine business operations.

Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.

Alert your staff

Teach them how to avoid phishing scams and show them some of the common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

WHAT TO DO IF YOU'RE ATTACKED

Limit the damage

Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.

Contact the authorities

Report the attack right away to your local FBI office.

Keep your business running

Now's the time to implement that plan. Having data backed up will help.

Should I pay the ransom?

Law enforcement doesn't recommend that, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. You can find it at FTC.gov/DataBreach.

CYBERSECURITY FOR
SMALL BUSINESS

PHISHING

You get an email that looks like it's from someone you know.

It seems to be from one of your company's vendors and asks that you click on a link to update your business account. Should you click? Maybe it looks like it's from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

HOW PHISHING WORKS

You get an email or text

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

It looks real

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

It's urgent

The message pressures you to act now — or something bad will happen.

What happens next

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

WHAT YOU CAN DO

Before you click on a link or share any of your sensitive business information:

Check it out

Look up the website or phone number for the company or person behind the text or email. Make sure that you're getting the real company and not about to download malware or talk to a scammer.

Talk to someone

Talking to a colleague might help you figure out if the request is real or a phishing attempt.

Make a call if you're not sure

Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.

HOW TO PROTECT YOUR BUSINESS

Back up your data

Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.

Alert your staff

Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.

Deploy a safety net

Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.

WHAT IF YOU FALL FOR A PHISHING SCHEME

Alert others

Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.

Limit the damage

Immediately change any compromised passwords and disconnect from the network any computer or device that's infected with malware.

Follow your company's procedures

These may include notifying specific people in your organization or contractors that help you with IT.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business* (FTC.gov/DataBreach).

Report it

Forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.

BUSINESS EMAIL IMPOSTERS

A scammer sets up an email address that looks like it's from your company.

Then the scammer sends out messages using that email address. This practice is called spoofing, and the scammer is what we call a business email imposter.

Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

HOW TO PROTECT YOUR BUSINESS

Use email authentication

When you set up your business's email, make sure the email provider offers email authentication technology. That way, when you send an email from your company's server, the receiving servers can confirm that the email is really from you. If it's not, the receiving servers may block the email and foil a business email imposter.

Keep your security up to date

Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

Train your staff

Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.

WHAT TO DO
IF SOMEONE SPOOFS YOUR COMPANY'S EMAIL

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks. You don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

CYBERSECURITY FOR
SMALL BUSINESS

TECH SUPPORT SCAMS

You get a phone call, pop-up, or email telling you there's a problem with your computer.

Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then:

Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it

Install malware that gives them access to your computer and sensitive data, like user names and passwords

Try to sell you software or repair services that are worthless or available elsewhere for free

Try to enroll you in a worthless computer maintenance or warranty program

Ask for credit card information so they can bill you for phony services or services available elsewhere for free

Direct you to websites and ask you to enter credit card, bank account, and other personal information

HOW TO PROTECT YOUR BUSINESS

If a caller says your computer has a problem, hang up. A tech support call you don't expect is a scam — even if the number is local or looks legitimate. These scammers use fake caller ID information to look like local businesses or trusted companies.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

If you're worried about a virus or other threat, call your security software company directly, using the phone number on its website, the sales receipt, or the product packaging. Or consult a trusted security professional.

Never give someone your password, and don't give remote access to your computer to someone who contacts you unexpectedly.

WHAT TO DO IF YOU'RE SCAMMED

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn't approve. Keep checking your credit card statements to make sure the scammer doesn't try to re-charge you every month.

Report the attack right away to the FTC at FTC.gov/Complaint.

VENDOR SECURITY

Your business vendors may have access to sensitive information.

Make sure those vendors are securing their own computers and networks. For example, what if your accountant, who has all your financial data, loses his laptop? Or a vendor whose network is connected to yours gets hacked? The result: your business data and your customers' personal information may end up in the wrong hands — putting your business and your customers at risk.

HOW TO MONITOR YOUR VENDORS

Put it in writing

Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable.

Verify compliance

Establish processes so you can confirm that vendors follow your rules. Don't just take their word for it.

Make changes as needed

Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date.

HOW TO PROTECT YOUR BUSINESS

Control access

Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job.

Use multi-factor authentication

This makes vendors take additional steps beyond logging in with a password to access your network — like a temporary code on a smartphone or a key that's inserted into a computer.

Secure your network

Require strong passwords: at least 12 characters with a mix of numbers, symbols, and both capital and lowercase letters. Never reuse passwords, don't share them, and limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Safeguard your data

Use properly configured, strong encryption. This protects sensitive information as it's transferred and stored.

WHAT TO DO IF A VENDOR HAS A DATA BREACH

Contact the authorities

Report the attack right away to your local police department. If they're not familiar with investigating information compromises, contact your local FBI office.

Confirm the vendor has a fix

Make sure that the vendor fixes the vulnerabilities and ensures that your information will be safe going forward, if your business decides to continue using the vendor.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. Find it at FTC.gov/DataBreach.

CYBERSECURITY FOR
SMALL BUSINESS

CYBER INSURANCE

Recovering from a cyber attack can be costly.

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?

Make sure your policy includes coverage for:

- ☐ Data breaches (like incidents involving theft of personal information)
- ☐ Cyber attacks (like breaches of your network)
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Cyber attacks that occur anywhere in the world (not only in the United States)
- ☐ Terrorist acts

Also, consider whether your cyber insurance provider will:

- ☐ Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- ☐ Provide coverage in excess of any other applicable insurance you have
- ☐ Offer a breach hotline that's available every day of the year at all times

NAIC
National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.

CYBERSECURITY FOR

SMALL BUSINESS

WHAT IS FIRST-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- ☐ Legal counsel to determine your notification and regulatory obligations
- ☐ Customer notification and call center services
- ☐ Crisis management and public relations
- ☐ Forensic services to investigate the breach
- ☐ Recovery and replacement of lost or stolen data
- ☐ Lost income due to business interruption
- ☐ Cyber extortion and fraud
- ☐ Fees, fines, and penalties related to the cyber incident

WHAT IS THIRD-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- ☐ Payments to consumers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages, and judgments
- ☐ Accounting costs

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness

NAIC
National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.

EMAIL AUTHENTICATION

Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they're from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

WHAT TO KNOW —

Some web host providers let you set up your company's business email using your domain name (which you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they're from your business. If your business email uses your company's domain name, make sure that your email provider has these three email authentication tools:

Sender Policy Framework (SPF)

tells other servers which servers are allowed to send emails using your business's domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can't find a match, the email can be flagged as suspicious.

Domain Keys Identified Mail (DKIM)

puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization's servers and hasn't been tampered with in transit.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

is the essential third tool for email authentication. SPF and DKIM verify the address the server uses "behind the scenes." DMARC verifies that this address matches the "from" address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have other servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you're notified when this happens.

It takes some expertise to configure these tools so that they work as intended and don't block legitimate email. Make sure that your email hosting provider can set them up if you don't have the technical knowledge. If they can't, or don't include that in their service agreement, consider getting another provider.

WHAT TO DO IF YOUR
EMAIL IS SPOOFED

Email authentication helps keep your business's email from being used in phishing schemes because it notifies you if someone spoofs your company's email. If you get that notification, take these actions:

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks: you don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. And if your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

HIRING A WEB HOST

You may want a new or upgraded website for your business.

But if you don't have the skills to set up the web presence you want, you may want to hire a web host provider to do it for you. Whether you're upgrading a website or launching a new business, there are many web-hosting options. When comparing services, security should be a top concern.

WHAT TO LOOK FOR

Transport Layer Security (TLS)

The service you choose should include TLS, which will help to protect your customers' privacy. (You may have heard of its predecessor, Secure Sockets Layer, or SSL.) TLS helps make sure that your customers get to your real website when they type your URL into the address bar. When TLS is correctly implemented on your website, your URL will begin with https://.

TLS also helps make sure the information sent to your website is encrypted. That's especially important if you ask customers for sensitive information, like credit card numbers or passwords.

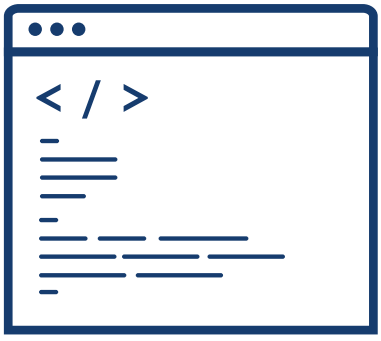
Email authentication

Some web host providers let you set up your company's business email using your domain name (that's part of your URL, and what you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. If you don't have email authentication, scammers can impersonate that domain name and send emails that look like they're from your business.

When your business email is set up using your company's domain name, make sure that your web host can give you these three email authentication tools:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

WHAT TO LOOK FOR



Software updates

Many web host providers offer pre-built websites or software packages designed to make it quick and easy to set up your company's website. As with any software, it is essential that you use the latest versions with up-to-date security patches. Make sure you know how to keep the website's software up to date, or whether the web host provider will do this for you.

Website management

If a web host provider is managing your website, you may have to go through that provider to make any changes — though you may be able to log in and make some changes yourself. Some web host providers may instead offer you the option of managing the website on your own. It's important to clarify from the beginning who will manage the website after it's built.

WHAT TO ASK

When you're hiring a web host provider, ask these questions to make sure you're helping protect your customer information and your business data.

- ☐ Is TLS included in the hosting plan? paid add-on? Will I set it up myself or will you help me set it up?
- ☐ Can my business email use my business website name? If so, can you help me set up SPF, DKIM, and DMARC email authentication technology? (If not, consider looking for a provider that does.)
- ☐ Are the most up-to-date software versions available with your service, and will you keep software updated? If it's my responsibility to keep software updated, is it easy for me to do?
- ☐ After the website is set up, who will be able to make changes to it? Will I have to go through you? Will I be able to log in and make changes on my own? If I can log in to make changes, is multi-factor authentication available?

CYBERSECURITY FOR
SMALL BUSINESS

SECURE REMOTE ACCESS

Employees and vendors may need to connect to your network remotely.

Put your network's security first. Make employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routine.

HOW TO
PROTECT DEVICES

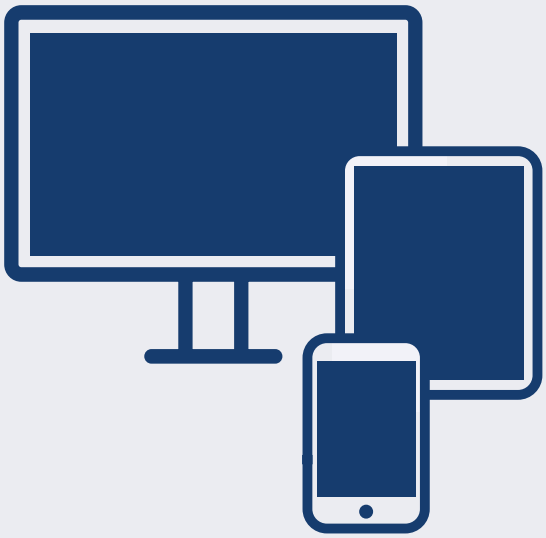
Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and make sure your employees and vendors do as well:

Always change any pre-set router passwords and the default name of your router. And keep the router's software up to date; you may have to visit the router's website often to do so.

Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it's lost or stolen. This is especially important if the device stores any sensitive personal information.

Change smartphone settings to stop automatic connections to public Wi-Fi.

Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.



HOW TO CONNECT REMOTELY — TO THE NETWORK

Require employees and vendors to use secure connections when connecting remotely to your network. They should:

Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can't read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

WHAT TO DO TO MAINTAIN SECURITY —

Train your staff:

Include information on secure remote access in regular trainings and new staff orientations.

Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

Before letting any device — whether at an employee's home or on a vendor's network — connect to your network, make sure it meets your network's security requirements.

Tell your staff about the risks of public Wi-Fi.

Give your staff tools that will help maintain security:

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.
- Consider creating a VPN for employees to use when connecting remotely to the business network.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it's separate from and not connected to your business network.
- Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

This information is part of the Federal Trade Commission's efforts to help small business navigate the cybersecurity world. It was developed in collaboration with:

FEDERAL TRADE COMMISSION

As the nation's consumer protection agency, the FTC's mission is to protect all consumers, including small business owners. In addition to law enforcement efforts, we provide information for small businesses about cybersecurity, protecting sensitive information, and avoiding scams. This information is available at FTC.gov/SmallBusiness, where you also can find links to sign up for our Business Blog and to report a scam. Print publications can be ordered for free at FTC.gov/Bulkorder.

Homeland Security

The U.S. Department of Homeland Security's National Protection and Programs Directorate (NPPD) leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. NPPD provides a range of cybersecurity programs to public and private sector stakeholders, including small and midsize businesses.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The mission of the National Institute of Standards and Technology (NIST), an agency within the U.S. Department of Commerce, is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. As part of its mission, NIST collaborates with federal agencies, as well as other public and private partners, to provide resources for small and medium-sized businesses to reduce their cybersecurity risks.

SBA
U.S. Small Business Administration

As the only go-to resource and voice for small businesses backed by the strength of the federal government, the SBA empowers entrepreneurs and small business owners with the resources and support they need to start, grow or expand their businesses, or recover from a declared disaster. It delivers services through an extensive network of SBA field offices and partnerships with public and private organizations. To learn more, visit www.sba.gov.

FEDERAL TRADE COMMISSION

Homeland Security

FTC.gov/SmallBusiness

October 2018