Small Business Employee Training Resources

During my military service, one of the most important lessons I learned was the value of proper training. Training helps ensure that everyone understands their role, knows how to respond when something goes wrong, and can work together to accomplish the mission while maintaining consistent standards.

Small businesses deserve that same level of preparation.

At MJS Technology, we believe antivirus protection, network monitoring, firewalls, secure backups, and other technical safeguards are essential parts of protecting a business. However, technology alone cannot stop every threat. One of the most important parts of any security system is the person using it.

Every employee has access to some part of the business, whether that includes email, customer information, financial records, shared files, software, or the company network. That access is necessary for employees to do their jobs, but it also means that a single convincing email, phone call, text message, login page, or remote-access request can create an opening for a criminal.

Most security incidents are not caused by employees intentionally doing something wrong. They often happen because a threat looked legitimate, a request felt urgent, or the employee had never been shown which warning signs to look for.

That is the side of cybersecurity this toolbox is designed to address.

The **MJS Technology Resource Hub** is intended to give small-business employees practical knowledge, clear guidance, and the confidence to make safer decisions.

Employees should not be expected to become cybersecurity experts. They should know when to slow down, what questions to ask, how to recognize common warning signs, and who to contact when something doesn't feel right.

By working together, asking questions, and following simple security practices, every employee can help protect the business, its customers, its data, and one another.

Cybersecurity is not only an IT responsibility. It is a team effort, and proper training helps make that team stronger.

Businesses interested in more specialized support may contact MJS Technology to discuss customized employee training developed around their specific operations, technology, and security needs.

Table of Contents

Educational Use and Limitations

This resource is provided by MJS Technology for general educational and cybersecurity-awareness purposes only. It is intended to help small businesses introduce employees to common technology risks and safer workplace practices.

This material is not legal, regulatory, insurance, compliance, or individualized cybersecurity advice. It is not a complete cybersecurity program and may not address every threat, system, industry requirement, or business environment. Organizations are responsible for evaluating and adapting the information to their own operations, technology, policies, contractual obligations, and applicable requirements.

Cybersecurity incidents can occur even when commonly recommended safeguards and training practices are followed. MJS Technology does not represent or guarantee that use of this resource will prevent fraud, unauthorized access, data loss, malware, business interruption, or any other technology or cybersecurity incident.

Downloading, sharing, or using this resource does not establish a managed-services, consulting, professional-client, or other service relationship with MJS Technology. Any customized recommendations or services must be separately agreed upon in writing.

This resource is provided without warranties regarding its completeness or suitability for any particular organization. Businesses should seek qualified professional guidance when their circumstances require legal, regulatory, insurance, compliance, or organization-specific advice.

1. Why Small Businesses Are Targeted

Many people assume cybercriminals are only interested in large corporations, banks, or government agencies. In reality, small businesses are frequently targeted because criminals often expect them to have fewer security protections, limited IT support, and employees who have not received formal cybersecurity training.

Cybercriminals do not always choose one specific business and carefully plan an attack. Many scams are automated and sent to hundreds or thousands of people at once. The criminal is simply waiting for someone to click a link, open an attachment, provide a password, approve a login request, or respond to a convincing message.

Why a Small Business May Be Appealing

Even a very small business may have access to valuable information and systems, including:

- Customer names and contact information
- Employee and payroll records
- Banking and payment information
- Vendor accounts
- Email accounts
- Business documents and shared files
- Passwords and login credentials
- Customer payment information
- Access to other companies through email or shared systems

A criminal may also use a compromised business account to target customers, vendors, or other employees. Because the message comes from a real business email address, the next person may be more likely to trust it.

Small Businesses Often Move Quickly

In a small business, employees frequently handle several responsibilities. One person may answer emails, process payments, communicate with vendors, access customer records, and manage scheduling throughout the same day.

This flexibility is valuable, but it can also create opportunities for criminals. Employees may be busy, interrupted, or under pressure when a suspicious request arrives. A message that appears to come from an owner, customer, bank, or vendor may be acted upon before anyone has time to stop and verify it.

Criminals Take Advantage of Normal Workplace Behavior

Many scams are designed to take advantage of helpful employees. Criminals may create situations that appear urgent, confidential, or important.

For example, an employee may receive a message that says:

- A payment must be made immediately.
- A password is about to expire.
- An invoice is overdue.
- The owner needs gift cards for a customer.
- A vendor has changed its banking information.
- A customer needs a document sent right away.
- An account will be closed unless the employee logs in.
- A computer is infected and technical support must be contacted.

The employee may believe they are helping the business when they are actually responding to a criminal.

What Employees Should Remember

Being targeted does not mean an employee has done anything wrong. Scammers are skilled at making messages and requests look legitimate. Employees can help protect the business by slowing down, asking questions, and verifying unusual requests before taking action.

You should never feel pressured to immediately:

- Send money
- Change payment information
- Share a password
- Provide a verification code
- Open an unexpected attachment
- Sign in through an unfamiliar link
- Install software
- Allow someone to remotely access a computer
- Send sensitive customer or employee information

When something seems unusual, urgent, or unexpected, stop and contact a manager or the company’s approved IT provider.

Key Takeaway

Small businesses are not too small to be targeted. Every employee plays an important role in recognizing suspicious activity and protecting the business.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

2. Email, Text, and Phishing Scams

Phishing is a type of scam in which a criminal pretends to be a trusted person, company, or organization in order to convince someone to take an action.

That action may include:

- Clicking a link
- Opening an attachment
- Entering a password
- Providing a verification code
- Sending money
- Purchasing gift cards
- Sharing customer or employee information
- Installing software
- Allowing remote access to a computer

Phishing attempts may arrive through email, text message, social media, messaging applications, or even a phone call.

Phishing Messages Are Designed to Look Familiar

Scammers often impersonate companies and services that employees already recognize, such as:

- Microsoft
- Google
- QuickBooks
- DocuSign
- Banks and credit-card companies
- Delivery services
- Payroll providers
- Internet and phone providers
- Government agencies
- Vendors and customers
- The business owner or another employee

A scammer may copy a company’s logo, colors, email format, and wording. Some messages are very convincing and may not contain obvious spelling or grammar mistakes.

Employees should never rely on appearance alone when deciding whether a message is legitimate.

Common Types of Phishing Messages

Password and Account Alerts

These messages may claim:

- Your password is expiring.
- Someone logged into your account.
- Your mailbox is full.
- Your account has been suspended.
- You must verify your identity.
- Your email will be deleted unless you act immediately.

The link may lead to a fake website designed to steal the employee's username and password.

Fake Invoices and Payment Requests

An employee may receive an unexpected invoice, receipt, renewal, or overdue warning.

The message may include:

- A link to view the invoice
- An attachment
- A phone number to call
- Instructions to make an immediate payment
- A notice that services will be disconnected

Employees should confirm unexpected invoices using known contact information before opening attachments, following links, or making payments.

Owner or Manager Impersonation

A criminal may pretend to be the owner, manager, or another employee.

The message may say:

- "Are you available?"
- "I need you to handle something privately."
- "I am in a meeting and cannot talk."
- "Purchase gift cards for a customer."
- "Send me the numbers from the back of the cards."
- "Please process this payment immediately."
- "I have a new phone number."

These messages are often brief and may create a sense of secrecy or urgency.

Vendor and Banking Changes

A criminal may impersonate a real vendor and claim that the vendor has changed banks or payment instructions.

The email may appear inside an existing email conversation if the vendor's account has been compromised.

Any change involving banking, direct deposit, payment methods, or account numbers must be independently verified using a known phone number or trusted contact.

Fake Shared Documents

Employees may receive a message claiming that someone shared a document, voicemail, fax, file, or electronic signature request.

The message may appear to come from services such as Microsoft 365, Google Drive, Dropbox, DocuSign, or Adobe.

Before signing in, employees should consider whether they were expecting the document and whether the sender normally shares information that way.

QR Code Scams

Some phishing messages use QR codes instead of clickable links.

Scanning the code may open a fake login page on the employee's phone. Because the employee is viewing the page on a smaller screen, it may be harder to notice that the website address is incorrect.

QR codes should be treated the same as links. Employees should not scan an unexpected code simply because it appears in a professional-looking message.

Warning Signs to Watch For

A message may be suspicious when it:

- Was unexpected
- Creates fear, panic, or extreme urgency
- Requests secrecy
- Asks for money, gift cards, passwords, or verification codes
- Contains an unfamiliar attachment

- Uses a link that does not match the company it claims to represent
- Comes from a slightly misspelled email address
- Uses an unusual greeting or writing style
- Requests information the sender should already have
- Asks the employee to bypass a normal process
- Claims the sender cannot speak by phone
- Pressures the employee not to ask questions

One warning sign does not always prove that a message is fraudulent. However, unusual requests should always be verified before the employee takes action.

Check the Actual Sender

The display name shown in an inbox is not proof of who sent the message. An email may display the owner's name while coming from a completely unrelated address.

Employees should look at the full email address, especially when a message involves:

- Money
- Passwords
- Payroll
- Customer information
- Banking changes
- Sensitive documents
- Unusual requests

Scammers may use addresses that are only slightly different from the legitimate address.

For example, a criminal may replace one letter, add a word, or use a different ending after the company name.

Be Careful With Links

Before clicking a link, employees should pause and consider:

- Was I expecting this message?
- Does the request make sense?
- Is this how the sender normally communicates?
- Is the website address correct?
- Can I reach the account by opening the official website myself?

Whenever possible, employees should avoid using a login link from an unexpected message. Instead, open the normal website or application directly.

Employees should never enter a business password on a page reached through a suspicious or unexpected link.

Attachments Can Be Dangerous

Unexpected attachments may contain malicious software or may lead to a fake login page.

Employees should be especially careful with:

- Compressed or ZIP files
- Documents that ask them to enable editing or enable content
- Unexpected invoices
- Files with unfamiliar extensions
- Attachments from unknown senders
- Attachments that do not match the conversation

Even an attachment from a familiar person may be dangerous if that person's email account has been compromised.

Use the Five-Question Pause

Before clicking, replying, sending information, or making a payment, ask:

1. Was I expecting this?
2. Does the request make sense?
3. Is the sender's actual address correct?
4. Is the message pressuring me to act immediately?
5. Can I verify the request another way?

Verification should be done through a separate communication method.

Do not reply to the suspicious message and ask whether it is legitimate. Instead, call the person using a known phone number, speak to them in person, or start a new message using contact information already on file.

What to Do With a Suspicious Message

When an employee receives a suspicious email or text message:

1. Do not click any links.
2. Do not open attachments.
3. Do not reply.
4. Do not call a phone number provided in the message.

5. Take a screenshot or preserve the message if needed.
6. Report it to a manager or the company's approved IT provider.
7. Delete it only after being instructed or after it has been properly reported.

Employees should report suspicious messages even when they did not click anything. One employee's report may help protect everyone else in the company.

If You Already Clicked

Employees should report the incident immediately, even when nothing unusual appears to have happened.

Be prepared to explain:

- What was clicked
- Whether a file was opened
- Whether a password was entered
- Whether a verification request was approved
- Whether any information was sent
- Whether software was installed
- The approximate time the incident occurred

Prompt reporting gives the business and its IT provider the best opportunity to change passwords, secure accounts, inspect the device, and limit further damage.

Employees should not hide a mistake, attempt to fix it alone, or wait to see whether a problem develops.

Key Takeaway

Unexpected messages should be treated with caution. Slow down, examine the request, and verify it through a trusted method before clicking, replying, sending information, or making a payment.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

3. Passwords and Account Security

Passwords protect access to email, customer information, financial systems, business documents, software, and other important company resources.

A strong password is important, but password security also depends on how employees store, use, and protect their login information.

Use a Unique Password for Every Account

Employees should not use the same password for multiple business accounts.

When one company experiences a data breach, criminals may try the stolen email addresses and passwords on other websites. If an employee reused the same password, one compromised account can lead to several others.

Business passwords should also be different from passwords used for personal email, shopping, social media, or entertainment accounts.

Longer Passwords Are Better

Short passwords are often easier for criminals or automated tools to guess.

A longer passphrase made from several unrelated words can be easier to remember and more difficult to break than a short password with only a few substitutions.

For example, employees may use a structure such as:

Unrelated Word + Unrelated Word + Number + Symbol

Employees should create their own passphrases and should not use examples shown in training materials.

Passwords should not include information that is easy to learn or guess, such as:

- The business name
- The employee’s name
- A child’s or pet’s name
- A birthday
- A phone number
- The current year
- The word “password”
- Simple patterns such as 123456

- Information visible on social media

Use a Password Manager When Available

A password manager can create and store unique passwords so employees do not have to remember every password themselves.

Employees should use only the password manager approved by the business.

Passwords should not be stored in:

- Email drafts
- Unprotected spreadsheets
- Notes on a phone
- Shared documents
- Text messages
- Browser files that anyone can access
- Sticky notes attached to a monitor or desk

If a business does not currently use a password manager, employees should ask a manager or approved IT provider how passwords should be stored.

Never Share Passwords

Employees should not give their passwords to:

- Coworkers
- Vendors
- Customers
- Unexpected technical-support callers
- Anyone requesting them by email or text
- Anyone claiming they need the password to verify an account

When more than one employee needs access to a system, the business should provide separate accounts whenever possible.

Separate accounts help protect information and make it easier to determine who accessed or changed something.

Protect Verification Codes

A verification code is a temporary password.

Criminals may call, text, or email an employee and claim they need a code to:

- Confirm the employee's identity
- Stop a fraudulent transaction
- Repair an account
- Complete a password reset
- Fix an email problem
- Verify a software license

Employees should never provide an unexpected verification code to another person.

If a code arrives that the employee did not request, it may mean someone is trying to access the account. The employee should deny any unexpected login request and report it immediately.

Use Multifactor Authentication

Multifactor authentication, sometimes called MFA or two-step verification, requires more than a password to access an account.

The second step may include:

- A code from an authentication application
- A security key
- A fingerprint or face scan
- A login approval notification
- A texted code, when no stronger method is available

Multifactor authentication provides an additional layer of protection if a password is stolen.

Employees should never approve an authentication request they did not initiate.

Repeated approval notifications may be an attempt to pressure the employee into accepting a fraudulent login.

Be Careful With Password Reset Requests

An employee should be cautious when receiving an unexpected password-reset email, text, or notification.

Before following a reset link, consider:

- Did I request this?
- Is the message coming from the real company?
- Can I open the official website or application directly?

- Is someone else trying to access my account?

Whenever possible, employees should go directly to the official website or application rather than using a link from an unexpected message.

Do Not Save Passwords on Shared Devices

Employees should avoid saving passwords on:

- Public computers
- Shared front-desk computers
- Temporary devices
- Customer devices
- Personal devices that are not approved for business use

When a shared computer must be used, employees should sign out completely when finished.

Closing the browser window may not sign the account out.

Lock the Computer When Stepping Away

An unlocked computer may give another person access to email, documents, customer information, and saved accounts.

Employees should lock the computer whenever they step away, even if they expect to return quickly.

On most Windows computers, employees can press:

Windows key + L

Employees should follow the business's approved process for locking other devices.

Change a Password Immediately When Needed

A password should be changed promptly when:

- It was entered on a suspicious website
- It may have been seen by another person
- It was sent through email or text
- An unexpected login was detected
- The same password was used on a compromised account
- The business or IT provider instructs the employee to change it

When a password may have been stolen, it should be changed from a known-safe device.

Employees should also report the situation instead of changing the password silently, because other action may be needed to secure the account.

What Employees Should Remember

Employees should:

- Use a unique password for every important account
- Use long, difficult-to-guess passphrases
- Use the company-approved password manager
- Turn on multifactor authentication
- Deny unexpected login requests
- Protect verification codes
- Lock computers when unattended
- Report suspicious password activity immediately

Employees should never:

- Reuse business passwords on personal accounts
- Share passwords by email or text
- Give a verification code to a caller
- Approve a login they did not initiate
- Store passwords where others can easily find them
- Ignore an unexpected password-reset notification

Key Takeaway

A password should be unique, protected, and supported by multifactor authentication. Never share a password or verification code, and never approve a login you did not initiate.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

4. Safe Computer and Internet Use

Business computers, phones, tablets, and internet connections provide access to important company information and systems. Everyday actions—such as installing software, visiting websites, connecting a device, or saving a file—can affect the security of the entire business.

Employees do not need to understand every technical risk. They do need to follow approved processes and report anything unusual.

Use Business Devices Appropriately

Whenever possible, employees should use business-owned or business-approved devices for company work.

Business information should not be accessed, stored, or transferred using an unapproved personal device unless the company has specifically allowed it.

Personal devices may not have the same:

- Security software
- Updates
- Password protections
- Backups
- Monitoring
- Access controls

Employees should ask before using a personal computer, phone, tablet, or storage device for business purposes.

Install Only Approved Software

Employees should not download or install software without approval.

Even legitimate-looking programs may contain unwanted software, advertisements, browser extensions, or security risks.

Employees should be especially cautious with programs that claim to:

- Speed up the computer
- Clean the registry
- Update drivers
- Remove viruses
- Recover lost files

- Convert documents
- Provide free PDF tools
- Unlock premium features
- Fix browser problems
- Offer coupons or shopping discounts

If a program is needed for work, employees should ask a manager or the company's approved IT provider to confirm that it is safe and properly licensed.

Be Careful With Browser Extensions

Browser extensions can read information from websites, change search results, display advertisements, and sometimes access information entered into online forms.

Employees should not add extensions, toolbars, coupon finders, password tools, or other browser add-ons without approval.

An extension that appears harmless may have access to:

- Email
- Customer portals
- Business applications
- Browsing activity
- Login pages
- Information copied and pasted into websites

Unfamiliar extensions or changes to the browser should be reported.

Keep Devices Updated

Updates often include important security fixes.

Employees should not repeatedly delay or ignore update notices from approved software or operating systems.

When instructed, employees should:

- Save their work
- Allow updates to install
- Restart the device
- Leave the computer powered on when required
- Report repeated update failures

Employees should not click unexpected update advertisements that appear inside a website or pop-up.

When uncertain, close the message and contact the company's approved IT provider.

Restart Computers Regularly

Restarting a computer can complete updates, refresh security software, and resolve minor performance issues.

Closing the laptop lid or turning off the monitor is not the same as restarting the computer.

Employees should follow the company's restart schedule or restart the device when instructed by IT.

Before restarting, employees should save their work and close open programs.

Lock the Computer When Stepping Away

Employees should lock their computer whenever they leave it unattended, even for a short time.

An unlocked device may allow someone to access:

- Email
- Customer information
- Shared files
- Financial systems
- Saved passwords
- Business applications

On most Windows computers, employees can press:

Windows key + L

Employees should follow the approved locking process for other devices.

Use Approved Storage Locations

Business files should be saved only in locations approved by the company.

Approved locations may include:

- A company server
- A managed shared drive

- Microsoft OneDrive or SharePoint
- Google Drive
- A company-approved cloud service
- A business application

Employees should avoid saving important business information only on:

- The computer desktop
- The Downloads folder
- A personal cloud account
- A personal email account
- A personal USB drive
- A local folder that is not backed up

If an employee is unsure where a file should be saved, they should ask before storing it.

Do Not Use Unknown USB Devices

Unknown USB drives, external hard drives, charging cables, and other devices may contain malicious software or may allow unauthorized access.

Employees should not plug in a device that:

- Was found in a parking lot or public area
- Arrived unexpectedly in the mail
- Belongs to an unknown person
- Was provided by a customer or vendor without explanation
- Has not been approved for business use

When files need to be transferred from an outside device, employees should ask the approved IT provider how to handle it safely.

Use Caution on Public Wi-Fi

Public Wi-Fi may be convenient, but it may not be appropriate for sensitive business work.

Employees should avoid accessing banking, payroll, customer records, or other sensitive systems on public Wi-Fi unless the company has approved a secure method.

Employees should be cautious with networks at:

- Hotels
- Airports
- Restaurants

- Coffee shops
- Conference centers
- Public buildings

A network name that appears legitimate may still be fake.

When working remotely, employees should use the company's approved connection method, such as a trusted hotspot or secure business connection.

Do Not Disable Security Tools

Employees should not turn off or remove:

- Antivirus protection
- Firewall settings
- Monitoring software
- Web filtering
- Backup software
- Device encryption
- Security notifications

A website or program may tell the employee that security software must be disabled before something can be installed. That is a warning sign.

Employees should stop and contact the approved IT provider before making security changes.

Watch for Unusual Computer Behavior

Employees should report unusual activity, including:

- Repeated pop-ups
- Unexpected advertisements
- The browser opening unfamiliar pages
- A changed homepage or search engine
- Programs opening on their own
- The mouse moving without the employee
- Files disappearing or changing
- Security software being disabled
- New programs or extensions appearing
- The computer becoming unusually slow
- Unexpected login prompts
- A camera or microphone activating unexpectedly

These symptoms do not always mean the device has been compromised, but they should not be ignored.

Avoid Unsolicited Technical Support

Employees should never allow an unexpected caller, email sender, pop-up, or website to remotely access a business device.

Legitimate companies generally do not call unexpectedly to announce that a computer is infected.

Employees should not:

- Call a support number shown in a pop-up
- Install remote-access software for an unknown caller
- Share the screen with an unexpected contact
- Provide passwords or verification codes
- Give control of the mouse or keyboard to an unverified person

Employees should contact the business's known IT provider using trusted contact information.

Ask Before Making Changes

Employees should contact a manager or approved IT provider before:

- Installing software
- Changing security settings
- Connecting unfamiliar equipment
- Moving important business files
- Using a personal device for business work
- Taking a computer to another repair provider
- Resetting a business device
- Removing company software

A quick question can prevent data loss, downtime, security problems, and unnecessary repair costs.

What Employees Should Remember

Employees should:

- Use approved devices, software, and storage
- Install updates when instructed

- Restart devices regularly
- Lock computers when unattended
- Report unusual behavior
- Ask before changing settings or installing programs
- Use caution on public Wi-Fi
- Contact the approved IT provider for support

Employees should never:

- Disable security software
- Install unapproved programs
- Use unknown USB devices
- Give an unexpected caller remote access
- Store business information in personal accounts without approval
- Ignore repeated pop-ups or unexplained changes

Key Takeaway

Use only approved devices, software, and storage. When something changes unexpectedly or you are unsure whether an action is safe, stop and ask before proceeding.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

5. Fake Technical Support and Remote Access Scams

Technical support scams are designed to make employees believe there is an urgent problem with a computer, account, network, or business service.

The scammer may claim to represent:

- Microsoft
- Google
- QuickBooks
- A bank
- An internet provider
- A phone company
- A printer company
- A software vendor
- A government agency
- The business's IT provider

The goal is often to convince the employee to install software, share login information, provide a verification code, pay a fee, or allow remote access to the computer.

How Technical Support Scams Begin

These scams may begin with:

- A pop-up warning on a website
- An unexpected phone call
- An email claiming an account has a problem
- A text message with a support number
- A fake virus warning
- A message saying a subscription has renewed
- A caller claiming suspicious activity was detected
- A notice saying the computer or account will be locked

The message may look official and may include logos, technical terms, case numbers, or urgent instructions.

Employees should not assume a message is legitimate simply because it appears professional.

Pop-Up Support Scams

A pop-up may claim:

- The computer is infected
- Personal information is at risk
- The device has been locked
- A virus has been detected
- Microsoft or another company must be contacted immediately
- The employee must call a phone number to prevent damage

Some pop-ups may play loud sounds, repeat warnings, or make it difficult to close the browser.

Employees should not call the number shown in the pop-up.

Instead, they should:

1. Stop interacting with the page.
2. Do not click any buttons inside the warning.
3. Do not download anything.
4. Do not call the displayed number.
5. Contact the company's approved IT provider.
6. Follow instructions for safely closing the browser or disconnecting the device.

Unexpected Support Calls

A caller may say they are contacting the business because:

- The computer has a virus
- The network is sending errors
- A subscription has expired
- An email account was compromised
- A bank transaction is suspicious
- A refund must be processed
- A software license must be verified
- The caller needs to complete maintenance

The caller may know the employee's name, the business name, or other basic information. That does not prove the call is legitimate.

Much of this information can be found online, purchased from data brokers, or obtained from earlier scams.

Remote Access Is Powerful

Remote-access software allows another person to see or control a computer from a different location.

Legitimate IT providers use remote access, but criminals use the same tools.

Once connected, a scammer may be able to:

- View business files
- Access email
- Watch the employee enter passwords
- Copy customer information
- Install malicious software
- Change security settings
- Access banking or payment systems
- Lock the computer
- Demand payment
- Create continued access for later use

Remote access should only be granted to a known and approved IT provider through the company's normal support process.

How to Verify an IT Support Request

Before allowing remote access, employees should confirm:

- Did I request support?
- Is this the company's approved IT provider?
- Did I contact them using a known phone number or support method?
- Does the request match an open service ticket?
- Has a manager approved the work, when required?
- Is the person using the normal remote-support process?

Employees should not rely on a caller ID, display name, email signature, or number provided in a suspicious message.

When uncertain, end the call and contact the approved IT provider using trusted information already on file.

Passwords and Verification Codes

A scammer may ask for:

- An email password
- A banking password
- A computer login
- A verification code
- A password-reset code
- An authentication approval
- A credit-card number
- Payment through gift cards, wire transfer, cryptocurrency, or another unusual method

Employees should never provide passwords or unexpected verification codes to a caller.

An IT provider may need an employee to enter a password directly into a legitimate login screen, but the employee should not read the password aloud, send it by text, or email it.

Refund and Overpayment Scams

Some technical support scams claim that:

- A subscription renewed accidentally
- The business is owed a refund
- Too much money was refunded
- The employee must access online banking
- The employee must return money immediately

The scammer may manipulate what appears on the screen to make it look as though money was deposited or transferred.

Employees should never log in to business banking while an unexpected caller has remote access to the computer.

Any refund, overpayment, or banking issue should be independently verified with the company using a trusted phone number.

Warning Signs

A technical support request may be fraudulent when:

- The contact was unexpected
- The person creates fear or urgency
- The caller says the computer is infected without inspecting it

- The caller asks the employee to install remote-access software
- The caller asks for a password or verification code
- The caller wants access to online banking
- The caller requests payment by gift card, wire transfer, or cryptocurrency
- The caller says not to contact a manager or IT provider
- The caller becomes angry when questioned
- The employee is told to ignore security warnings
- The employee is asked to disable antivirus protection

What Employees Should Do

When contacted unexpectedly by someone claiming to provide technical support:

1. Do not provide information.
2. Do not install software.
3. Do not allow remote access.
4. Do not share passwords or verification codes.
5. Do not access online banking.
6. End the call or close the message.
7. Contact a manager or the approved IT provider using trusted contact information.
8. Report what happened, even if no access was granted.

If Remote Access Was Already Allowed

The employee should act immediately.

1. Disconnect the computer from the internet if it is safe to do so.
2. Do not continue communicating with the caller.
3. Do not attempt to remove software or repair the device alone.
4. Contact a manager and the approved IT provider immediately.
5. Explain what access was granted and what actions occurred.
6. Identify whether any passwords, verification codes, payments, or banking information were involved.
7. Preserve emails, phone numbers, screenshots, and other evidence.

The employee should not feel embarrassed or hide the incident. Technical support scams are designed to be convincing, and rapid reporting can significantly reduce the damage.

What Employees Should Remember

Employees should:

- Use only the company's approved support process
- Verify unexpected support requests independently
- Contact IT using a known phone number
- Report suspicious calls, emails, and pop-ups
- Disconnect and report immediately if remote access was granted

Employees should never:

- Call a support number shown in a pop-up
- Allow an unexpected caller to control a business computer
- Install remote-access software for an unknown person
- Share passwords or verification codes
- Access banking while another person controls the computer
- Pay an unexpected support fee without approval

Key Takeaway

No unexpected caller, message, or pop-up should be allowed to access a business computer. End the contact and reach the company's approved IT provider through a trusted method.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

6. Protecting Customer, Employee, and Business Information

Small businesses collect and use many types of information every day. Some of that information may seem routine, but it can still be valuable to criminals or damaging if it is shared with the wrong person.

Employees should understand which information requires extra care and how to handle it safely.

Information That Should Be Protected

Sensitive business information may include:

- Customer names, addresses, phone numbers, and email addresses
- Payment and billing information
- Employee records
- Payroll information
- Social Security numbers
- Driver's license information
- Medical or insurance information
- Banking details
- Tax documents
- Contracts
- Passwords and login information
- Internal financial reports
- Vendor records
- Business plans and pricing
- Security system details
- Customer files and photographs

Not every employee will have access to all of this information. Employees should only access the information needed to perform their job.

Confirm Before Sending

Before sending an email, text message, file, or document, employees should confirm:

- The recipient is correct
- The email address is spelled correctly
- The correct attachment is included
- The document does not contain information meant for someone else
- The message is being sent through an approved method

- Everyone copied on the message needs the information

Email applications may automatically suggest a recipient with a similar name. Employees should slow down and verify the address before sending sensitive information.

Use BCC When Appropriate

When sending an email to a large group of customers or unrelated recipients, employees should use the business's approved mailing process.

In some situations, this may include using the BCC field so recipients cannot see everyone else's email addresses.

Employees should not place a large group of unrelated customers in the visible To or CC fields unless that is specifically appropriate and approved.

Be Careful With Attachments and Shared Links

Before attaching or sharing a file, employees should confirm that it is the correct document.

A file may contain:

- Hidden customer information
- Previous versions
- Comments or tracked changes
- Internal notes
- Information on additional spreadsheet tabs
- Data belonging to another customer
- Private employee information

Employees should also check the permissions on shared links.

A link that is set to "Anyone with the link" may be accessible to more people than intended.

Use Approved Communication Methods

Sensitive information should only be sent through methods approved by the business.

Employees should not move business information into:

- Personal email accounts
- Personal cloud storage
- Personal messaging applications
- Unapproved file-sharing websites

- Personal social media accounts
- Unapproved artificial intelligence tools
- Personal USB devices

A service may be convenient without being appropriate for customer, employee, or business information.

Protect Printed Information

Paper records can be lost, photographed, copied, or viewed by unauthorized people.

Employees should:

- Store sensitive papers securely
- Avoid leaving documents unattended
- Collect pages from printers promptly
- Use secure disposal or shredding when required
- Keep customer and employee records out of public view
- Avoid discussing private information where others can hear

Sensitive documents should not be placed in a regular trash can when secure disposal is required.

Avoid Sharing Information Over the Phone Without Verification

A caller may pretend to be:

- A customer
- An employee
- A vendor
- A bank representative
- An insurance company
- A government agency
- A manager
- A technical support provider

Employees should verify the caller before providing sensitive information. When appropriate, employees should end the call and call back using a trusted number already on file.

Caller ID can be manipulated and should not be treated as proof of identity.

Limit Access to What Is Needed

Employees should not browse customer, employee, or business records out of curiosity.

Access should be limited to information required for the employee's job.

Employees should also avoid:

- Sharing accounts
- Leaving records open on an unattended screen
- Printing information unnecessarily
- Downloading large amounts of data without a business reason
- Keeping copies after they are no longer needed
- Giving coworkers access without approval

Access controls help protect both the business and the employee.

Protect Information in Public Areas

Employees should be careful when working in:

- Reception areas
- Restaurants
- Coffee shops
- Airports
- Hotels
- Shared offices
- Vehicles
- Conferences
- Customer locations

Other people may be able to see the screen, overhear conversations, or view printed documents.

Employees should avoid discussing passwords, customer details, financial information, or internal business matters in public.

Lost or Misplaced Information

Employees should immediately report:

- A lost business phone or laptop
- Missing paperwork
- A lost USB drive

- An email sent to the wrong person
- A file shared with incorrect permissions
- Information posted publicly by mistake
- A document left at a customer location
- A business device left in a vehicle or public place

Prompt reporting may allow the business to remove access, recover the device, change permissions, notify affected people, or take other protective action.

Accidental Disclosure

Mistakes can happen even when an employee is trying to be careful.

If information is sent, shared, printed, or disclosed incorrectly, the employee should:

1. Report the incident immediately.
2. Explain what information was involved.
3. Identify who may have received or viewed it.
4. Preserve the message or document.
5. Follow instructions from management or the approved IT provider.
6. Avoid attempting to hide or quietly correct the mistake without reporting it.

The sooner the business knows what happened, the more options it may have to limit the impact.

Artificial Intelligence and Online Tools

Employees should not enter confidential or sensitive business information into an artificial intelligence service or other online tool unless the business has approved that service and its use.

Information entered into an online service may be stored, processed, reviewed, or handled outside the company's control.

Employees should not enter:

- Customer records
- Employee information
- Passwords
- Financial details
- Contracts
- Internal reports
- Proprietary information
- Medical or legal information

When uncertain, employees should ask before uploading or pasting business information into any online platform.

What Employees Should Remember

Employees should:

- Access only the information needed for their job
- Confirm recipients and attachments before sending
- Use approved communication and storage methods
- Protect both electronic and printed records
- Verify callers before sharing information
- Report lost devices and accidental disclosures immediately
- Ask before entering business information into online tools

Employees should never:

- Send business information through personal accounts without approval
- Leave sensitive documents unattended
- Share information simply because a caller sounds convincing
- Browse records without a business reason
- Hide an accidental disclosure
- Upload confidential information into an unapproved service

Key Takeaway

Protecting information means knowing who should have access, confirming where the information is going, and reporting mistakes immediately.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

7. Payments, Vendors, and Owner-Impersonation Scams

Requests involving money, payroll, banking information, or sensitive records require extra caution.

Criminals often impersonate business owners, managers, vendors, employees, banks, and customers because they know employees may feel pressure to respond quickly—especially when the request appears urgent or confidential.

Owner and Manager Impersonation

A scammer may pretend to be the owner, manager, or another trusted employee.

The message may arrive through email, text message, or a messaging application and may say:

- “Are you available?”
- “I need you to handle something quickly.”
- “I am in a meeting and cannot call.”
- “This is confidential.”
- “Purchase gift cards for a customer.”
- “Send me the numbers from the back of the cards.”
- “Process this payment immediately.”
- “I have a new phone number.”
- “Do not mention this to anyone yet.”

These messages are designed to make the employee feel helpful, trusted, and responsible for completing an urgent task.

Employees should remember that a display name, profile picture, email signature, or familiar writing style does not prove who sent the message.

Gift Card Scams

Gift card requests are a common form of impersonation fraud.

The scammer may ask the employee to:

- Purchase gift cards
- Buy cards from several stores

- Send photos of the cards
- Scratch off the security codes
- Keep the purchase confidential
- Use a personal card and request reimbursement later

Once the numbers are sent, the money may be gone immediately.

Employees should never purchase or send gift-card information based only on an email or text request.

Any gift-card purchase for business purposes should follow the company's normal approval process and be independently verified.

Vendor Payment Changes

A criminal may impersonate a real vendor and request a change to:

- Bank account information
- Routing numbers
- Payment methods
- Mailing addresses
- ACH instructions
- Wire-transfer instructions
- Contact information

The message may appear legitimate and may even be part of an existing email conversation if the vendor's account has been compromised.

Employees should never change vendor payment information based only on an email.

Verify Changes Independently

Any request involving a change to payment or banking information should be verified through a separate, trusted method.

Employees should:

1. Use a phone number already on file.
2. Speak with a known contact.
3. Confirm the exact change.
4. Document who approved it.
5. Follow the company's established approval process.

Employees should not use a phone number included in the suspicious message unless that number has already been independently verified.

Payroll and Direct-Deposit Scams

A criminal may impersonate an employee and request that direct-deposit information be changed.

The message may claim:

- The employee changed banks
- The old account was closed
- The next paycheck must go to a new account
- The employee cannot speak by phone
- The change must be completed immediately

Changes to payroll or direct deposit should always be verified directly with the employee using a trusted method.

The business should also follow its normal payroll-change process, including any required forms or approvals.

Fake Invoices

Employees may receive invoices for:

- Products the business did not order
- Services the business does not use
- Domain-name renewals
- Software subscriptions
- Advertising
- Office supplies
- Technology support
- Government filings
- Memberships
- Shipping charges

Some fake invoices are designed to look like ordinary bills. Others may appear to be renewal notices or official forms.

Before paying, employees should confirm:

- The product or service was actually ordered
- The vendor is legitimate

- The amount matches the agreement
- The invoice number is valid
- The payment instructions have not changed
- The person approving the payment has authority to do so

Overpayment and Refund Scams

A criminal may claim that:

- A customer accidentally overpaid
- A refund is required
- A deposit was made in error
- The business received too much money
- Funds must be returned immediately

The criminal may provide fake proof of payment or manipulate what appears on a computer screen.

Employees should never send money back until the original payment has been independently confirmed through the business's bank, payment processor, or accounting system. A pending transaction, screenshot, email receipt, or caller's statement is not enough.

Wire Transfers and Urgent Payments

Wire transfers and certain electronic payments can be difficult or impossible to reverse.

Employees should treat unexpected wire-transfer requests with extreme caution.

A request may be suspicious when it:

- Bypasses the normal approval process
- Comes from a new email address
- Uses unusual urgency
- Involves a new bank account
- Requests secrecy
- Claims the owner cannot be reached
- Changes the amount or recipient at the last minute
- Pressures the employee not to verify the request

The more unusual the payment, the more important independent verification becomes.

Customer Payment Scams

Criminals may also impersonate customers.

They may:

- Send a fake payment confirmation
- Claim an invoice was paid twice
- Request a refund to a different account
- Ask the business to forward part of a payment
- Use a stolen credit card
- Request unusual shipping or delivery arrangements
- Ask the business to pay a third party on their behalf

Employees should follow the company's approved payment and refund procedures and report unusual requests.

Requests for Tax or Employee Records

A scammer may impersonate an owner or executive and ask for:

- W-2 forms
- Payroll reports
- Employee lists
- Social Security numbers
- Tax documents
- Direct-deposit information
- Copies of identification

Because these documents contain valuable personal information, employees should verify the request and confirm that the recipient is authorized to receive it.

Sensitive employee records should not be sent simply because a request appears to come from management.

Use a Two-Person Approval Process When Possible

For larger or unusual transactions, businesses should consider requiring approval from more than one person.

A two-person process can help protect against:

- Impersonation scams
- Accidental payments

- Incorrect account information
- Unauthorized purchases
- Rushed decisions

Even in a very small business, a second verification step can be as simple as a phone call to the owner or another authorized person.

Warning Signs

A payment-related request may be fraudulent when it:

- Is unexpected
- Creates extreme urgency
- Requests secrecy
- Bypasses normal procedures
- Involves gift cards, wire transfers, or cryptocurrency
- Changes banking information
- Comes from a new phone number or email address
- Claims the sender cannot speak by phone
- Requests sensitive employee or tax records
- Pressures the employee not to ask questions
- Includes unusual grammar, tone, or instructions
- Asks for payment to a different person or account

What Employees Should Do

Before processing an unusual request involving money or sensitive information:

1. Stop and review the request.
2. Check the actual sender address or phone number.
3. Do not rely on the contact information in the message.
4. Verify the request through a trusted method.
5. Follow the company's normal approval process.
6. Document the verification when appropriate.
7. Ask a manager when anything feels unusual.
8. Report suspected fraud immediately.

Employees should never allow urgency or fear of disappointing someone to replace normal verification procedures.

If a Payment Was Already Sent

The employee should immediately:

1. Notify management.
2. Contact the bank or payment processor.
3. Contact the approved IT provider if email compromise is suspected.
4. Preserve emails, messages, payment details, and phone numbers.
5. Explain exactly what occurred.
6. Follow instructions for securing affected accounts.

Speed is important. Some fraudulent transfers may be recoverable only if they are reported quickly.

What Employees Should Remember

Employees should:

- Verify unusual financial requests independently
- Use trusted contact information
- Follow normal approval procedures
- Confirm vendor and payroll changes
- Report suspicious requests immediately
- Ask for a second approval when appropriate

Employees should never:

- Purchase gift cards based only on an email or text
- Change banking information without verification
- Send money because a message feels urgent
- Return funds before confirming the original payment
- Send payroll or tax records without confirming authorization
- Bypass procedures because the request appears to come from an owner

Key Takeaway

Any request involving money, banking information, payroll, gift cards, or sensitive records should be independently verified before action is taken.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

8. What to Do When Something Goes Wrong

Even careful employees can make mistakes. A suspicious link may be clicked, a password may be entered on the wrong website, information may be sent to the wrong person, or an unexpected caller may be given access to a computer.

The most important action is to report the incident quickly. Delays can give a criminal more time to access accounts, move money, send fraudulent messages, steal information, or cause additional damage.

Report the Incident Immediately

Employees should immediately report:

- Clicking a suspicious link
- Opening an unexpected attachment
- Entering a password on an unfamiliar website
- Approving a login request they did not initiate
- Sharing a verification code
- Allowing an unknown person to access a computer
- Installing software at the direction of an unexpected caller
- Sending money or gift-card information to the wrong person
- Sending sensitive information to the wrong recipient
- Losing a business phone, laptop, USB drive, or document
- Seeing unusual pop-ups, programs, or account activity
- Receiving an alert about an unfamiliar login
- Suspecting that an email or business account has been compromised

Employees should report the situation even when they are unsure whether an incident occurred.

It is better to report a concern that turns out to be harmless than to ignore a problem that becomes more serious.

Do Not Hide a Mistake

Employees may feel embarrassed, worried, or afraid that they will be blamed. Criminals depend on those feelings. The longer an incident remains unreported, the more time they may have to continue the attack.

A prompt, honest report can help the business:

- Change passwords
- Disable compromised accounts

- Stop fraudulent payments
- Remove remote access
- Isolate an affected device
- Recover files
- Warn other employees
- Contact customers or vendors
- Preserve important evidence

The focus should be on protecting the business and limiting the damage.

Stop What You Are Doing

When an employee believes something may be wrong, they should stop interacting with the message, website, caller, or program.

Employees should not:

- Continue clicking
- Reply to the suspicious sender
- Follow additional instructions
- Send more information
- Make another payment
- Delete messages or files
- Attempt to cover up the mistake
- Search online for random repair instructions
- Install cleanup tools
- Try to investigate the incident alone

Further action may make the problem worse or destroy useful evidence.

Disconnect When Remote Access or Active Compromise Is Suspected

If an unknown person is controlling the computer, the employee should disconnect the device from the internet if it is safe to do so.

This may include:

- Disconnecting the Ethernet cable
- Turning off Wi-Fi
- Placing the device in airplane mode
- Turning off the device when instructed

Employees should not take additional technical action unless directed by the company's approved IT provider.

If disconnecting the device may interfere with a critical business system, the employee should contact management or IT immediately for instructions.

Preserve Evidence

Employees should preserve information that may help explain what happened.

Useful information may include:

- The suspicious email or text
- Screenshots
- The sender's email address
- The phone number used
- The website address
- The name of any software installed
- Payment details
- Gift-card receipts
- The time the incident occurred
- Any instructions provided by the scammer

Employees should not delete messages, clear browser history, remove software, or throw away documents unless instructed.

Be Ready to Explain What Happened

When reporting an incident, employees should provide as much detail as possible.

Helpful questions include:

- What happened?
- When did it happen?
- What device was being used?
- What account was involved?
- Was a link clicked?
- Was an attachment opened?
- Was a password entered?
- Was a verification code shared?
- Was a login approved?
- Was software installed?
- Was remote access allowed?

- Was money sent?
- Was customer or employee information involved?
- Is the suspicious person still connected?

Employees should be honest about what occurred. Accurate information helps the response team act more quickly.

Passwords and Account Access

When a password may have been exposed, employees should contact the approved IT provider or manager before making extensive changes.

The employee may be instructed to:

- Change the password from a known-safe device
- Sign out of all active sessions
- Review recent account activity
- Reset multifactor authentication
- Remove unfamiliar devices
- Secure other accounts that used the same password
- Notify contacts who may have received fraudulent messages

A password should not be changed from a computer that may still be under a criminal's control.

Financial Incidents

When money, banking information, payroll, or gift cards are involved, employees should immediately contact:

- The business owner or manager
- The bank or payment processor
- The approved IT provider, when an account may be compromised
- Any other person identified in the company's incident process

Employees should preserve:

- Receipts
- Transaction numbers
- Account information
- Emails
- Text messages
- Phone numbers
- Screenshots

Quick reporting may improve the chance of stopping or recovering a fraudulent payment.

Lost or Stolen Devices

A lost business device should be reported immediately, even when it has a password.

The business may need to:

- Lock or erase the device remotely
- Remove account access
- Change passwords
- Review recent activity
- Contact customers or employees
- File a report
- Replace security credentials

Employees should not wait until the end of the day or assume the device will be found.

Accidental Email or Data Disclosure

When information is sent to the wrong person or shared incorrectly, the employee should:

1. Report the incident immediately.
2. Identify what information was involved.
3. Identify the unintended recipient.
4. Preserve the original message.
5. Avoid sending additional messages unless instructed.
6. Follow the company's response process.

Attempting to recall an email or asking the recipient to delete it may be appropriate in some cases, but those steps should not replace reporting the incident.

Follow Instructions From the Response Team

After an incident is reported, employees should follow instructions from management and the approved IT provider.

They may be asked to:

- Stop using the device
- Bring the device to IT
- Change a password
- Forward a suspicious message

- Contact a vendor or customer
- Complete an incident report
- Avoid discussing the incident publicly
- Watch for additional suspicious activity

Employees should not make independent changes that could interfere with the response.

Learn From the Incident

After the immediate problem is handled, the business may review what happened and identify ways to reduce the risk of a similar incident.

This may include:

- Updating procedures
- Providing additional training
- Changing account permissions
- Improving payment verification
- Adding multifactor authentication
- Strengthening email security
- Updating contact lists
- Adjusting backup or monitoring systems

The purpose of this review should be to improve the company's protection, not simply assign blame.

What Employees Should Remember

Employees should:

- Report incidents immediately
- Stop interacting with suspicious messages or callers
- Preserve evidence
- Disconnect when directed
- Explain honestly what occurred
- Follow instructions from management and IT
- Report lost devices and accidental disclosures promptly

Employees should never:

- Hide a mistake
- Wait to see whether something bad happens
- Delete evidence
- Attempt to repair a compromised device alone

- Continue communicating with a suspected scammer
- Change important settings without instructions
- Assume an incident is too small to report

Key Takeaway

Mistakes can often be contained when they are reported quickly. Stop, report the incident, preserve the evidence, and follow the company's response process.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

Stop and Verify

Cybercriminals often try to create urgency, fear, confusion, or pressure. Their goal is to make someone act before they have time to think. When a message, call, request, or computer warning seems unusual, use the **STOP** process before taking action.

S — Slow Down

Do not allow urgency to make the decision for you.

Pause before you:

- Click a link
- Open an attachment
- Send money
- Change banking information
- Share business information
- Enter a password
- Approve a login
- Install software
- Allow remote access
- Follow instructions from an unexpected caller

A legitimate request can usually wait long enough to be verified.

T — Think About the Request

Ask yourself:

- Was I expecting this?
- Does the request make sense?
- Is this how the person or company normally contacts me?
- Is the request unusual for my job?
- Am I being asked to bypass a normal process?
- Is the message creating unnecessary urgency or secrecy?

If something feels different, unusual, or out of place, treat it with caution.

O — Observe the Details

Look closely at:

- The full sender email address
- The phone number
- The website address
- The wording and tone
- Any attachment
- The requested action
- Changes to payment or contact information
- Requests for passwords or verification codes
- Claims that the sender cannot speak by phone
- Instructions not to tell anyone else

A familiar name, logo, signature, or profile picture does not prove the message is legitimate.

P — Proceed Only After Verification

Verify the request using a trusted method.

You may:

- Call the person using a number already on file
- Speak with them in person
- Start a new email using a known address
- Open the company's official website directly
- Contact a manager
- Contact the company's approved IT provider

Do not use the phone number, link, or contact information provided in a suspicious message.

Always Verify Requests Involving

Extra verification is required when a request involves:

- Money or payments
- Gift cards
- Banking information
- Payroll or direct deposit
- Passwords
- Verification codes
- Customer information
- Employee records
- Tax documents
- Remote access
- Software installation

- Sensitive business files

When You Are Unsure

You are not expected to investigate a possible scam alone.

Stop and ask for help when:

- A request feels unusual
- You are being pressured to act quickly
- You cannot confirm the sender
- The normal process is being bypassed
- You are uncomfortable with the request
- You are unsure whether a link, file, or caller is safe

It is better to delay a legitimate request briefly than to act immediately on a fraudulent one.

If You Already Took Action

Report the incident immediately if you:

- Clicked a suspicious link
- Opened an unexpected attachment
- Entered a password
- Approved an unfamiliar login
- Shared a verification code
- Sent sensitive information
- Made a payment
- Installed software
- Allowed remote access

Do not wait to see whether a problem develops.

Remember

Slow down. Think about the request. Observe the details. Proceed only after verification.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

How to Spot a Phishing Message

Phishing messages are designed to look legitimate and convince you to act quickly. They may arrive through email, text message, social media, messaging applications, or shared-document notifications.

A message does not have to contain every warning sign to be suspicious. Even one unusual detail may be enough to stop and verify the request.

Check the Sender

Look beyond the display name.

A message may show the name of:

- The business owner
- A coworker
- A customer
- A vendor
- Microsoft
- Google
- QuickBooks
- A bank
- A delivery company

The display name can be changed easily. Check the full email address or phone number.

Watch for:

- Misspelled company names
- Added letters, numbers, or words
- Unusual email domains
- Personal email addresses used for business requests
- A new phone number
- An address that is almost—but not exactly—correct

Watch for Urgency or Pressure

Phishing messages often try to prevent you from thinking carefully.

Common phrases include:

- “Act immediately”

- “Your account will be closed”
- “Payment is overdue”
- “This must be handled today”
- “Do not tell anyone”
- “I am in a meeting and cannot call”
- “Your password expires now”
- “Your computer is infected”
- “This is your final warning”

Urgency does not always mean a message is fraudulent, but urgent requests should still be verified.

Be Suspicious of Unusual Requests

Stop and verify messages asking you to:

- Purchase gift cards
- Change banking information
- Send a wire transfer
- Update direct deposit
- Share a password
- Provide a verification code
- Open an unexpected attachment
- Sign in through a link
- Install software
- Allow remote access
- Send customer or employee records
- Bypass the normal approval process

Examine Links Carefully

A link may look legitimate while directing you to a fake website.

Before clicking:

- Hover over the link when possible
- Look at the full website address
- Check for misspellings
- Look for added words or unusual endings

- Consider whether you were expecting the message

When possible, open the company's official website or application directly instead of using the link.

Treat QR Codes Like Links

A QR code can lead to a fake login page or malicious website.

Do not scan an unexpected QR code simply because it appears in a professional-looking email, invoice, poster, or document.

Ask:

- Was I expecting this?
- Who sent it?
- Why am I being asked to scan it?
- Can I access the information another way?

Be Careful With Attachments

Unexpected attachments may contain malicious software or lead to a fake login page.

Use extra caution with:

- ZIP files
- Unexpected invoices
- Documents asking you to enable editing
- Files asking you to enable content or macros
- Attachments from unfamiliar senders
- Files that do not match the conversation
- Unexpected electronic signature requests
- Voicemail or fax attachments

Even a message from a familiar account can be dangerous if that account has been compromised.

Look at the Tone and Wording

A message may be suspicious when:

- The writing style is different from normal
- The greeting is unusual
- The sender uses unexpected language
- The message feels overly formal or overly casual

- The request does not fit the sender's role
- The sender claims they cannot talk by phone
- The message asks for secrecy

Modern phishing messages may be well written, so good spelling and grammar do not prove that a message is safe.

Be Careful With Login Pages

A fake login page may closely resemble Microsoft, Google, QuickBooks, a bank, or another familiar service.

Before entering a password:

- Check the website address
- Confirm you opened the official website
- Consider whether you expected to sign in
- Stop if the page looks different
- Do not continue if the browser shows a warning

Never enter a business password on a page reached through an unexpected message unless the request has been verified.

Five Questions to Ask

Before clicking, replying, sending information, or making a payment, ask:

1. Was I expecting this?
2. Does the request make sense?
3. Is the sender's actual address correct?
4. Is the message creating urgency, fear, or secrecy?
5. Can I verify the request another way?

How to Verify Safely

Use a separate, trusted method.

You may:

- Call a known phone number
- Speak with the person directly
- Start a new email using an address already on file
- Open the official website or application yourself

- Ask a manager
- Contact the approved IT provider

Do not reply to the suspicious message or use the contact information it provides as your only verification.

If You Think a Message Is Phishing

1. Do not click links.
2. Do not open attachments.
3. Do not reply.
4. Do not call the number in the message.
5. Preserve the message if needed.
6. Report it to a manager or the approved IT provider.
7. Delete it only after following the company's reporting process.

If You Already Clicked

Report it immediately.

Be ready to explain:

- What you clicked
- Whether a file opened
- Whether you entered a password
- Whether you approved a login
- Whether you sent information
- Approximately when it happened

Remember

A familiar name, logo, or writing style does not prove a message is legitimate. Slow down, check the details, and verify unusual requests through a trusted method.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

What to Do After a Suspicious Click

Clicking a suspicious link does not always mean that an account or computer has been compromised. However, quick reporting gives the business the best chance to prevent further damage.

Do not wait for something unusual to happen before asking for help.

Stop Immediately

If you believe you clicked a suspicious link:

- Stop interacting with the website
- Do not enter any additional information
- Do not download files
- Do not approve login requests
- Do not call phone numbers shown on the page
- Do not follow further instructions
- Do not attempt to investigate the website yourself

Close the page only if you can do so safely. If the page will not close, contact the approved IT provider for guidance.

Report What Happened

Contact your manager or the company's approved IT provider immediately.

Be ready to explain:

- What message you received
- What link you clicked
- Approximately when it happened
- What device you were using
- Whether a website opened
- Whether a file downloaded
- Whether you entered a username or password
- Whether you provided a verification code
- Whether you approved a login request
- Whether you installed software
- Whether you allowed remote access

Do not leave out details because you feel embarrassed or are unsure whether they matter.

If You Entered a Password

Tell the approved IT provider which account was involved.

You may be instructed to:

- Change the password from a known-safe device
- Sign out of all active sessions
- Review recent account activity
- Remove unfamiliar devices
- Reset multifactor authentication
- Change other accounts that used the same password
- Warn coworkers or contacts about possible fraudulent messages

Do not change the password from a computer that may still be under another person's control unless instructed.

If You Approved a Login

An unexpected login approval may allow someone into the account even if the password was not shared directly.

Immediately report:

- Which account was involved
- What type of approval was used
- The time of the approval
- Whether additional notifications appeared

Deny any further login requests you did not initiate.

If a File Downloaded

Do not open the file.

Do not:

- Move it
- Rename it
- Forward it
- Upload it somewhere else

- Try to scan or inspect it yourself
- Delete it unless instructed

Tell the approved IT provider where the file appears to be located and what it is called.

If Software Was Installed

Disconnect the device from the internet if directed or if an unknown person is actively controlling it.

This may include:

- Turning off Wi-Fi
- Disconnecting the Ethernet cable
- Placing the device in airplane mode

Do not attempt to uninstall the software or run random cleanup tools unless instructed.

If Remote Access Was Allowed

Act immediately.

1. End the call or message.
2. Disconnect the device from the internet if it is safe to do so.
3. Do not continue using the computer.
4. Contact management and the approved IT provider.
5. Explain what the other person viewed or accessed.
6. Report whether banking, email, files, passwords, or customer information were opened.
7. Preserve phone numbers, emails, receipts, and screenshots.

Never log in to banking or financial systems while an unexpected person has remote control of the device.

If Money or Payment Information Was Involved

Immediately notify:

- The business owner or manager
- The bank or payment processor
- The approved IT provider if an account may have been compromised

Preserve:

- Transaction numbers
- Receipts
- Emails
- Text messages
- Phone numbers
- Screenshots
- Gift-card information
- Bank instructions

Time matters. Some fraudulent transactions may only be stopped or recovered if they are reported quickly.

Preserve the Message

Do not delete the suspicious email, text, or document unless instructed.

The message may help identify:

- The sender
- The website used
- What information was requested
- Whether other employees may be targeted
- What accounts may be affected

Take a screenshot when appropriate, but do not continue interacting with the suspicious content.

Do Not Try to Fix It Alone

Avoid:

- Searching for random repair tools
- Installing antivirus programs from advertisements
- Calling a support number from the suspicious page
- Deleting files or browser history
- Resetting the computer
- Continuing to use the device for sensitive work
- Asking the suspected scammer for help

These actions may make the problem worse or remove useful evidence.

Watch for Additional Activity

After reporting the incident, employees may be asked to watch for:

- Unexpected password resets
- Login alerts
- New email forwarding rules
- Messages sent from their account
- Missing or changed files
- Unfamiliar charges
- Repeated verification requests
- Customers or coworkers receiving strange messages

Report any additional activity immediately.

Remember

A suspicious click is not something to hide. Stop, report what happened, preserve the evidence, and follow the instructions of your manager or approved IT provider.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.

What to Do When a Security Pop-Up Appears

Some scam websites display loud, alarming pop-ups claiming that your computer has been infected, locked, or compromised.

The warning may:

- Play a loud alarm or recorded voice
- Cover the entire screen
- Display Microsoft, Windows, Apple, or antivirus logos
- Claim your information is being stolen
- Tell you not to turn off the computer
- Provide a technical-support phone number
- Warn that the computer will be damaged if you close the page
- Make the browser difficult to close

These warnings are designed to create panic and convince you to contact a scammer.

How These Pop-Ups Appear

A security pop-up does not necessarily mean that you visited an unsafe or inappropriate website.

These warnings can appear while browsing ordinary websites, including news pages, recipe sites, shopping sites, search results, weather pages, or other familiar websites. In some cases, a legitimate website may display an unsafe advertisement, redirect the browser through another page, or contain third-party content that has been compromised.

A scam page may also appear after clicking an advertisement, search result, notification, or link that looked normal. Sometimes the redirect happens so quickly that the employee may not realize the browser opened a different website.

The pop-up itself also does not automatically mean that the computer has already been infected. In many cases, the warning is simply a webpage designed to look like a serious computer alert. Its purpose is to frighten the user into calling a fake support number, downloading software, or granting someone remote access.

Employees should not feel embarrassed or assume they did something wrong. The important thing is to avoid interacting with the warning, close the browser safely, and report the incident when required.

First: Do Not Call the Number

Do not:

- Call the phone number shown
- Click buttons inside the warning
- Download anything
- Enter a password
- Provide a verification code
- Pay for technical support
- Follow instructions from the pop-up
- Allow anyone to remotely access the computer

A legitimate company will not normally provide an unexpected technical-support phone number through a browser warning.

If It Is Only a Pop-Up

Use these instructions when:

- You have not called the number
- You have not downloaded or installed anything
- You have not entered a password
- You have not allowed anyone to remotely access the computer
- Nobody else is controlling the mouse or keyboard

The warning may only be running inside the browser.

Close the Browser

On a Windows computer:

1. Press **Ctrl + Shift + Esc** to open the Task Manager.
2. Find the browser, such as Chrome, Edge, or Firefox.
3. Select the browser.
4. Choose **End task**.

You may also press **Ctrl + Alt + Delete** and select **Task Manager**.

If you cannot safely close the browser, restart the computer.

When Reopening the Browser

- Do not restore the previous session.
- Do not reopen the suspicious tabs.
- Close any page that returns to the warning.
- Report the pop-up according to your company's procedure.
- Contact the approved IT provider if the warning returns or anything else seems unusual.

A browser-only pop-up will often stop after the browser is completely closed, but employees should not assume that every incident is harmless.

If Someone May Have Remote Access

Treat the situation as an active security incident when:

- You called the number in the warning
- Someone called you and claimed to be technical support
- You downloaded or installed remote-support software
- Someone is moving the mouse or typing
- Another person can see or control your screen
- You gave someone permission to access the computer
- You are unsure whether someone is still connected

The first priority is to stop the person's connection to the computer.

Disconnect the Computer From the Internet

You may:

- Disconnect the Ethernet cable
- Turn off Wi-Fi
- Place the device in airplane mode
- Shut down the computer

Important

Disconnecting the Ethernet cable may not be enough if the computer is also connected to Wi-Fi.

Make sure both Ethernet and Wi-Fi are disconnected.

If you are unsure how to disconnect both connections, press and hold the computer's power button until it shuts down.

Stopping an active unauthorized connection is more important than completing a normal shutdown.

After Disconnecting

1. Do not reconnect the computer to the internet.
2. Do not continue speaking with the caller.
3. Do not continue using the affected computer.
4. Do not attempt to remove programs yourself.
5. Do not log into email, banking, payroll, or other sensitive accounts from that computer.
6. Contact the business owner, manager, or approved IT provider from another device.
7. Explain exactly what happened.

How to Turn Off Wi-Fi in Windows

1. Select the network, sound, or battery area near the clock.
2. Select the **Wi-Fi** button.
3. Confirm that Wi-Fi is turned off.

The exact appearance may vary depending on the version of Windows.

Employees should be shown in advance how to:

- Turn off Wi-Fi
- Disconnect an Ethernet cable
- Place a laptop in airplane mode
- Shut down the computer
- Contact the approved IT provider

Information to Preserve

Do not delete messages, remove software, or clear the browser history unless instructed.

Preserve any available:

- Phone numbers
- Emails
- Text messages
- Screenshots
- Receipts
- Website addresses
- Names used by the caller

- Names of programs that were installed

Information to Report

Be prepared to explain:

- What appeared on the screen
- Whether you called a number
- Whether someone called you
- Whether anything was downloaded or installed
- Whether someone controlled the mouse or keyboard
- Whether you entered a password
- Whether you shared a verification code
- Whether email, banking, payroll, or customer records were opened
- Whether money or payment information was involved
- Approximately when the incident occurred

Do not leave out information because you feel embarrassed. The faster the business understands what happened, the faster it can protect the computer and affected accounts.

If You Are Not Sure Which Situation Applies

Take the safer approach:

1. Disconnect the computer from the internet or shut it down.
2. Stop using the device.
3. Contact the company's approved IT provider from another device.

Remember

Only a pop-up? Do not call the number. Close the browser and report it.

Someone controlling the computer? Disconnect both Ethernet and Wi-Fi—or shut the computer down—and contact the approved IT provider immediately.

General educational guidance only. This resource is not a guarantee against cybersecurity incidents and does not replace organization-specific policies, technical safeguards, or professional advice.