



Cybersecurity Awareness Month 2026

Employee Education Packet

Table of Contents

Introduction.....3

Why Multifactor Authentication Matters4

Identifying and Responding to Phishing Scams6

The Value of Using a Virtual Private Network8

Safe Internet Browsing Practices10

Password Management Best Practices.....12

Identifying and Responding to Business Email Compromise Scams14

Identifying and Responding to Deepfake Scams16

Identifying and Responding to Ransomware Attacks18

Remote Work Best Practices20

Don't Become an Insider Threat.....22

Conclusion.....25

Introduction

October is Cybersecurity Awareness Month. Throughout this month, the public and private sectors work together to raise awareness of the importance of cybersecurity. This year marks the 23rd Cybersecurity Awareness Month.

This annual campaign offers employers an opportunity to reinforce a simple truth: Protecting the organization isn't just IT's job; it's every employee's responsibility. Between the emails staff open, the websites they visit and the passwords they choose, each team member plays a role in safeguarding company data, colleagues and customers from harm.

This resource packet provides 10 articles employers can distribute to their workforce, designed to make cybersecurity practical, approachable and easy to apply in everyday work. Each article tackles a different topic, including spotting different types of social engineering scams, ensuring safe internet browsing practices and enabling company security tools. Whether employees are at their desks, working remotely or on the go, these articles offer clear, actionable tips they can put to use right away.

Cyberthreats are constantly evolving, and a well-informed workforce remains one of the best defenses an organization has. Employers are encouraged to share these articles across teams, incorporate them into internal communications, and keep them accessible as ongoing references throughout the year, not just during this month.

CYBERSECURITY ESSENTIALS

Why Multifactor Authentication Matters

While complex passwords may help deter cybercriminals, they can still be cracked. According to telecommunications company Verizon, an estimated 80% of hacking-related data breaches involve stolen credentials. With these findings in mind, it's clear that passwords alone aren't enough to protect your workplace accounts.

Fortunately, that's where multifactor authentication (MFA) can help. MFA is a layered approach to securing data and applications, in which a system requires a user to present a combination of two or more credentials to verify their identity during login. This article provides more information on MFA, explains how it protects you and your employer, and offers related best practices.

MFA Overview

Through MFA, employees must confirm their identities by providing extra information, such as a phone number, biometric data or one-time security code, in addition to their passwords when attempting to access sensitive corporate information and infrastructure. Companies generally require MFA for remote access to their networks, for the administrative functions within their networks and for any enterprise-level cloud applications.

With this method, it's not enough to just have your username and password. In order to log in to a workplace account, you'll need another "factor" to verify your identity, similar to needing both a key and an identification badge to gain physical access to a corporate building. This additional login hurdle means that cybercriminals won't be able to easily unlock your account, even if they have your compromised credentials in hand.

Key Protections

Although proper password management can prove beneficial, stolen credentials remain a common and pervasive cybersecurity threat. Even the most sophisticated passwords can be stolen, whether via brute-force techniques or advanced phishing scams. In these instances, all it takes is one compromised account to expose the entire company, potentially resulting in devastating and disruptive cyberattacks (e.g., account takeovers, data breaches or ransomware incidents).

Without MFA in place, you could be leaving personal information and sensitive projects stored on your workplace accounts, as well as your employer's larger corporate systems, vulnerable to cybercriminals. Using this method can help halt these hackers in their tracks, safeguarding both you and the company.

While MFA may seem like a tedious or unnecessary step in the login process, it's well worth it to avoid potential cybersecurity incidents. Technology company Microsoft confirmed that MFA can block over 99% of automated and bulk account compromise attacks, demonstrating its effectiveness.

Best Practices

When leveraging MFA at work, remember the following guidelines:

- **Use approved methods.** Adhere to company policies and any related

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

documentation on how to set up MFA services across your workplace accounts. Use only approved methods, whether it's a mobile authenticator application, biometric scanner, text messaging system or hardware key.

- **Pay attention to prompts.** Be prepared to comply with MFA prompts when logging in to your workplace accounts (e.g., “enter the unique code sent to your device” or “use facial recognition to approve login attempt”), as these prompts must usually be completed within a brief time frame. However, never follow or approve prompts you didn't initiate.
- **Report suspicious activity.** If you receive unexpected MFA requests, unusual prompts or other login problems, report them immediately.

For More Information

Cybersecurity can be challenging, but you don't have to navigate it alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Identifying and Responding to Phishing Scams

Phishing is a type of cyberattack that utilizes deceptive electronic communications to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. While emails are the most common delivery method of phishing scams, cybercriminals may also use text messages, social media interactions, fake or misleading websites, or even phone calls.

Employees are often targeted by phishing scams because they have access to valuable corporate systems, funds and data. These scams are among the most prevalent cybercrimes, with billions of phishing emails distributed each day. When these scams occur, they can lead to costly and disruptive cyber incidents, including data breaches and ransomware attacks. This article outlines common types of phishing scams, highlights red flags to watch for and explains what to do when you come across a suspicious message.

Common Phishing Scams

Top phishing tactics and formats include the following:

- **Deceptive phishing** is when a cybercriminal impersonates a recognized sender to steal personal data and login credentials. These emails often trick recipients by asking them to verify account information, change a password or make a payment.
- **Spear-phishing** schemes are typically aimed at specific individuals or companies and use personalized information to convince recipients to share their data. In these instances, cybercriminals will research a target's online behavior—such as whom

they report to in their department and the co-workers they speak to most—to collect personal details that make them seem legitimate.

- **Vishing**, or “voice phishing,” occurs when a criminal calls a recipient's phone to get them to share personal or financial information. These scammers often disguise themselves as trusted sources, such as a bank or the IRS, and rely on creating a sense of urgency or fear to trick a target into giving up confidential information.
- **Smishing** refers to “SMS phishing” and incorporates malicious links into SMS text messages. These messages often appear to be from a trustworthy source and lure recipients in by offering a coupon code or a chance to win a free prize.
- **Pharming** redirects a target to a website of the cybercriminal's choosing by installing a malicious program onto their device. The goal is to have users input their login credentials or personal information, such as credit card numbers, on the fraudulent site.

Red Flags to Watch for

Here are some red flags you can watch for to help identify potential phishing scams:

- **Unknown or copycat senders**—This includes unverified numbers, profiles or email addresses, especially those claiming to be trusted individuals or organizations.

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

Some cybercriminals may even hack into real accounts or copy legitimate email addresses, only changing one character.

- **Threatening, generic or error-ridden language**—These messages may contain an unnerving sense of pressure or urgency, pushing you to take immediate action on a specific matter to obtain a reward or avoid potential consequences. They may also lack personalized greetings (e.g., “Dear account holder”) or use poor spelling or grammar.
- **Unsolicited links or attachments**—This includes hyperlinked words and images with mismatched URLs and password-protected files with uncommon file extensions (e.g., .exe, .zip, .scr, .iso or .jar) or vague naming conventions. You should be particularly wary of opening links or attachments that you didn’t initially request.
- **Sensitive requests**—These messages may ask you to disclose private information, such as your login credentials or workplace records, or demand that you perform unusual tasks, such as using company funds for wire transfers or downloading new software.

- **Delete it.** Once the message has been properly reported, be sure to remove it from your inbox (including the trash or spam folders), if applicable.

For More Information

Cybersecurity can be challenging, but you don’t have to navigate it alone. Reach out to your employer for more information on cybersecurity best practices.

Handling Suspicious Messages

If you receive an unusual or off-putting message and suspect a phishing scam, take the following steps:

- **Don’t interact.** Refrain from responding to the message, answering any prompts, or opening embedded links or attachments.
- **Verify the request.** If the message claims to be from a trusted individual or organization and includes a sensitive request, use an alternative method (e.g., a verified phone number or email address) to contact the supposed sender and verify the request.
- **Report it.** When you are unable to verify a message, report it immediately. Depending on the message’s nature and format, this may entail forwarding it to designated IT staff or using a built-in email alert system (e.g., a “report phishing” button) to flag it for further review.

CYBERSECURITY ESSENTIALS

The Value of Using a Virtual Private Network

A virtual private network (VPN) uses an encrypted connection to route internet traffic through a remote server, granting a user access to certain digital services while masking their online activity. Connecting to a VPN establishes a secure tunnel between a user's device and the internet, making it appear as though they are browsing from the server's location and protecting their data from interception by malicious parties.

VPNs are a crucial cybersecurity tool for many companies, particularly those that permit employees to work from different locations and use public Wi-Fi networks. This article provides more information on the benefits of a VPN, when to use it and how to safely connect.

The Benefits of a VPN

Using a VPN can benefit both you and your employer in several ways:

- **Enhanced asset protection**—This tool is designed to help you keep a secure internet connection when accessing corporate information and infrastructure, such as files, emails and applications. This is most important when you are working remotely, whether from home or in public settings (e.g., hotels, airports or coffee shops).
- **Reduced cyberattack exposures**—Using a VPN can halt hackers in their tracks, blocking various types of eavesdropping and certain account compromise attempts. This, in turn, can limit the likelihood of subsequent data breaches and ransomware attacks.
- **Bolstered compliance**—Maintaining a secure VPN can support your employer's efforts to meet applicable data protection requirements, thereby reducing the risk of related legal penalties.

Provided by Connor & Gallagher OneSource

When to Use a VPN

It's best to use your workplace VPN in these circumstances:

- Whenever you are off the corporate network (e.g., remote work or business travel)
- Prior to accessing sensitive internal databases, systems and shared drives
- Anytime you have to connect to a public or otherwise untrustworthy Wi-Fi network

Remember to review your employer's VPN policy for any additional usage requirements.

Ensuring a Safe Connection

In some cases, your workplace device may automatically connect to the VPN when you sign in to your account. If you must manually connect, follow these general guidelines:

- Log in to your device and open the designated VPN application.
- Provide your credentials when prompted. You may also be asked to complete a multifactor authentication request.
- Click "connect" to create a secure, encrypted tunnel to the corporate network via the VPN server.

Keep in mind that specific setup instructions may vary between different VPN applications. Consult your employer for detailed guidance. If you experience issues connecting to the VPN

or suspect any unusual network activity, report these concerns immediately.

For More Information

VPNs are a valuable safeguard that can protect both you and your employer. However, it's worth noting that these tools contain some limitations. In particular, VPNs can't defend against phishing scams, previously compromised account credentials or malware that has already been deployed on a workplace device. As such, it's imperative to use your workplace VPN alongside other cybersecurity tools and precautions to ensure maximum protection.

Cybersecurity can be challenging, but you don't have to navigate it alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Safe Internet Browsing Practices

Whenever you connect to the internet at work, you create a potential entry point for cybercriminals. Every link you click and website you visit is an opportunity for hackers to gain a foothold and infiltrate sensitive company systems and data. Fortunately, many of these incidents are preventable with a few smart habits.

You don't need to be a security expert to stay protected online. By adhering to safe internet browsing practices, you can better defend yourself and your employer against cyberthreats. This article provides more information on common internet risks, outlines browsing do's and don'ts, and offers tips to handle suspicious activity.

Common Internet Risks

As you browse the internet at work, it's important to be aware of the following risks:

- **Spoofed or lookalike websites**—Cybercriminals may create convincing copycat websites of trusted domains to trick you into clicking on harmful URLs during online searches. Once you've landed on a spoofed website, hackers may hijack your device or inject it with viruses.
- **Suspicious pop-up messages**—While browsing the internet, you may receive unexpected pop-up messages with various claims, often urging you to provide your login credentials or other sensitive information in exchange for a prize or device upgrade. These pop-ups are usually phishing scams intended to deploy account takeovers and data breaches.
- **Harmful software**—When downloading seemingly harmless workplace attachments or programs from the internet, these files

may be infected with harmful software. Upon download, this software could pave the way for destructive ransomware attacks.

Browsing Do's and Don'ts

Given these risks, it's crucial to implement robust online safeguards. When browsing the internet on the job, remember to always:

- Connect to the company's virtual private network, especially when working remotely or using public Wi-Fi.
- Use only approved web browsers and extensions. Ask your employer for an approved list if you are unsure.
- Keep web browsers and any related plugins up to date.
- Verify URLs before clicking on them, looking for minor changes in the domain name.
- Use websites containing HTTPS whenever possible. This can help block hackers from eavesdropping and accessing the data sent between your device and the website.

In addition, you should never:

- Browse unfamiliar or suspicious websites.
- Download unanticipated attachments, software or extensions, particularly from unknown sources.
- Enter account credentials or other sensitive data into unverified pop-ups or domains.

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

Handling Suspicious Activity

If you come across anything suspicious while browsing the internet at work, whether it's an off-putting website, unexpected pop-up message or potentially dangerous file, take these steps:

- Never ignore your instincts. If something seems off, don't engage with it.
- Report any suspicious online activity immediately. Contact the IT or security team and follow their instructions before taking any further action on your device.
- Don't try to investigate or remedy a potential cyberattack by yourself. Always notify others and ask for assistance.

For More Information

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Password Management Best Practices

Strong passwords are one of the first lines of defense against cyberattacks. Developing lengthy, complex and hard-to-guess passwords across your workplace accounts can significantly increase the time and computing power required to crack your credentials, making it far more difficult for cybercriminals to gain unauthorized access to sensitive systems and data.

With this in mind, it's crucial to understand how to create effective passwords and, in turn, better protect your workplace accounts. This article highlights the key pillars of a strong password and offers additional tips to safeguard your credentials on the job.

Key Pillars of a Strong Password

When developing passwords for your workplace accounts, remember these guidelines:

- **Make it lengthy.** Every additional character in a password multiplies the number of possible combinations a cybercriminal must guess to exploit your credentials. A good password length is generally 15 or more characters. Using a combination of uppercase and lowercase letters, numbers, and symbols can also vastly complicate a hacker's ability to steal your password.
- **Never include personal information.** Cybercriminals may gather public records and social media posts to uncover your personal information and use these details to compromise your credentials. As such, refrain from incorporating family or pet names, your favorite hobbies or sports teams, or special dates (e.g., birthdays and anniversaries) within your passwords.

Provided by Connor & Gallagher OneSource

- **Avoid predictable patterns.** Common character combinations (e.g., "welcome123," "p@ssw0rd," "qwerty" or "letmein") are among hackers' first guesses when attempting to swipe a password. In many situations, these combinations can be uncovered in mere seconds. The most effective passwords usually involve a string of four or more words or unique characters that form a memorable, albeit random, sentence (e.g., "@pplesRtheB3stFruit!"). Also known as passphrases, these combinations are often the hardest to crack.
- **Don't reuse or repeat.** If you use the same passwords across different workplace (and personal) accounts, you could be increasingly vulnerable to credential stuffing—a tactic in which cybercriminals use one stolen password to compromise multiple accounts and associated systems. Be sure to vary your passwords between accounts and never reuse previous combinations.

Safeguarding Your Credentials

Keep in mind that your passwords aren't permanent. Your workplace systems and related applications may prompt you to change your passwords at set intervals (e.g., quarterly or semiannually). It's also best to update your passwords if you suspect that your account has been compromised or if you are notified that a service or platform you use has been breached. When creating your passwords,

keep these credentials private. Never, under any circumstances, share your passwords with others.

While you may be tempted to use a physical notebook or a plain-text document stored on a personal device to keep track of all your passwords, this is a dangerous practice, as this confidential information could end up in the hands of a malicious party. Rather, it's important to leverage any password tools and further credential safeguards provided by your employer to keep your accounts safe. These resources may include:

- **Password managers**—A password manager stores and organizes your credentials in a digital vault, often secured by a master password and/or biometric identifier (e.g., a fingerprint or facial scan). When it's time to sign into your account, this tool automatically enters your login information. Using a password manager can help you maintain unique credentials while removing the burden of memorizing these complex combinations.
- **Multifactor authentication (MFA)**—Through MFA, you must confirm your identity by providing extra information, such as a phone number, biometric identifier, one-time security code or approval from a third-party authenticator application, in addition to your password when attempting to access sensitive corporate data and infrastructure. Many companies require MFA to access their networks, perform administrative functions within these networks and use enterprise-level cloud applications.

Talk to your employer to review the specific resources available to you. Furthermore, if you run into any problems when signing into workplace accounts or notice signs of suspicious activity (e.g., unexpected logins or password reset emails), report these issues immediately.

For More Information

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Identifying and Responding to Business Email Compromise Scams

Cybercriminals continue to become more sophisticated, leveraging a wide range of tactics in order to attack their targets. One tactic that has increased in frequency, complexity and resulting losses over the past few years is the use of business email compromise (BEC) scams.

A BEC scam entails a cybercriminal impersonating a seemingly legitimate source—such as a senior-level employee, supplier, vendor, business partner or other company—via email. The cybercriminal uses these emails to gain the target's trust, tricking them into believing they are communicating with a genuine sender. From there, the cybercriminal convinces their target to wire money, share sensitive information or engage in other compromising activities.

BEC scams can lead to numerous consequences for both you and your employer, including account exploitation, stolen data and lasting financial hardship. As such, it's crucial to understand these scams and how to mitigate them. This article outlines common BEC tactics, highlights red flags to watch for and explains what to do when you come across a suspected scam.

Common BEC Tactics

BEC scams involve cybercriminals impersonating individuals or entities within their targets' trusted networks for malicious gain. These scams are categorized as a form of social engineering. This broader cyberattack method preys on key human behaviors (e.g., trust in authority, fear of conflict and the

promise of rewards) to obtain unwarranted access to corporate systems, funds or data.

According to the FBI, there are several different types of BEC tactics, including:

- **False invoice scheme**—With this tactic, a cybercriminal impersonates a company supplier to trick their target into transferring funds to a phony account.
- **CEO fraud**—This tactic entails a cybercriminal impersonating a senior-level employee or executive and requesting that their target conduct a wire transfer to a fake account. The request often threatens the target with work-related consequences or other punishments for failing to comply.
- **Account compromise**—Through this tactic, a cybercriminal hacks into an employee or executive's actual email account and sends messages to various contacts, attempting to fool these recipients into sharing corporate data or paying fraudulent invoices.
- **Attorney impersonation**—This tactic refers to a cybercriminal impersonating a lawyer or other legal representative and requesting a payment be made to a phony account in order to handle a corporate matter deemed "sensitive" or "pressing."
- **Data theft**—With this tactic, a cybercriminal impersonates an HR professional to trick their target into sharing private information about employees or executives. The

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

cybercriminal can then leverage this data during future attacks.

Red Flags to Watch for

Even though BEC scams can be convincing, there are some red flags you can watch for:

- Messages that lack personalization; contain awkward phrasing; or have glaring spelling, formatting or grammatical errors (although scams powered by artificial intelligence tools may appear polished and error-free)
- Mismatched domains or reply-to addresses, especially those that closely mirror a genuine website or account, with the exception of a single character (e.g., janedoe@samplecompanyy.com versus janedoe@samplecompany.com)
- Unusual requests from known or otherwise trusted contacts, particularly those that push you to act fast, click on suspicious links or attachments, bypass company protocols, or keep the interaction a secret

Handling a Suspected BEC Scam

If you receive an unusual message and suspect a BEC scam, take these steps:

- **Don't interact.** Refrain from immediately responding to the message, fulfilling any requests, or opening embedded links or attachments.
- **Follow verification protocols.** Never, under any circumstance, bypass your employers' verification requirements for sharing sensitive data, paying invoices or otherwise transferring corporate funds. These requests should be carefully analyzed and discussed with multiple parties—such as management, HR and accounting professionals, and the supposed sender—either in person or over the phone to confirm their validity, especially if they involve alternative payment procedures.
- **Report it.** When you are unable to verify a message or related request, report it immediately. This may entail forwarding it to

designated IT staff or using a built-in email alert system to flag it for further review.

- **Delete it.** Once the message has been properly reported and investigated, be sure to remove it from your inbox (including the trash or spam folders).

For More Information

BEC scams are a growing threat, but staying informed is your best defense. By recognizing common tactics, watching for red flags and following proper verification protocols, you can help defend yourself and your employer against costly breaches. When in doubt, verify before you act, and always report suspicious activity promptly.

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Identifying and Responding to Deepfake Scams

Deepfakes refer to sophisticated forgeries of images, videos or audio recordings. They have been around for years; you can even find versions of them on social media applications. For example, with Snapchat, face-changing filters take real-time data and feed it through an algorithm to produce a synthetic image.

However, as technology has evolved, deepfakes can now alter media so well that it's often difficult to detect any manipulation. Using artificial intelligence (AI) tools, deepfakes leverage existing audio and video of an individual and continuously learn to produce increasingly convincing forgeries. As a result, deepfakes have become so advanced that they can deceive people into thinking trusted individuals have said or done something they normally wouldn't.

In today's workplace, cybercriminals have begun using deepfake scams to sway public opinion on business leadership and trick employees into divulging sensitive information or wiring corporate funds. These scams can lead to numerous consequences for both you and your employer, including stolen data and lasting financial and reputational hardship. As such, it's crucial to understand deepfake scams and how to mitigate them. This article outlines common deepfake tactics, highlights red flags to watch for and explains what to do when you come across a suspected scam.

Common Deepfake Tactics

While deepfakes were historically used to impersonate political figures in "fake president scams," cybercriminals are now using them to pose as key stakeholders (e.g., CEOs, board members, managers, IT or HR professionals,

vendors and business partners) and target companies across industry lines in damaging attacks. Using these forgeries, malicious parties can fool even the most perceptive individuals.

Some common deepfake tactics leveraged against businesses and their staff include:

- **Social engineering plots**—Social engineering is a broader cyberattack method that preys on human behaviors (e.g., trust in authority, fear of conflict and the promise of rewards) to obtain unwarranted access to corporate systems, funds or data. Because AI-powered deepfakes have become less expensive and more accessible over the years, the prospect of tricking an employee into performing compromising actions through social engineering plots, whether it's a deceptive video conference or fraudulent voicemail, has grown that much easier.
- **Public manipulation**—By deepfaking a company's CEO or other figureheads, cybercriminals can quickly spread false or potentially damaging information. These forgeries can make key stakeholders say or do just about anything. They could have a board member share false business plans, say or do socially unacceptable things or attempt to influence consumer behavior. All of these actions can harm a company's reputation, sometimes irreparably.

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

Red Flags to Watch for

Although deepfake scams can be convincing, there are some red flags you can watch for:

- **Visual cues**—The people portrayed on deepfaked video conferences may blink or move their heads awkwardly, appear somewhat blurry, have inconsistent background lighting, or speak out of sync with their audio.
- **Audio cues**—During both deepfaked video conferences and phone calls, voices may sound robotic, have odd pacing or be interrupted by suspicious background noise.
- **Behavioral cues**—The conversations that take place amid deepfaked interactions may feel unnatural or lack certain social cues. They also often include a heightened sense of urgency, requests that bypass company protocols and pressure to keep specific details of the conversation secret.

In addition to these red flags, your employer may have tools or systems in place to help detect potential deepfakes, such as using company-issued code words when discussing sensitive matters or advanced detection technology that alerts you to suspected forgeries. Be sure to familiarize yourself with any available resources.

Handling a Suspected Deepfake Scam

If you attend an unusual video conference or receive an unexpected phone call and suspect a deepfake scam, take these steps:

- **Pause and reflect.** Take a moment to evaluate the interaction and trust your instinct if anything feels off. Refrain from immediately fulfilling any requests made during the conversation, even if they are deemed urgent.
- **Verify all requests.** Never, under any circumstance, bypass your employer's verification requirements for sharing sensitive data or wiring corporate funds. These requests should be carefully analyzed and discussed with multiple parties—such as management, HR and accounting

professionals, and the supposed sender—through trusted channels (preferably in person) to confirm their validity, especially if they involve alternative payment procedures.

- **Report the conversation.** If you are unable to verify an interaction or related request, report it right away. This may entail discussing the origin and details of the conversation with designated IT staff or using a built-in alert system on your laptop or mobile device to flag the interaction for further review.

For More Information

Deepfakes are a growing threat, but staying informed is your best defense. By recognizing common tactics, watching for red flags and following response measures, you can help protect yourself and your employer against potential scams. When in doubt, verify before you act, and always report suspicious interactions promptly.

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Identifying and Responding to Ransomware Attacks

Ransomware is malicious software that infects a device and either prevents it from working as intended or restricts access to certain files until the target pays a ransom. Typically, the cybercriminals behind ransomware demand payment in cryptocurrency, such as bitcoin, which allows them to collect funds outside the traditional banking system. Businesses of all sizes have become targets of ransomware, as it can infect not only personal devices but also entire networks and servers.

Employees are often the initial targets in ransomware attacks due to their access to valuable corporate systems, funds and data. These attacks often start with phishing scams, in which cybercriminals leverage deceptive emails or other forms of communication to manipulate employees into visiting unsafe websites, clicking on harmful attachments or downloading dangerous programs that ultimately launch malicious software.

When these incidents occur, they can lead to prolonged operational disruptions and serious financial challenges for your employer. In fact, these attacks are among the costliest cybercrimes, resulting in billions of dollars in losses each year. As such, it's crucial that you play your part in preventing these attacks. This article explains what ransomware does to a device, outlines potential warning signs and offers related mitigation strategies.

What Ransomware Does to a Device

There are two main types of ransomware that can hold devices (and any systems and data stored on them) hostage. This includes:

- **Lock-screen ransomware**—This software works by displaying a window on the device's lock screen that attempts to prevent access to it. The message on the lock screen may even claim to come from the federal government, accuse the target of violating a law and demand a fine.
- **Encryption ransomware**—This software works by keeping the device available but encrypting certain types of files, thus making them unreadable. The files most commonly targeted are those containing sensitive information, which cybercriminals assume are of the greatest value. When people try to access the files, they see a pop-up screen that instructs them to buy a private decryption key to unlock the scrambled files.

Some operating systems provide instructions for responding to lock-screen ransomware, although results aren't guaranteed. In contrast, encryption ransomware has no quick fix without an encryption key, which only the cybercriminals typically have access to.

Warning Signs of an Attack

In the lead-up to a ransomware attack, you may notice the following warning signs on your device:

- Sluggish performance (e.g., applications taking longer to open or closing unexpectedly, websites loading slower than normal or simple tasks freezing)

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

- Files suddenly being renamed, using unfamiliar extensions or restricting access
- Unusual network activity, especially within shared drives and cloud storage

While these issues can occur, they may not be obvious. In some cases, you might not detect any warning signs of a ransomware attack, with the first and only indicator being a locked screen or ransom note.

Mitigation Strategies

The best way to mitigate a ransomware attack is to prevent it from occurring in the first place. This primarily entails keeping all security software on your device up to date, creating complex and unique passwords across your workplace accounts and enabling any additional company safeguards, such as a virtual private network, data encryption tools, firewalls, patch management systems, antivirus programs and multifactor authentication services. Ask your employer for more information on these resources.

Furthermore, since many ransomware attacks stem from phishing scams, it's best to be prepared to identify key indicators of these scams (e.g., unknown or copycat senders, generic or threatening language, unsolicited links or attachments and unusual or sensitive requests) and act accordingly. Never respond to these messages or answer any prompts without first verifying them through an alternative channel.

Even with these precautions in place, ransomware attacks may still occur. If you notice any warning signs of an impending attack, experience a locked screen or receive a ransom note, take these steps to help minimize the damage:

- **Don't interact.** Never interact with a ransom note or comply with other demands from a cybercriminal. Regardless of the circumstance, experts advise against paying the ransom, as there's no guarantee the cybercriminal will restore your device after payment. By paying the ransom, you could also be encouraging future cybercrimes against your employer. In addition, don't panic or take matters into your own hands

by trying to recover any affected systems or data yourself, as this could cause more harm than good.

- **Report it.** Whether it's suspected or genuine, inform the IT team of the incident immediately. From there, the team will determine appropriate next steps. In some cases, this may involve internal remediation efforts. For more severe incidents, this may entail an in-depth investigation with the Cybersecurity and Infrastructure Security Agency (CISA), the FBI and local authorities.
- **Document any evidence.** Depending on the nature of the attack, you may be asked to share any relevant details you can recall about the incident, such as initial warning signs and ransom note phrasing. With this in mind, be sure to take notes regarding what you noticed and when. This could help support the investigation process and promote a faster recovery.

For More Information

Ransomware poses a serious threat to both your device and your employer's broader systems and data. By staying alert to warning signs, practicing strong cyber hygiene and knowing how to respond if an attack occurs, you can help minimize the associated damage and disruptions.

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Remote Work Best Practices

Working remotely offers flexibility, but it also expands the ways cyberthreats can reach you. Outside the office, the usual safety nets, namely IT oversight, threat detection tools and physical security, may not be readily available. This, in turn, can permit cybercriminals to exploit potential vulnerabilities and launch damaging attacks.

A weak Wi-Fi password, a convincing phishing email or an unlocked laptop left unattended can all open the door to serious risks, both for you and your employer. Fortunately, many of these risks can be managed with smart habits. This article provides more information on common remote work threats and related mitigation strategies.

Common Remote Work Threats

Cybercriminals have been targeting businesses for decades, continually seeking new ways to compromise confidential systems and data. Depending on a company's size, it may receive dozens or thousands of attack attempts each day. These attempts are typically blocked by IT teams and workplace security tools. However, when employees work remotely, these safeguards aren't guaranteed.

Here are some of the most common cyberthreats facing remote workers:

- **Malware**—Malicious software, also called malware, is software designed to damage, disrupt or gain unauthorized access to devices, networks or data. Malware includes viruses, ransomware, spyware, trojans and other harmful programs. This software can perform a variety of tasks, typically hidden from the user. For instance, they might store passwords, track website activity or download personal files.
- **Brute-force attacks**—This attack method involves repeated attempts to log into someone's account until their credentials are cracked. Such attacks also frequently use credential-stuffing tactics, where usernames and passwords stolen from one breach are automatically tested against other accounts. These attempts are most successful when individuals reuse credentials across multiple accounts.
- **Shoulder-surfing incidents**—This attack method involves cybercriminals stealing sensitive data, whether it's through no-tech means (e.g., peeking over an employee's shoulder and writing notes on what they see), low-tech means (e.g., zooming in on a smartphone camera to peer at classified records from a distance) or high-tech means (e.g., leveraging a professional camera and other advanced equipment to surreptitiously record confidential information displayed on a screen).
- **Phishing scams**—This attack method utilizes deceptive electronic communications to manipulate recipients into sharing sensitive information, clicking on dangerous links or opening harmful attachments. While emails are the most prevalent delivery method for phishing scams, cybercriminals may also use text messages, social media interactions, fake or misleading websites, or even phone calls.

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

Altogether, these threats can lead to costly and disruptive attacks, such as data breaches, account takeovers and ransomware incidents.

Mitigation Strategies

Considering the risks of remote work, it's crucial to take steps to boost your security. Whether you are working from home or a public location (e.g., a hotel, airport or coffee shop), follow these best practices:

- **Protect your device.** Only use devices specifically designated for work purposes. Never allow family or other household members to use these devices. When working from home, ensure a secure connection to your private Wi-Fi network, regularly update your router's firmware and lock your device whenever it's not in use. When working from a public location, maintain a proper distance from onlookers, dim your screen to make it harder for others to read and don't leave your device unattended. In any location, always connect to your employer's virtual private network or other secure access solution before handling company resources and keep all security software up to date.
- **Maintain data security.** Keep sensitive information safe by using only company-approved tools and applications for communication (e.g., email, direct messaging and video conferencing) and file sharing. Remain aware of your physical surroundings and the visibility of your screen to ensure maximum privacy.
- **Ensure strong passwords.** Utilize complex and hard-to-guess passwords across your work accounts, applications, devices and, if applicable, your household Wi-Fi network. Passwords should be at least 15 characters; use a combination of uppercase and lowercase letters, numbers and symbols; and spell out unique, unpredictable phrases (e.g., "@pplesRtheB3stFruit!"). Never reuse or repeat passwords or share your credentials with others. In addition to creating strong passwords, use your employer's multifactor authentication services as an extra layer of security.

- **Recognize phishing scams.** Be prepared to identify key indicators of phishing scams (e.g., unknown or copycat senders, generic or threatening language, unsolicited links or attachments, and unusual or sensitive requests) and act accordingly. Never respond to these messages or answer any prompts without first verifying them through an alternative channel.
- **Enable company safeguards.** Ensure corporate security tools remain enabled on your device, including endpoint protection software, host firewalls and automatic updates. Ask your employer for more information on these resources.
- **Report potential incidents promptly.** If you notice any unusual activity or suspect a possible cyberthreat while working remotely, report these issues immediately. This may entail using a built-in alert system on your device, flagging concerning messages or other content for further review, or contacting the IT team directly.

For More Information

Cyberattacks targeting remote workers are an ongoing, pervasive threat; nevertheless, you aren't defenseless against them. By understanding key risks and implementing proper precautions, you can help stay one step ahead of cybercriminals.

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

CYBERSECURITY ESSENTIALS

Don't Become an Insider Threat

An insider threat refers to an individual who has been entrusted with access to or knowledge of a company's confidential resources and information. Due to their unique privileges, insider threats can compromise organizations' most valuable assets and leave them increasingly vulnerable to cyberattacks, also known as insider events.

You may think that insider threats are primarily malicious individuals (e.g., disgruntled staff or fraudulent vendors) intentionally abusing their access to engage in harmful activities for personal gain, but the reality is quite the opposite. Many insider threats are actually well-meaning employees who unknowingly expose their company's data and assets to unauthorized parties. This is often due to a lack of experience, awareness or attentiveness to potential security risks, making them more error-prone and easily manipulated by cybercriminals' tactics.

The Ponemon Institute has found that 55% of insider events stem from well-meaning employees. Additionally, IBM's Cyber Security Intelligence Index found that human error is a factor in 95% of cyber incidents. As such, it's crucial to take steps to avoid becoming an insider threat and putting your employer at risk. This article outlines habits that may lead to cybersecurity exposures, highlights several insider threat scenarios and explains what you can do differently.

Risky Habits

As an employee, you represent the most prevalent type of insider threat. Some everyday habits that can create cybersecurity risks include:

- Reusing passwords across work accounts or sharing credentials with others (even trusted co-workers)
- Clicking unverified links, downloading unanticipated attachments or otherwise interacting with suspicious messages sent by unfamiliar parties
- Oversharing certain company information (e.g., project details or organizational structures) on social media
- Rushing through work assignments and risking additional mistakes, especially when handling sensitive data or assets
- Using unapproved devices or applications to complete work assignments
- Losing or leaving workplace devices in public settings (e.g., airports, hotels or coffee shops)
- Neglecting to regularly review workplace cybersecurity policies and related documentation or attend awareness training
- Ignoring routine software updates or failing to enable company-provided cybersecurity tools, such as a virtual private network (VPN) or multifactor authentication (MFA)

Even the most diligent employees may engage in these habits, whether out of perceived convenience, pressure to meet project deadlines, risk fatigue or complacency, misplaced trust, or overdependence on existing

Provided by Connor & Gallagher OneSource

This Cybersecurity Essentials document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.

security resources. When left unchecked, these habits can cause serious consequences.

Insider Threat Scenarios

Here are some insider threat scenarios involving well-meaning employees:

- An employee is deceived by a phishing scam, in which a cybercriminal impersonates a manager via email and manipulates the employee into sharing their login credentials, thereby giving the perpetrator unauthorized access to the company's larger IT infrastructure.
- An employee doesn't review company resources and forgets to attend training on a new type of workplace software, resulting in them making several errors while using this technology and compromising the sensitive data stored on it.
- An employee rushes through their work assignments and makes multiple mistakes, ultimately sending confidential business files to the wrong recipients and downloading a malicious program disguised as a software update.

What You Can Do

To minimize the risk of insider events and play your part in promoting strong cybersecurity on the job, follow these guidelines:

- **Maintain account security.** Utilize complex and hard-to-guess passwords across your work accounts. Passwords should be at least 15 characters; use a combination of uppercase and lowercase letters, numbers and symbols; and spell out unique, unpredictable phrases (e.g., "@pplesRtheB3stFruit!"). Never reuse or repeat passwords or share your credentials with others. Alongside strong passwords, use your employer's MFA services as an extra layer of account security.
- **Safeguard devices and data.** Only use devices specifically designated for work purposes, and refrain from sharing them with others. If you work from home, ensure a secure connection to your private Wi-Fi network, regularly update your router's

firmware and lock your device whenever it's not in use. When working in a public setting, never leave your device unattended. In any location, always connect to your employer's VPN or other secure access solution before handling corporate assets and keep all security software up to date. Furthermore, use only approved applications for communication (e.g., email, direct messaging and video calls) and file sharing.

- **Think before you act.** Be cautious of sharing company information online, especially via public social media accounts. Also, be ready to identify key indicators of phishing scams (e.g., unknown or copycat senders, generic or threatening language, unsolicited links or attachments, and unusual or sensitive requests) and act accordingly. Don't respond to these messages or answer prompts without first verifying them through an alternative channel.
- **Take your time.** Avoid rushing through work assignments or taking any shortcuts to meet deadlines, as this could increase the likelihood of mistakes and related cybersecurity issues. Never be afraid to ask for help or additional support if you are feeling overwhelmed by your task load.
- **Leverage company resources.** Make the most of all cybersecurity protections available to you. This may entail reviewing workplace policies, attending training sessions and ensuring corporate security tools (e.g., endpoint protection software, host firewalls and automatic updates) remain enabled.
- **Report suspicious activity.** If you notice any unusual activity or suspect a possible cyberthreat, report it immediately. This may entail using your device's built-in alert system, flagging concerning messages or other content for further review, or contacting the IT team directly.

For More Information

Cybersecurity can be challenging, but you don't have to navigate this topic alone. Reach out to

your employer for more information on cybersecurity best practices.

Conclusion

By investing in employee awareness, employers can foster a strong culture of cybersecurity, where small habits add up to meaningful protection for the entire organization. Above all, making cybersecurity a shared priority rather than an isolated initiative can help employers build lasting resilience, protect valuable data, and support a workforce that feels confident and equipped to face an ever-changing digital landscape.

Contact us today for additional Cybersecurity Awareness Month resources and content solutions that expand beyond this annual campaign, including in-depth guides, checklists, case studies, scorecards, articles and infographics.