

SWC

Tax planning and financial strategy.
Simplified.©

Cybersecurity Awareness Month: Timely Tips to Protect You and Your Business

©2026 SWC (Stees. Walker & Company, LLP) | All rights reserved. | No portion of this singlet may be used without the express and written permission of SWC

Think about all the sensitive information that passes through your computer or phone every single day. You might check your bank account, open an investment statement, send a tax document, approve a payment, access payroll information, make a purchase, or receive an email from someone who appears to be a customer or vendor.

Each interaction creates another reason to pay attention to cybersecurity.

October is Cybersecurity Awareness Month, an annual campaign led by the Cybersecurity and Infrastructure Security Agency (CISA). For 2026, the theme is “Securing the Next 250,” recognizing the nation’s 250th anniversary and encouraging individuals and organizations to take practical steps that support a safer digital future.

For individuals, cybersecurity often starts with protecting the accounts and devices that contain your personal and financial information. Businesses face those same concerns while also managing employee access, customer and vendor information, business systems, and the ability to continue operating after a disruption. Cybersecurity Awareness Month provides a good reason to review both.

For Individuals: Make Your Accounts Harder to Compromise

Many cybersecurity precautions begin with something familiar: the accounts you use every day. Your email account deserves particular attention because it often connects to other services. Password-reset messages, financial notifications, tax correspondence, and account verification requests may all arrive there. Someone who gains access to your email may be able to use that access in attempts to compromise other accounts.

Start by reviewing the accounts that contain sensitive information or provide access to it. These may include email, banking, investment, accounting, tax, shopping, and social media accounts.

Use Unique Passwords and a Password Manager

Reusing the same password across several accounts creates unnecessary exposure. If someone obtains that password from one compromised account, they can try the same

Continued onto next page

credentials elsewhere. Even worse? They can sell your information to the highest bidder through the dark web.

CISA and the National Institute of Standards and Technology (NIST) recommend password management tools such as 1Password, Apple Passwords, and Proton Pass as a way to create and store passwords rather than relying on passwords that are easy to remember or repeatedly reused. https://www.nist.gov/itl/smallbusinesscyber also recommends changing default passwords and protecting important accounts with passwords that differ from those used elsewhere. A password management tool can make that process easier because you do not have to memorize every password yourself.



Add Multifactor Authentication

A password should not have to do all the work. Multifactor authentication, commonly called MFA or 2FA for two factor authentication, requires another form of verification before granting access to an account. Depending on the service, that second step might involve an authentication application, security device, biometric identifier, or another verification method. MFA and 2FA tools to consider using include Authy, Okta, and Google Authenticator.

CISA recommends requiring MFA or 2FA wherever possible for business systems and using phishing-resistant MFA when available. For individuals, the same principle makes sense for accounts containing sensitive information. Email and financial accounts deserve particular attention, along with tax and accounting services.

NIST's Small Business Quick-Start Guide specifically identifies banking, accounting and tax accounts among the types of accounts where MFA should be considered.

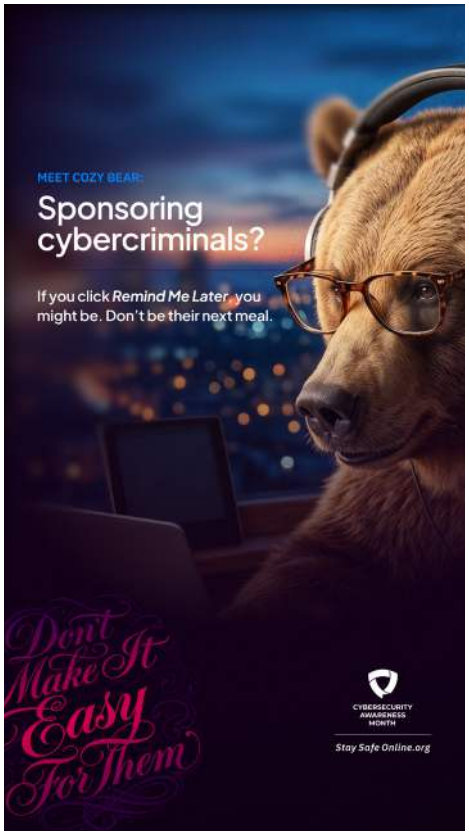
Think Before You Click, Reply, or Pay

Cybercriminals frequently rely on people to provide the access they need. A message may appear to come from your bank, a delivery service, a government agency, your employer, a website you frequently make purchases from, or someone you know. The message may ask you to click a link, open a document, confirm account information, send money, or act immediately.

Urgency should give you a reason to inspect the request more closely. If an unexpected message asks for money, login credentials, financial information, or other sensitive data, verify the request using contact information you already trust. Avoid relying on a telephone number or link supplied in the suspicious message itself.

The Internal Revenue Service (IRS) gives similar instructions for suspicious tax-related communications. It advises taxpayers who receive suspicious IRS or Treasury emails to avoid

Continued onto next page



replying, clicking links, or opening attachments. The IRS also provides procedures for reporting suspicious emails, texts, websites, telephone calls, and other communications. (For additional guidance and warnings from the IRS, read IRS Dirty Dozen for 2026: 12 Tax Scams to Watch Out For on the SWC Blog.)

Consider an IRS Identity Protection PIN

Taxpayers have another security measure available specifically for federal tax returns: the IRS Identity Protection PIN, or IP PIN.

An IP PIN is a six-digit number that helps prevent someone from filing a fraudulent federal income tax return using your Social Security number (SSN) or Individual Taxpayer Identification Number (ITIN). Anyone with an SSN or ITIN who can verify their identity can enroll in the program. Parents and legal guardians may also request IP PINs for dependents.

The IRS generates a new IP PIN each year. You can generally enroll through your IRS Online Account, with alternative enrollment methods available in certain circumstances. Once an IP PIN applies, you need to use the applicable number when filing covered federal tax returns during that calendar year.

> **A Tax-Specific Security Step:** An IP PIN can add another barrier against someone using your identity to file a fraudulent federal income tax return. Keep the number private and provide it to your tax professional when preparing and filing your return. The IRS says it will never call, email, or text you asking for your IP PIN.

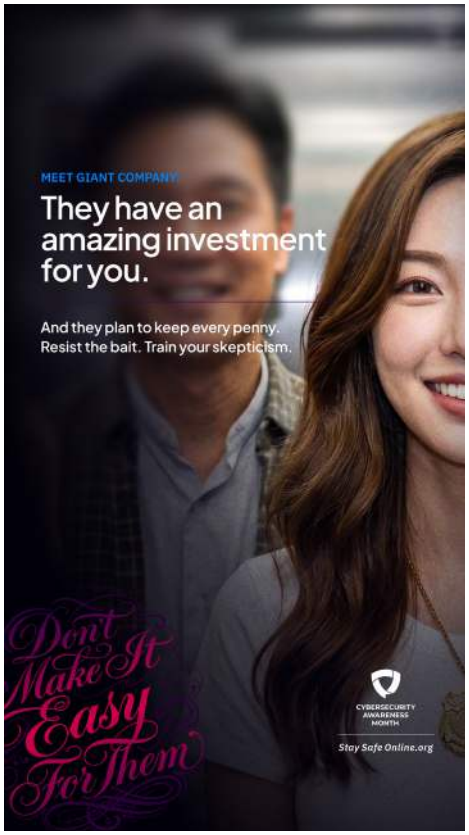
Know the Signs of Tax-Related Identity Theft

Sometimes the first warning comes when you try to file a return or receive correspondence concerning tax activity the taxpayer does not recognize. If the IRS contacts you about a return you did not file or asks you to verify your identity because of suspected tax-related identity theft, read the correspondence carefully and follow the IRS' instructions for your situation.

> **Identity Theft Affidavit:** Form 14039, Identity Theft Affidavit (PDF), may apply in certain circumstances, although most people experiencing identity theft do not automatically need to file it. The IRS identifies specific situations in which the form should or should not be used. Responding to suspected tax identity theft should follow the procedure appropriate to what actually occurred.

Continued onto next page

For Businesses: Treat Cybersecurity as a Business Risk



A business entity may hold far more sensitive information than its owners realize. Accounting records can contain bank information, payroll systems contain employee data, and email accounts may contain invoices, contracts, tax documents, and payment instructions. Vendors and outside service providers may also have access to your business information or systems.

The potential consequences of a cyber incident can extend well beyond a stolen password. An incident may interrupt operations, expose information, interfere with payments, or prevent employees from accessing the systems they need to work.

NIST's Cybersecurity Framework 2.0 Small Business Quick-Start Guide (PDF) approaches cybersecurity through six distinct functions:

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

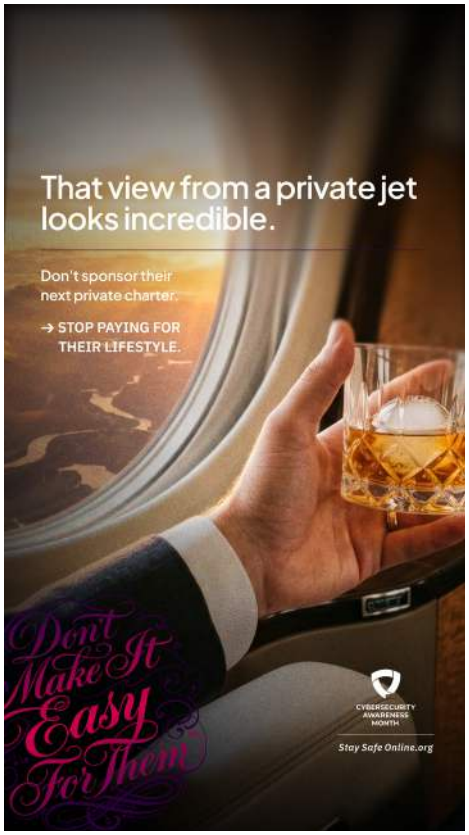
The guide was developed for small and medium-sized businesses, particularly those with modest or no existing cybersecurity plan. The framework provides a useful way to think about cybersecurity because businesses need to understand their risks and protect their systems. It also needs ways to recognize suspicious activity and respond when something happens, as well as restore operations afterward.

Get the Fundamentals Right

CISA recommends several basic practices for small and medium-sized businesses. Those recommendations include:

- Train employees to recognize and report phishing attempts
- Require unique passwords and make password managers available
- Require MFA, especially for administrative accounts, remote access, and employees handling sensitive information
- Install software security updates promptly
- Use logging and monitoring to identify unusual system activity
- Back up business data
- Encrypt sensitive business data

Continued onto next page



These measures address different parts of the same problem. Passwords and MFA / 2FA help control access. Software updates address known vulnerabilities. Logging can help a business detect unusual activity. Backups can support recovery when primary data or systems become unavailable. CISA provides small-business resources addressing each of these practices.

Your Employees and Vendors Are Part of the Plan

Business owners and managers should decide who owns the above responsibilities. Depending on the company's size and technology, that may involve internal employees, an outside information technology provider, a cybersecurity professional, or some combination of them.

Technology can block many threats, but employees still make decisions throughout the day that affect security. They open email attachments, receive requests to change payment instructions, create passwords, and access company systems from different locations. They may also be the first people to notice that something unusual has happened.

Employee education should therefore cover more than an annual reminder to "watch for phishing." Employees need to know what suspicious communications can look like, how to verify unusual requests, and where to report something that concerns them.

Management also sets the tone. When reporting a suspicious message takes only a few minutes and employees know whom to contact, they have a clearer path for raising concerns.

Look Beyond Your Own Business Systems

Few businesses these days operate entirely within their own technology. Payroll processors like Paychex, cloud software providers like Amazon Web Services, accounting platforms like QuickBooks, financial institutions, vendors, and other outside providers may store your company's information or connect with company systems.

NIST's Cybersecurity Framework recognizes cybersecurity supply-chain risk as part of cybersecurity risk management. For a business owner or manager, the practical question is straightforward: Who outside the company has access to important information or systems, and what happens if that access creates a problem?

Your business can start by identifying the providers that handle sensitive information or have system access. Contracts, access permissions, data-handling practices, and procedures for ending access when a relationship changes may warrant review with the appropriate technology and legal professionals.

Continued onto next page

Prepare for the Day Something Goes Wrong



While prevention deserves attention, you also need to think about response and recovery. CISA recommends that businesses develop and exercise an incident-response plan, a document that addresses who needs to become involved, how the business will respond to a ransomware incident or other disruption, and how important systems and data will be restored.

> **Backups:** Backups play a major role here. Your business should know what information it backs up and where those backups reside, as well as whether the data can actually be restored when needed.

The plan should also consider how the company would continue essential operations if normal systems or internet access became temporarily unavailable. A tabletop exercise revolving around these topics can expose gaps before an actual incident. Management, technology personnel, legal counsel, CPAs, and other appropriate advisers can work through a hypothetical incident and determine who would make decisions and what resources the company would need.

Watch for Business Tax Identity Theft

Businesses also face tax-specific identity theft. The IRS warns that criminals may use stolen business information to file fraudulent returns or commit other crimes. Warning signs can include an electronically filed return being rejected because another return has already been filed using the same Employer Identification Number (EIN) or Social Security number. A business might also receive an unexpected tax transcript or IRS notice, or stop receiving expected IRS correspondence because someone changed the business address.

If someone appears to be using a business name or EIN to file fraudulent tax returns or Forms W-2, Form 14039-B, Business Identity Theft Affidavit, may apply. The IRS identifies specific circumstances for filing the form and advises businesses against submitting it for a data breach that has no identified tax-related impact.

The IRS also recommends that businesses keep EIN information current and protect both business and employee data. Its security recommendations include unique passwords, password managers, MFA / 2FA, encryption, secure backups, access restrictions, and employee education.

Make Cybersecurity a Year-Round Practice

Cybersecurity Awareness Month gives individuals and businesses a reason to examine habits that can easily fade into the background during a busy year. For an individual, October might be the time to replace reused passwords, set up a password manager, enable MFA / 2FA on accounts,

Continued onto next page



update devices, and consider obtaining an IRS IP PIN.

For a business, the review should go further. Look at who can access sensitive systems, whether employees know how to report suspicious activity, whether software receives timely updates, and whether backups can be restored. You should also review outside providers that have access to company information, then examine what the company would actually do if a cyber incident interrupted normal operations.

The appropriate safeguards will vary with the size of the business, the information it handles, its systems, and its exposure to outside parties. NIST's small-business guidance specifically allows organizations to tailor cybersecurity risk management to their circumstances.

Cybersecurity issues can also create tax and financial consequences. If you receive suspicious IRS correspondence, discover unexpected tax filings, experience a loss of tax or financial information, or learn that sensitive business records may have been compromised, contact your tax planning professional or CPA right away.

Here at SWC, we can help you evaluate the tax and financial issues that may arise from suspected tax-related identity theft or a business data incident and coordinate with your cybersecurity, legal, insurance, and other advisers when their expertise is needed. We can be reached by calling (858) 487-4580 or writing to us at admin@swc.cpa.

Cybersecurity Awareness Month may last through October, but the habits and planning that protect your personal, tax, and business information need to continue throughout the year.

Disclaimer: *The information in this SWC singlette about Cybersecurity Awareness Month is provided for general informational purposes only and may not reflect current financial thinking or practices. No information contained in this singlette should be construed as financial advice from the staff at SWC (Stees, Walker & Company, LLP), nor is this the information contained in this singlette intended to be a substitute for financial counsel on any subject matter, or intended to take the place of hiring a Certified Public Accountant in your jurisdiction. No reader of this singlette should act or refrain from acting on the basis of any information included in, or accessible through, this singlette without seeking the appropriate financial planning advice on the particular facts and circumstances at issue from a licensed financial professional in the recipient's state, country or other appropriate licensing jurisdiction.*

Tax planning and financial strategy.
Simplified.©

Keep in touch.
16875 W. Bernardo Drive, Suite. 290
San Diego, CA 92127
p: (858) 487-4580 | **f:** (858) 487-8033
w: www.SWC.cpa

Laura A. Stees, CPA
Co-founder | Partner | Business Strategist
Laura@SWC.cpa

Marni L. Walker, CPA
Co-founder | Managing Partner | Estate Strategist
Marni@SWC.cpa