ACT SMART I.T.
www.ACTSmartIT.com
February, 2025
Helping You Benefit From Today's Technologies

Cybersecurity For Tax Season—Protect Your Identity and Your Refund

Tax season brings enough stress without adding scammers to the mix. But the reality is that criminals ramp up attacks in the first few months of the year, often impersonating the IRS or trusted services like H&R Block and TurboTax. By adopting smart security habits, you can protect your data and ensure your tax refund goes where it belongs—your bank account.

Essential cybersecurity tips for tax season

1. File your taxes early. Here's our top tip for tax time cybersecurity: file your taxes as soon as possible. Filing quickly reduces the risk of tax fraud. A common scam is for criminals to try to submit fraudulent tax returns using stolen Social Security numbers to claim refunds. Employers must send out W-2s and 1099 forms by January 31, so once you have your documents, don't delay. If a criminal files before you do, reclaiming your refund is a lengthy and stressful process. If you are in this situation, contact the IRS as soon as possible.

2. Secure your return with an IRS IP PIN. The IRS offers an **Identity Protection PIN (IP PIN)**—a six-digit code that prevents unauthorized tax filings using your Social Security number. You can apply for an IP PIN through the IRS website. While we recommend that everyone signs up for an IP PIN, this is especially true if your SSN has been exposed in a data breach. Once issued, this number should be kept private and used only when filing your return.

3. Enable multifactor authentication (MFA).

Use **MFA** on all accounts related to your taxes, including your IRS account, tax preparation software, and any account with a financial institution, like your bank. MFA requires an additional verification step, like a scan of your face, making it much harder for hackers to gain access—even if they have your password.

4. Look out for tax scams and phishing.

Cybercriminals commonly impersonate the IRS, tax preparers, and financial institutions. Be on high alert for phishing emails, scammy phone calls, and fake websites designed to steal your personal information.

Red flags of a tax phishing scam:

- **Unsolicited IRS communications:** The IRS **never** initiates contact via email, text, or social media.
- **Urgency and threats:** Scammers use scare tactics, like threats of arrest or financial penalties, to pressure you into immediate action. They play on your emotions and use a sense of urgency to try to get you to not think about what you're doing.

Continued on page 3

From The Desk of David Snell

Welcome to February! It seems that winter is here

What fun we had on our trip to Somerville and the Lego Discovery Center! We recommend it highly, and I think it is my favorite attraction that we've ever attended!

We spent 2 nights at the local Holiday Inn and, other than lacking kid-friendly dinners in the restaurant, it was perfect! The pool area included a basketball hoop area and a rock-climbing wall.

We each got to make a mini Lego character to take home, spent an hour learning from a Master Builder, and really enjoyed the Virtual Reality ride and the 4-D movie! We didn't get to do everything and we can't wait to go back!

This month's newsletter is PACKED! Tax season is just starting so our front page article has great advice to keep you, your identity, and your tax refund SAFE,

Dave Sawyer of Safer Places, Inc. offers advice on background checks "One Size Does NOT Fit All."

Susan Rooks continues her series on LinkedIn with more information to help you fill out your "About" section. Be sure to see the back page for information about Susan's FREE seminars sponsored by the Cranberry Country Chamber. Pam be there because she *always* learn something new to help us on LinkedIn.

Vinny Pircio, Rockland Trust's East Wareham Branch Manager and our resident Scam Buster, offers 4 tips for safer banking. Everyone should be following these words to the wise.

Debra Parent and Kate Almeida, RDH, of Right Fit Recruiting recommends that you "Hire for Attitude—Train for Skill." Debra says, "I can teach someone the knowledge, skills, and abilities needed for the job, but I can not teach them how to have a good attitude. "

It's getting harder and harder to fit so much information into these 8 pages! Head over to OfficeManagersSociety.com for more articles and valuable information.

If you'd like to see more of any topic, be sure to let Pam know! Pam@ACTSmartIT.com

Have a great month!

Continued from front page

Requests for sensitive data: Don't respond to emails or calls asking for your Social Security number, banking details, or login credentials. The IRS and financial institutions don't use these methods to transmit sensitive data because they are not secure.

Attachments or links: Phishing emails typically contain malicious links or attachments that can install malware on your device. Think before you click.

5. Ask about your tax preparer's cybersecurity practices.

If you use a tax professional, make sure they take cybersecurity seriously. Ask these critical questions and take note of their responses:

- **How do you protect client data?**
- **Do you use encrypted portals for document sharing?**
- **Who has access to my information within your firm?**
- **How do you back up sensitive tax records?**
- **How long do you store tax records?**

Encryption for protecting data, documents, and communications is critical, and you want them to limit who can access your records. You also want a tax service that uses encrypted, secure backup systems and only stores your records for three to seven years.

6. Safely exchange tax documents.

Avoid emailing tax documents as regular attachments. Instead, use **encrypted email services** or a **secure file-sharing portal** your tax preparer provides. If mailing documents, send them through a **trusted courier service with tracking options**.

7. Back up your tax records.

Make digital and physical backups of your tax documents. Store electronic copies in an encrypted cloud storage service or an external hard drive (or both!), and keep printed copies in a secure location. The IRS generally recommends retaining tax records for **three years**, but depending on your situation, you may need to keep them longer.

8. Report scams to the authorities.

If you think you are the target of a tax scam, report it immediately.

IRS victims of identity theft:
IRS Identity Theft Central
(https://www.irs.gov/identity-theft-central)

Treasury Inspector General for Tax Administration (TIGTA):
Report IRS-related Impersonation
(https://www.tigta.gov/)

IRS, Treasury, and tax-related online scams: Report Phishing
(https://www.irs.gov/privacy-disclosure/report-phishing)

FTC: Report Fraud
(https://reportfraud.ftc.gov/)

IC3: Report Cybercrime
(https://www.ic3.gov/)

By staying vigilant and following these cybersecurity best practices, you can protect your identity, secure your tax return, and reduce the risk of fraud. Don't let cybercriminals make tax season more stressful than it already is! Stay safe online and file with confidence!

Thanks to StaySafeOnline.org for this information!
https://www.staysafeonline.org/articles/tax-season-security-tips

Everyday Banking Tips To Keep From Getting Scammed

In today's increasingly digital world, fraud has become more sophisticated, leaving individuals vulnerable to financial loss and identity theft. Whether through phishing scams, compromised accounts, or fraudulent transactions, the risks are ever-present. Fortunately, there are proactive steps you can take to safeguard your financial information and reduce the likelihood of falling victim to fraud. In this article, we'll explore essential strategies that will help protect your bank accounts, personal details, and peace of mind from fraudsters. These strategies are things you can do in your everyday life to pro-actively protect yourself from the increasing risk of being scammed.

1. Regularly Monitor Your Bank Statements

Frequently check your bank statements for any unauthorized transactions. If you spot anything suspicious, immediately report it to your bank to minimize potential losses. While unauthorized fraud is not your fault, you must notify the bank as soon as possible to mitigate loss to yourself. Make sure that the money coming out of your account is something you authorized, and be sure to review often!

2. Use Credit Over Debit for Online Purchases

Credit cards often offer better fraud protection than debit cards, as you're not directly accessing your bank funds. If your credit card is used fraudulently, your money is still safe and sound in your bank account. The credit card company is out of money, and they will work extra hard to recover their own funds. By using credit online, you avoid using your banking info online and keep your personal funds safe. And as long as you pay it in full monthly, you don't even pay interest and could even get some cash rewards!

3. Educate Yourself on Phishing Tactics

Stay informed about common phishing techniques and how to recognize them. Scammers often use urgency or fear tactics, like claiming your account has been compromised or that you owe money, to pressure you into acting quickly. I can't stress this enough: Scammers are evolving every single day, and while you may think you are up to date on the most common scam, you aren't. Always stay in the loop, only trust people you know personally, and if you have any questions, reach out to your local bankers. Their fraud departments are always keeping them in the loop regarding the newest scams.

4. Don't Share Personal Information Over the Phone

Scammers may call pretending to be from your bank or a legitimate organization. Never provide personal information, passwords, or account details over the phone unless you've initiated the call and verified the identity of the person on the other end. Your bank will **NEVER** ask for your PIN to your debit card, they will **NEVER** ask for your online banking password. **NEVER** provide these to ANYONE you do do not know personally or trust fully. These passwords and PINs are for your eyes only.

Staying in the know, being extra cautious, and protecting your personal information are the only ways to be safe in this digital world. Make sure you are doing everything you can to keep your hard-earned money safe and in your wallet!

Hire For Attitude—Train For Skill

This is an old HR tenet, which all HR professionals know well. Unfortunately, many hiring managers may have never heard it before.

As an HR professional with 35 years' experience in a variety of industries, I have learned that that old HR tenet is the best philosophy to adopt when hiring. You may find the candidate with the experience, but the wrong attitude for your organization, business or practice.

There is another thing I have learned over the years as an HR professional, and that is, you cannot train for attitude. An employee with a poor attitude is not valuable to me as employer.

I can teach someone the knowledge, skills and abilities needed for the job, but I cannot teach them how to have a good attitude.

This includes interpersonal skills, which are often overlooked.

How do we know anything about a candidate's attitude and interpersonal skills?

We have signs from the very first contact with the candidate, and then every interaction following that first contact. Take note of the professionalism and respect the candidate shows when communicating with the recruiter, or employer, from the first email, the first phone conersation, and even scheduling of the interviews. Does the candidate respond promptly, and use professional language in their communication, both oral and written? I have had candidates supply one-word answers to me when communicating via email. That is not a sign of respect. I have had candidates fail to respond to my outreach efforts, only to, weeks or months later, blow up my phone repeatedly asking for an interview. Candidates show you what they will be like on the job from the moment they contact you. Pay attention to all of it, as their attitude is on display.

For any position, within any industry, I would rather hire someone with a good attitude who I could train, rather than hire someone with the experience and a poor attitude.

I have to keep in mind that hiring someone with a poor attitude will ultimately impact the rest of a workforce, and sometimes, rather quickly. Then, you will have more than one problem to deal with. Hire for attitude. Train for skill.

One Size Does NOT Fit All

When it comes to background checks

If you've been performing background checks on the people you hire for several years, now may be a good time to reassess your screening package(s). Do the components of your screening packages align with mitigating the inherent risks associated with the positions for which you hire?

You probably include some level of screening for criminal convictions in your background checks. For example, if you send service technicians into your clients' homes or offices, you certainly want to be sure they don't have a recent conviction involving violence or theft. A check of the sex offender registry is usually added and helps ensure you aren't putting clients at risk for sexual assault. But, what about the drive from your office to the client's location? Does your employee have a current, valid driver's license? What does their driving record look like? Even employees who run an occasional errand for you in their own vehicles can create liability if they are doing so on a suspended license.

And speaking of criminal record checks, how thorough are your searches? Some states have a mechanism to search for records throughout the state with one search. Others leave you to search at the county level. Should you search only the county of current residence? What if a record exists in a neighboring county? What if your applicant resided in a different state last year and in another state the year before that? How would you know, and should those states be added to the search for criminal records?

Did you know that the federal government keeps their own criminal records and if someone is charged with a crime by a federal agency like the FBI, DEA or IRS, the case will be tried in federal district court. If your applicant is charged with drug trafficking by the FBI in Boston, MA, the case will be tried in Boston Federal District Court but a search for criminal records in Massachusetts using the CORI system or searching at the county level will not reveal these charges. Background checks that do not specifically include a federal criminal record search will always miss convictions for crimes at the federal level.

Think of your background checks like doing a jigsaw puzzle. Each piece you add helps to reveal a more complete picture. A drug test, verification of previous employment, verification of education, a check of the national wants & warrant system, even a credit history report in some cases can help to provide a more-robust image of your applicant, helping you to decide if he or she is the right fit.

Finally, let's talk about social media searches. Statistics I've seen tell me that most of you are doing some form of this. The problem for the DIY crowd is that it can be quite time-consuming, and you'll likely see things that cannot be used in a hiring decision. Even if you decide not to hire for some legitimate reason, it can make it difficult to defend against a claim that your decision was based on the fact that Sally just announced on Facebook that she's expecting her first child.

Making social media searches part of your background screening report with a professional screening company should limit you to seeing only actionable items as the rest is redacted and never makes it into the report. Using AI, screening companies can screen all the popular platforms plus millions of other sources, including news, niche social media, boards, blogs, forums, review sites, and more. They can identify prejudice, threats, disparaging comments, and more from publicly available text and image content including nudity, drug images, gory/violent, rude gestures, extremist symbols, and weapons images.

Aligning candidate character to corporate values through social media background checks may improve workplace culture, reduce turnover, create a safer environment, and mitigate risk to your brand.

Ask your background screening company to review your screening package(s). Describe to them the positions for which you hire and ask what products they offer that may assist you in mitigating the risks that go with those job descriptions. You may find that you should have 2, 3 or more screening packages due to the varying types of employment you offer. There is no such thing as a standard background check, and you shouldn't settle for an off-the-shelf package.

David Sawyer

President, Safer Places, Inc.

www.saferplacesinc.com | david@saferplacesinc.com

508-947-0600

Helping You Benefit From Today's Technologies

More Help with LinkedIn About

So far in this series about the LinkedIn™ basics, we've learned more about using LinkedIn to draw others to our profile with information on the **banner**, the **picture**, and the **headline**, and the **About** section.

Now let's finish this conversation by talking about the smaller sections that still should be considered important enough to fill in.

Experience: What you've done in business, going as far back as you want or need to. Start with the most recent and give whatever details help you stand out.

Education: Again, whatever details you think are important. Schools you've attended. Courses you've taken.

Projects: What you are or have been involved in.

Volunteering: If you've helped out at any non-profit, mention it. That always helps you to stand out!

Recommendations: These are pure gold, especially if you have some current ones mentioning the work you've done that you're looking for.

Honors and Awards: Ones you've received—and it's not bragging if it's true!

Interests: Outside of work, who or what grabs your attention?

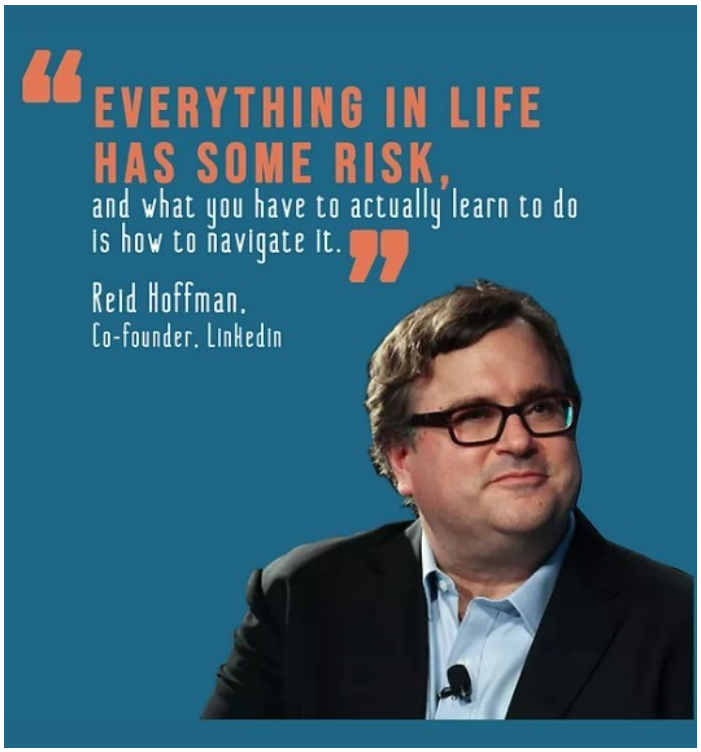
Causes: What causes do you believe in or help with?

You'll see the pencil at the right top side on each section; click it to be able to create or edit your choices.

Remember: Nothing is written in stone. We can always edit / update our profile as changes occur in our life!

Obviously we can fill these out as we wish, with more or less detail. But it does help to round out our profile, our persona, our humanity. It helps us be seen as a more-complete human, perhaps someone others would like to know / work with / connect with.

Beyond helping you fill out your profile, there are some ideas I'll share next month about using all this great information to connect with the right folks, use the right tools, and beyond that, use the right language.



ACTSmart IT
332 Main Street
Wareham, MA 02571

January, 2025—In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com

Want to Make a Bigger Impact on LinkedIn?

Ever feel like you're just another face in the crowd on LinkedIn? Wondering how to stand out and truly make a difference?

Join us for **two dynamic, one-hour LinkedIn Basics sessions** with **Susan Rooks, the Grammar Goddess**! She'll guide you from **struggling to thriving**, showing you the essentials to elevate your presence and grow your business.

Each power-packed session delivers **half of the LinkedIn know-how you need**—combine them both, and you'll be ready to make a real impact!

Don't miss out—your LinkedIn transformation starts here!

Be sure to register for both!
Compliments of the Cranberry Country Chamber

Session 1: Friday, February 28, 2025, 9:00 – 10:00 a.m.
Session 2: Friday, March 21, 9:00 – 10:00 a.m.
Cranberry Country Chamber Conference Room
9 Clayton Road, Middleboro

https://cranberrycountry.org/event/learn-how-linkedin-can-work-for-you-session-1/