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

10 overlooked security actions that you should prioritize in 2025

As we enter 2025, many people know the basic cybersecurity practices, but several overlooked or underappreciated actions can significantly improve personal security. Here are 10 security actions that are often overlooked but should be prioritized in 2025:

1. Disable Unnecessary Services and Ports

Why: Many devices and applications have services running in the background that attackers can exploit if left open.

How: Regularly audit your devices and disable unused ports, services, or software. For example, turn off remote desktop services or file sharing if you don't use them.

2. Review and Revoke Unused Permissions on Apps

Why: Apps often request permissions beyond what's necessary for their functionality, which can pose security risks.

How: Periodically review the permissions of apps on your smartphone, computer, and cloud services. Revoke unnecessary permissions such as location access, camera, and microphone usage.

3. Use Device Encryption (Full Disk Encryption)

Why: If your device is lost or stolen, encryption prevents unauthorized access to your data.

How: Ensure full disk encryption is enabled on all devices, including smartphones, laptops, and external drives. Use built-in encryption tools like BitLocker (Windows) or FileVault (Mac).

4. Secure Your Smart Home Devices

Why: IoT (Internet of Things) devices such as smart speakers, cameras, and thermostats can be vulnerable entry points for cybercriminals.

How: To limit exposure, change default usernames and passwords, update firmware regularly, and isolate IoT devices on a separate network from your main devices.

5. Limit Tracking and Use Privacy-Focused Search Engines

Why: Many online services track your behavior and data, creating potential security risks.

How: Use privacy-conscious browsers (e.g., Brave) and search engines (e.g., DuckDuckGo). Consider browser extensions like uBlock Origin or Privacy Badger to block trackers.

From The Desk of David Snell

Happy New Year!

We all had colds, so we celebrated New Year's Eve on Saturday, January 4th and stayed up until midnight to ring in the "New Year" with the grandchildren!
The noisemakers were the biggest hit and their mother thanked us for sending them home, and so did Dexter their dog! That's what good grandparents do, right? Share their wonderful surprises with the whole family!

They're great kids, having fun while excelling in school and we have a trip to the Lego Discovery Center in Somerville planned for the near future.

To avoid seeming like a broken record, and because we think you probably have a good grasp of basic cyber security awareness, our front page article is about the ***10 overlooked security actions that should be prioritized in 2025***. Don't do them all at once because you'll be overwhelmed. "Resolve" to do one a week and you'll get lots of satisfaction when completed.

On page 4, we have a post from Rick's Tech Tips about watching out for the "Confirmation Code" scam. This is one of the ways that people lose their Facebook and other social media accounts.

Bob Kagan recommends how to "Select Your Credit Card Processor" on page 5. Lots to consider if you are looking to switch companies.

On pages 6-7 Susan Rooks helps us improve our ***ABOUT profile on LinkedIn.*** She provides instructions with examples and recommends an article on LinkedIn that offers 15 examples of Summaries. You can access these URLs on her "Experts" page on the OfficeManagersSociety.com website. There, you can read all her LinkedIn articles and use the embedded links to gain more information.

Are you still doing Zoom webinars? We're looking to offer some free trainings in the near future. Would you attend? Do you have any suggestions on topics and/or speakers? Please send Pam your thoughts. Pam@ACTSmartIT.com.

Always at your service,

Continued from front page

6. Keep Physical Security in Mind

Why: Physical device access is a significant threat to digital security, especially in public or shared spaces.

How: Use privacy screens on laptops and mobile devices, avoid leaving devices unattended, and consider using a lock or biometric authentication for physical device access (e.g., phone or laptop).

7. Set Up Account Recovery Options Properly

Why: If you lose access to an account, proper recovery options can help you regain control without security issues.

How: Ensure recovery email addresses, phone numbers, and security questions are up to date. Consider using a secure recovery method, such as a secondary email or trusted contact.

8. Review Device and App Privacy Settings Regularly

Why: Privacy settings often change with software updates, and you might unknowingly share more data than intended.

How: Periodically audit your privacy settings across all devices, apps, and online services. Turn off features like location tracking and data collection where they are not needed.

9. Lock Your Devices with Stronger Authentication

Why: Many people rely solely on PINs or basic passwords for locking devices, which are often easily bypassed.

How: Use stronger authentication methods, such as biometric options (fingerprint or facial recognition) or a more secure PIN pattern. Avoid simple 4-digit PINs.

10. Consider a Privacy Audit for Your Online Presence

Why: As your online identity grows, you may inadvertently expose sensitive information.

How: Perform a privacy audit on your online accounts, including social media profiles, to ensure personal details (e.g., birthdate, address, employer) aren't publicly accessible. Use tools like Google's privacy checkup and review what personal data is shared with third parties.

Bonus Tip: Invest in a Personal Security System for Remote Work

Why: With remote work becoming more common, securing your home office is often overlooked.

How: Set up firewalls, use a VPN, and ensure secure Wi-Fi. Regularly scan for malware on remote devices, especially if working with sensitive or business-related information.

These overlooked actions will significantly boost your security posture and privacy in 2025, protecting you from many cyber threats that can slip under the radar.

If you need help, get in touch!

Don't fall for this dangerous 'Confirmation Code' Scam

Well, the scammers are at it again (as if they ever stop).

This time they're out to take control of your Facebook account (and some other accounts as well) by tricking you into helping them change the password so they can log in to it.

I've received several requests for help from readers who had their accounts hijacked via this scam, and unfortunately there was nothing I could do to help in most of those situations.

As usual, there are several variations of this scam, but most of them go something like this:

- You receive a private message from one of your Facebook friends saying they want to change the password on their account but for some reason they aren't receiving the confirmation codes that Facebook sends in order to confirm the account holder's identity.

- They then tell you they had Facebook send the code to YOUR phone instead.

After you receive the code on your phone the hacker asks you to send them the code so they can use it to change *their* Facebook password. However, this is all just a ruse...
That code is actually the code the hacker needs to enter in order to sign into YOUR account because he initiated a password change on your account, not his. That's why the code came to YOUR phone instead of his.

If you go along with the scammer's request, this is what will happen:

1 - The scammer will end up with YOUR Facebook confirmation code.

2 - The scammer will use that code to change the password on YOUR Facebook account, and thereby gain access to it.

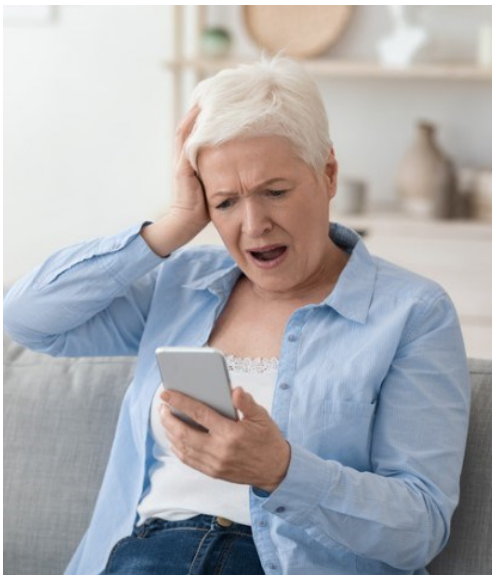
3 - The scammer will sign into your Facebook account with the new password and quickly change both the phone number and the email address that's connected to your account, effectively locking you out of the account.

As you can see, this is a very dangerous scam. And unfortunately, it's very easy to fall for. After all, we all want to help a friend get out of a jam, right?

Like I said, there are several variations of this scam. Just know that if someone asks you to send them a code that was sent to your phone, they are trying to scam you and hack your account.

Bottom line: If you receive any type of message from a Facebook friend asking you to send them a confirmation code that you received from Facebook, refuse to comply or else you'll likely end up losing access to your own Facebook account.

Bonus tip: This scam started out only targeting Facebook accounts, but it's now being used to hack into other types of accounts as well. If you receive a request like the above for *any* account, don't comply with the request. That innocent-looking code can really come back to bite you.



Thanks to Rick's Tech Tip Newsletter December 20, 2024 for this alert!

Selecting Your Credit Card Processor

Choosing the right Merchant Services company is very important to the success of your Practice. A reliable Merchant Services provider will ensure the smooth processing of credit card transactions and support your business growth. When evaluating which company you trust to handle your Credit Card Processing, you should consider what are the most important features offered, for you. Are you simply looking for the "Lowest" processing rate? Is it a particular processing platform you seek? Is the level of Customer service paramount to you? As you work your way through this process, here are some items to consider.

Honesty & Transparency

You should want to work with a company that will take the time to sit with you and properly analyze your current situation. You want them to be completely honest about not only if but how they can "SAVE YOU MONEY" and what makes their company the right fit for you. Pricing is important, of course, but you want your Rep to speak not only about their "Low" Processing Rates but, equally important, about their month-end fees. Their very low processing rates can often be offset with elevated Fees. What's important is your "Overall Processing Percentage."

Customer Service

Virtually all Merchant Services Companies offer a 24/7 800# level of service. This is a positive thing, except when you call it, you may not have the time to be "on hold" for 45 minutes, listening to elevator music. Franky, you deserve and should receive More! Instead of working with a Rep who says, "When you have a problem, here's the 800#, perhaps you want to work with one who says, "Make me your first call".

Security & Compliance

Security is paramount when handling customer payment information. In this day and age, all processors operate under the same strict security guidelines. As for you, the Merchant, you are required to maintain your annual PCI (Payment Card Industry) Security Compliance. This assessment must be completed annually, and if ignored or forgotten, it will automatically result in a significant monthly penalty. Most processors leave it up to you to complete. There are, however, Reps who will complete the Assessment for you, thus making certain that you are always in compliance and will never be penalized for Non-PCI Validation.

Selecting the right Merchant Services company involves careful consideration of the services offered, pricing transparency, customer service, and security measures. By prioritizing these factors, you can find a provider that meets both your current and future needs.

Bob Kagan, Summit Network LLC

781-820-4328

www.summitnetworkllc.com | bobkagan13@gmail.com

Credit Card Processing Made Easy

LinkedIn™ About Section

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**.

Now comes the real "meat" of any profile: the **About** section (sometimes called the Summary) that allows us to meet prospective clients where their pain points are by sharing ways we can help them.

While there are no absolute rules for creating this section, I've learned over time that a thoughtfully filled out section gets us what we're usually looking for: connections and/or clients.

What you'll see below are ideas I've gleaned from others and from my own experience on LI, which has
given me 95% of my clients in the last 10 or so years. It took me a while, but once I "got it," I GOT IT!

So, let's see if what I've suggested — strongly — below will help you here.

1. Remember that the About section is about YOU helping others, not some mythical person with your name. You get to use your own language, tell your own story, woo your own clients.

2. Use a "hook" to grab a scroller's attention quickly, like starting with a question about pain points you could help with.

Think about those who already work with you. What did they say when you asked them how you could help? What pain points did they instantly mention? If those pain points align with your strengths, mention them to pull in more clients!

> **Content Creators:** Have you ever published a document with "pubic" in it when you meant "public"? "Orgasm" when you meant "organism"? How could that happen?

3. <u>Always</u> write in the first-person (using "I"), never
in the third person (using your name). That does not
encourage anyone to want to be part of your world! Even worse is using your name and then using "we" or some other pronoun that doesn't seem to fit. Don't give the reader an excuse to move on to the next profile; you may never get that person back to yours.

I know that many of us think that using "I" is too much like shining a bright light on ourselves and bragging, but we are talking about what **we** do, right? It's not bragging when we stick to the facts of how we have helped others with the same issues. We just shouldn't embellish those facts with strong adjectives about ourselves.

> John Smith is a highly decorated expert in the field of …
>
> We are always looking for …
>
> John's managers have always said that he …

4. Tell a story about your success in your primary field. Show what you did, how you helped, etc. Be real. Use humor if you want to. Let others see who you are in a professional sense, as someone they'd feel comfortable working with!

5. Use this section to fully cover WHY you do what you do. What makes it important to you? Why is
helping others succeed important to you?

6. Feel free to highlight your achievements, but base them all on how they helped others — the kind of others you're hoping to land as clients / mentors / connections.

Mechanical things to know about:

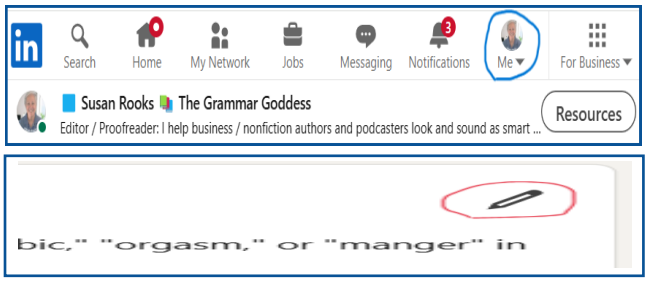
1. You can always edit your sections; no one is forced to always use their first version. Life changes. Your profile can and likely should change occasionally, too!

2. First go to the LI homepage by clicking the "home" icon on top of any page you're on. On

the homepage, look at the top again and see your picture where you see mine outlined in blue. Click on it to go to your own home page.

When you're on your page, you'll see a pencil at the top right side. Click on it to edit/make changes. Remember to click "save" at the bottom when you're done!

The pencil shows up in each section on your page, so you can always make changes to individual sections.



3. As of 2024, we have 2,600 "characters" to use in telling our story, and that includes spaces between words and paragraphs.

4. Please break your big paragraphs into smaller ones; it's really hard to read a paragraph that's more than about 8 or 9 lines of type. Huge paragraphs often have a reader decide to just move on to another profile.

5. Be sure to use past tense verbs for all work you show that ended. Many times that's overlooked and could confuse a reader.

Next month, we'll explore other less-critical sections that you might want to fill in.
And remember: I'm open to any questions you may have.

Remember: It's well worth the time you can spend looking closely at others' profiles, especially their About section. You never know where and when you'll see something you could use on your own!

Here's a worthwhile article that shows 15 other very decent examples of what they call a Summary.

https://www.linkedin.com/business/talent/blog/product-tips/linkedin-profile-summaries-that-we-love-and-how-to-boost-your-own.

Now this is a long URL, so here's one from Tiny URL that you can at least copy:
https://tinyurl.com/mt23sxms

Or, this QR Code:

ACTSmart IT
332 Main Street
Wareham, MA 02571

ACTSMART I.T.
www.ACTSmartIT.com

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