www.bazyncommunications.com

Bazyn Communications
Making the Impossible Possible
Newsletter

Summer 2018

For positive inspiration, contact Bazyn Communications
"True Vision with Insight"

If you wish to be added to my email newsletter list, please sign up in the subscription box on any BazynCommunications.com at the bottom of the navigation links. If you wish to be deleted from my newsletter list, please do so at the same place where you sign up.

Contents

Letter from the editor

Dear readers,

Life places us in many uncomfortable situations- travelling in unsafe locations, making a career choice, moving to a new area, or setting goals or priorities. However, making changes is how we survive and thrive. We have to face challenges in our businesses each day. We volunteer in organizations with limited resources as well. There is a wealth of information at our fingertips. Googling any topic leads us to unlimited ideas and facts.

I participated in a panel for my chapter of American Business Women's Association in Burbank, CA and wrote an article about the presentations since I thought it showed how "Using Your Strengths in Your Business" worked for the panel members. The second article I included covers some important "Ways to Protect Your Privacy". I'd found the full article online but just placed a few of the

easier tips in it.

A business or life coach can keep us motivated and on target. I offer a free consultation. Do you need help developing your strategies for the future? Are you considering retirement, deciding on whether to become an entrepreneur, or more fully develop your business with a new marketing or business plan? Please give me a call and we can discuss your projects. I can motivate you to move forward!

In recent months, my travels included Lawton, OK; Las Vegas, NV; Washington, DC; Long Beach, CA; Denver, CO; and Paso Robles, CA.

In the next few months, I'll be flying to Blue Bell, PA; St. Louis, MO; Reno, NV; Sioux Falls, SD; St. Cloud, MN; Denver, CO; and San Francisco, CA.

To give organizations and corporations discounted speaking fees, I try to coordinate events and trainings. Please let me know about events or possible speaking opportunities in these and other areas, since I’m always adding cities to my itinerary.

Have a fantastic summer,
Ardis Bazyn

Return to Table of Contents

Using Your Strengths In Your Business

By: Ardis Bazyn

In April, The American Business Women's Association VerdugoGlen presented: "Tips and Tricks from Local Entrepreneurs". The panel members told the audience how they started their business, initial challenges they encountered, and what positive efforts led to their success. As the women presented, the audience could tell how these entrepreneurs used their strengths to begin and grow their business. Panel members were: Patricia Nelson from Nelson Treasures, Vickie Parker as a Marriage and Family Therapist, and Ardis Bazyn from Bazyn Communications.

Patricia was working for another company when she decided to take a class on making jewelry. She found it stimulating and soothing to do. She wore the jewelry to work and other employees would ask about the jewelry. Some asked her to make jewelry for them. After receiving many requests, she decided to form a business selling jewelry. She later was able to leave her corporate job.

after finding women liked to match jewelry with clothing, she purchased clothing with a specific "look". She started to exhibit her jewelry and fashions at events and home shows. She now uses Facebook to promote her jewelry and events. She found selling a look, not just jewelry improved her business.

Vickie Parker is certified as a marriage and family therapist (MFT). She originally

was offered an internship under a therapy group. As a visually impaired therapist, this allowed her to get a hands-on start in the business. She then opened her own office, originally offering marriage counseling as well as trauma therapy. After her divorce, she was uncomfortable working with couples. She soon started working more with trauma victims, both children and adults using play therapy. She then added discussion groups of newly visually impaired persons, working one-on-one as requested. She has been able to capitalize on the fact she is visually impaired. Check her website www.vickieparkermft.com.

Ardis Bazyn started her career in food service management with staff of as many as 13. She trained other visually impaired persons to start their own food service business. After speaking to multiple schools about her disability, speaking for church women's groups, and becoming involved in multiple nonprofit organizations, she began to speak more and more for all sizes of groups. She returned to school and received two BA degrees in Public Relations and Speech Communications as well as a Master's degree in Education. She changed careers when she realized she enjoyed speaking and business coaching more than food service management.

Using her experience with solving solutions for challenges she faced, she started helping other business professionals and speaking to groups. Her most requested topic is "Secrets to Coping with Challenges and Change". She has published several books and writes many articles for publications.

(Other tips and helpful business resources can be found in Ardis's book "BUILDING BLOCKS TO SUCCESS: Does the Image of Your Business Attract Customers and Motivate Employees?" Order online at www.bazyncommunications.com)

Return to Table of Contents

Ways to Protect Your Privacy

By Consumer Reports

Privacy is not as hard as you might think

1. Wondering whether your personal data is for sale on the web? At haveibeenpwned.com you can check your email addresses and usernames against lists from 120 known breaches. If your name pops up, change the password for the compromised account and any other site where you were using the same password.

2. Laptops, smartphones, and other WiFi-enabled devices can automatically connect to familiar networks. That's convenient—no one wants to enter a password for their home or work WiFi every day—but it can also be risky. A hacker can set up a rogue WiFi network with the same name as a legitimate

one and trick your gadgets into joining it. Periodically get a fresh start by using your devices' network or WiFi settings to prune the networks you join automatically. Most devices let you delete networks one by one, but some allow you to delete all of them at once.

3. Set a password or PIN for every laptop, smartphone, and tablet you own. Any lost device without a screen lock is an unprotected gateway for thieves, who may be able to access your email, banking, and social accounts. By changing passwords, you are taking control.

4. Use a 6-digit pin. Be Unique . . . Don't use any of the following Pins because they're far too common: 0000, 1111, 1212, and 1234. Do not use any personal information such as birth date, last four digits of your Social Security number, or your phone number.

5. Provide better finger art passwords. Android users can unlock their phones by tracing a pattern on the screen. To be safe, it needs to be unpredictable, but often it's not. Don't use an initial, particularly the first initial of the user's name.

6. Shred these 5 document types. Destroy any health-related documents. Shred any documents containing: Social Security number - even just the last four digits, birth date, credit card numbers, account numbers from financial institutions, and medical insurance numbers. Get rid of credit card offers. These unsolicited mailings can be intercepted by identity thieves who have credit cards sent to their own addresses, piling up debt in your good name. You can put a stop to most of these offers by going to optoutprescreen.com or calling 888-567-8688. The service, run by the Consumer Credit Reporting Industry, will stop them permanently or for five years. You can always opt back in.

7. Receive Less Mail. When you give a company your name and address, the information will likely be added to direct-marketing lists and used by other companies to send you solicitations. Go to dmachoice.org to remove your info from many mailing lists if you don't want the offers.

8. Return to Sender. If an unwanted envelope is printed with the phrase "Address Correction Requested" or "Return Postage Guaranteed," you have an alternative. You can write Refused/Return to Sender and mail it back—no postage required. The marketing company will pay the return-trip postage.

9. Turn on automatic updates. Keeping your software up-to-date is the most critical step you can take to boost security. Hackers are always exploiting more vulnerabilities, while security pros play nonstop with malware. If you've got old software, you're missing the latest protections. Most modern software will update itself if you let it. Make sure you have auto-updates turned on.

10. It's easy to create passwords that are difficult for hackers to crack. Most passwords are just too predictable. Most use: foreign words, movie or book titles, patterns on the keyboard, and it doesn't take long for experts armed

with the latest computer technology to run through all of the familiar patterns. Strong passwords have two things in common: they avoid patterns and are long for a computer to run through possible combinations of characters—to succeed. Assuming a password is a truly random collection of characters, how long is long enough? String together unrelated words. Pick five long, random words and string them together into a nonsense sentence that you can remember.

11. Use a password manager, it's hard to remember long strings of random characters. Password managers can generate a complex, unique password for each account. You'll still need one well-crafted password for your password manager account. Write it down. As long as you're not leaving post-it notes under keyboards, it's totally ok to write passwords down. Keep vital passwords including the one for password manager and phone lock screen in a sealed envelope to be opened only if incapacitated. Loved ones can then access online accounts to pay bills and take care of other business.

12. If using password manager, don't change passwords unless there's a good reason, such as responding to a data breach. Switch often and you'll probably end up using weak options.

13. Stop ID theft after a death. Identity theft affects 2.5 million estates every year, according to the IRS. If a loved one has died, send a copy of the death certificate to the IRS (the funeral home may help). Also, cancel any driver's license and notify credit agencies, banks, insurance firms, and financial institutions.

14. Stay up to date on the latest product ratings. Subscribe for digital access.

15. Use two-Factor Authentication. Section 609(e) of the Fair Credit Reporting Act requires companies to provide victims of identity theft with all business records related to the incident. Fill out a template at identitytheft.gov, a site run by the Federal Trade Commission where you can report thefts and mail it in to the carrier. To keep it from happening to you, activate a pin. Sprint requires customers to set a pin and security questions for their accounts, and the other major mobile providers offer customers the option. Take it. Having a pin can help keep strangers from making changes to your account.

16. Watch your bills. Many wireless plans are based on a flat rate, so make sure your bill is consistent from month to month. If it's not, take a closer look at your account.

17. If you're just a bit suspicious of a document you've received by email, save it to Google Drive and open it there. If there's any malware enclosed, it will be isolated in a virtual environment, away from your operating system. As a second benefit, Google Drive automatically scans files for known viruses.

18. Check on your kids. Minors had their identity stolen 51 times more often than adults in a study. Keep an eye out for letters from collection agencies, bills for unpaid balances, or a warning that pops up when you try to file your

taxes electronically when listing your child as a dependent. Request reports from the three big credit-rating agencies when children turn 15. Then clear up any problems before they apply for college loans, jobs, or credit cards.

19. Web-connected devices promise convenience, but some can leak private data. Keep your information safe. Lock down your baby monitor. Hackers sometimes break into WiFi-connected baby cams, even hijacking the speakers to talk to children and caretakers. Change the default settings. When you set up any internet-enabled camera, create a unique username and password. Turn off the baby cam when it's not in use. Cover your webcam.

20. Outwit your Smart TV. Automatic content recognition across systems built into many smart televisions transmit data to analytics companies that may use it for marketing. If you don't want to pay again with your data, hunt through your TV's smart settings for the feature which may be called Live Plus, SynPlus, or anything but ACR—and turn it off.

21. Using WiFi file sharing is totally inappropriate at a coffee shop. To get your laptop ready to leave your home network, deploy your firewall, turn on your firewall, restrict file sharing. File sharing makes it easy to swap documents among devices. If you're on your home network, that's good. When you're on public WiFi, it's bad. Turn it off under the sharing settings on your computer. Turn off network Discovery to make it more difficult for other devices on the network to find your laptop. On pcs, it's under advanced sharing settings. Mac users can enter stealth mode through firewall options. Do all of this automatically. Changing laptop menus every time you leave home can be annoying. Windows makes it easy to automate the process using advanced sharing settings. Whenever you join a new WiFi network, Windows asks whether to add it to your home or public profile; the operating system forgets the public networks when you log off. To do something comparable on a Mac, use the free-to-download control Plane app.

22. Use a VPN, virtual private networks, route your traffic through a single remote server with tight security in place. Consider using a paid service such as IVPN or the free VPN recently introduced.

23. Toymakers are rolling out connected kids' products—including tablets and talking dolls—and asking families to divulge personal information to register them. This essentially provides marketers and potential hackers with details about your children. Consider providing fake information. Suggest Bart Simpson's—742 Evergreen Terrace.

24. Encryption is for everybody. Encryption scrambles your data so it's unreadable by anyone who doesn't have permission to access it. Do your phone first. Your smartphone knows everything about you. New iOS and many Android smartphones are encrypted by default; if you have an older mobile OS, you'll need to go into settings. You can encrypt your whole machine or just sensitive files. To encrypt specific files on a Mac, use the disk utility. Windows 10 home users can download a free app such as GPG4win (Gnu Privacy Guard). Your USB Drive Flash drives can be misplaced—along with your files. Apricorn flash drives with built-in

encryption are recommended.

25. It doesn't cost to use Facebook, but you pay for access with your data, which is vacuumed up. Take these steps to boost privacy and limit how much Facebook can learn about you. Keep GPS data private. Facebook can extract your whereabouts from your mobile phone. But you can turn the function off using your phone settings. For an iPhone, you'll find the controls under Location Services. If you've got an Android device, look under Facebook Permissions in Applications Manager.

26. Turn on Log-In Approvals. This is Facebook's name for two-factor authentication. It keeps strangers from accessing your account—even if they steal your password.

27. Don't want people finding your Facebook page when they type your name into a search engine? You can change that and more under the "Who Can Look Me Up?" section of Facebook Settings.

28. Facebook lets users add friends to groups without their consent. You can remove yourself from any group by going to your Activity Log. You can avoid being used in ads by tinkering with Facebook's Ad settings.

29. Hide ID-Theft Clues: your birthday. Your hometown. Your alma mater. Those are all things Facebook can reveal to the world—and they're answers to potential security questions. Hide such information by using the Privacy Checkup Tool found under the padlock on the upper right of any Facebook page.

30. Browsers should be set up with anti-tracking and ad-blocking extensions. Use one exclusively for all of your most important things, like banking and shopping. Use the other browser to do everything else, like reading the news or searching or whatever. If something bad happens within the second browser—a malicious software attack—it can't affect your bank account or credit card, because the browser doesn't even know those accounts exist.

31. Laptops, smartphones, and other devices you use at home all connect to the internet through your router. And so do web-connected devices such as smart TVs and some security cams and children's toys. Make your router more secure. Find an Ethernet Cable Then use it to temporarily connect the router to your computer. You'll be updating your router's firmware. It's safer to rely on old-fashioned wires and plugs.

32. Get the IP Number. Every router has two IP (internet protocol) addresses, an external one for communicating with the internet through a modem and an internal one for your laptop, smart TV, and other devices. To make changes to your router's settings, you need to access it through your browser using the local IP address. Update Firmware. Some routers automatically update their firmware, checking for updates, installing new software, and rebooting in the middle of the night. Not all of them do. Many routers that say they have automatic updates require users to log on and hit Okay. Make Sure Remote Management Is Off unless needed. Going out of

town? Turn off the router unless you need it to access smart devices such as your thermostat or a security camera. Get a New Router if it follows an old WiFi standard.

33. Check Links Before You Click. Web browsers don't come with every protection you might want. Download extensions to improve security. Add HTTPS Everywhere. When you see "https" and a green padlock alongside a URL in your browser's address bar, it means that the data is encrypted as it travels back and forth between the website and your computer. (The "s" stands for "secure.") Some sites that support https use it inconsistently. Add the HTTPS Everywhere extension, which you can download from the Electronic Frontier Foundation. Your connections will be encrypted anytime you connect to a website that supports https. Extensions are small pieces of software that can enhance the functionality of web browsers.

34. Extensions including Adblock Plus, Disconnect, Ghostery, Privacy Badger, and uBlock address the snooping issue using varying approaches. Most let you add URLs to a whitelist of sites they won't check. You can do that if a favorite website stops working once you download the extension. There are also additional settings you can use to adjust which ads get through.

35. Back Up Your Data. Use a system that backs up your files automatically. If you're hit with ransomware, you'll have the option of restoring the data. Keep Software Updated. Ideally, set your computer and key programs to update automatically.

36. One way to stay safe is to use two-factor authentication, which prevents a criminal just with a password from accessing your accounts.

37. Watch for Fake Email Notices. If an email from a bank or social site asks you to log on, don't click. Open a new browser window and type in the address of the company website instead. Call Customer Service.

38. Keep Your Fitness Data to Yourself. Many wearables are paired with users' smartphones using Bluetooth technology. Many Bluetooth devices don't prevent data access by those located nearby. Fitness trackers and running watches can broadcast sensitive information such as the user's name, address, password, and GPS data. Some trackers let you shut off Bluetooth. If possible, keep your wireless settings turned off until you choose to upload the data to your phone. (As an added benefit, that will extend the battery life.)

Return to Table of Contents

Updates

By Ardis Bazyn

www.bazyncommunications.com

To order books or seminars, check out www.bazyncommunications.com or call 818-238-9321. Checks, money orders, and Visa or MasterCard through Paypal are accepted.

All my books are available for purchase on my website: www.bazyncommunications.com in several formats. You can receive a discounted print copy of my third book by ordering it on my publisher's website: www.xlibris.com. BUILDING BLOCKS TO SUCCESS: Does the Image of Your Business Attract Customers and Motivate Employees?

Go to the author page and look for Ardis Bazyn or go to the book page and look for "Building Blocks to Success".

Return to Table of Contents

Products and Services

Bazyn Communications continues to offer inspirational and motivational speaking, business coaching, and writing. A free consultation by phone or in person is available upon request. For a list of speaking or coaching topics, visit www.bazyncommunications.com.

We're also available for a variety of writing projects, business plans, marketing plans, articles, and copy for most types of media for small businesses and nonprofits. Small Braille transcription projects including greeting cards or business cards are offered at reasonable prices. Contact us for pricing.

If you wish to receive a text version of this newsletter or receive any past issues, please email: abazyn@bazyncommunications.com or call (818) 238-9321.

Return to Table of Contents

Contributions Accepted

If you wish to contribute an article to a future newsletter, or make any suggestions, please send an email to abazyn@bazyncommunications.com . Each article received will be read and will be printed if it meets the newsletter criteria.

Return to Table of Contents

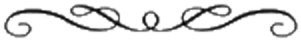
Links

Check out the links of organizations in which I participate:

www.bazyncommunications.com

American Council of the Blind	www.acb.org
Burbank activities	www.burbank.com
Burbank Business Network International	www.bniburbank.com
Burbank Chamber of Commerce	www.burbankchamber.com
California Council of the Blind	www.ccbnet.org
California Voter Empowerment Circle	www.CALVEC.org
Coaching and Speaking Internationally	www.247coaching.com
Democracy Live Accessible Voting	www.democracylive.com
Independent Visually Impaired Entrepreneurs	www.ivie-acb.org
Randolph Sheppard Vendors of America	www.randolph-sheppard.org
Speaker Match	www.speakermatch.com
Success Simplified	www.successsimplified.com
Xlibris Publishing	www.xlibris.com

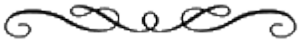
Return to Table of Contents



Contact Information

Bazyn Communications Ardis Bazyn
818-238-9321
abazyn@bazyncommunications.com www.bazyncommunications.com

Return to Table of Contents



Favorite Quotes

“I'm convinced that about half of what separates the successful entrepreneurs from the non-successful ones is pure perseverance” –Steve Jobs

“You can have everything you want by helping enough other

people” "The right idea with no follow-through is dead on arrival”

Return to Table of Contents

For positive Inspiration, contact Bazyn Communications!
“Making the Impossible Possible”