



Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • March 2018



Scott Bernstein, CPA President Nick Espinosa CIO & Chief Security Fanatic

WARNING: Your Business Is More Likely To Be The Victim Of Cybercrime NOW Than Ever Before...Take These Steps Today So You Don't Get Hacked!

Though we're in the midst of an unprecedented rise in high-profile cybercrime incidents, it's easy to assume that our own much smaller businesses are safe. Sure, we think, hacking into the data stores of J.P. Morgan, the U.S. Government, or Virgin America can net hackers millions and millions of dollars. Why would they bother with a small business?

But unfortunately for all of us, hackers actually do bother with small businesses across the country — these attacks just don't make the news. By some estimates, including one reported in Media Planet, more than half of small businesses have had their data compromised. According to StaySafeOnline.org, these attacks, targeting small to midsize companies, now comprise over 70% of all data breaches.

What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime.

Once you see these numbers, it's easy to understand why hackers seek the little guy. These days, massive corporations like Google or Citigroup employ incredibly sophisticated digital measures. Their digital vaults, though containing ludicrously attractive sums of potential money to grab, are located at the end of a virtual labyrinth covered in traps, with a final, inches-thick steel door protecting their assets for good measure. In contrast, the digital assets of small businesses are often hidden behind nothing more than a single, often weak, password. With thousands of business owners going about their day-to-day, utterly oblivious to their paper-thin security, the question turns from "Why would hackers bother with my small business?" to "Why wouldn't they?"

Though cybercriminals may come away with less than they might have had they targeted a Fortune 500 company, it certainly isn't going to seem cheap to you. According to one

TechRepublic analysis, an average cyber-attack on a small business can cost as much as \$256,000. Is that a sudden cost your company can weather?

Luckily, there is hope. Though small business owners often assume that effective cyber security solutions lie far outside their budget range, robust digital security is now more affordable than ever. By investing in comprehensive protection, small businesses can deflect even the most persistent hackers.

Today, a cyber-attack on your business is almost statistically inevitable. And when that attack comes, you'll definitely want to be prepared. If you haven't needed a doctor for the past two years, does that mean you're going to abandon your health insurance coverage? Of course not. What about car insurance? Does it become unnecessary in the absence of a crash? No, because even if you're the best driver in the world, sometimes a collision is out of your control.

What's more, both your body and your car require regular upkeep and maintenance to remain in peak condition. It's no different with your network security. As technology hurdles forward at an ever-increasing speed, the ways that hackers can infiltrate your network multiply. The best digital security platforms constantly update, enabling them to anticipate these shifts and prevent them from becoming liabilities. This way, you can be proactive prior to a digital crisis, ensuring that no matter what comes, your network is protected.

Even as digital crime climbs at a staggering rate, and hundreds of small businesses are forced to close their doors for good, thousands of owners fail to notice, assuming they'll somehow be spared from an attack. Don't be one of them. Invest in regularly maintained, powerful cyber security, and ensure the future of your company.



Three Ways to Think Differently about Your LinkedIn Profile

by Lynne Franklin

I recently gave a program on the "10 Biggest Mistakes in LinkedIn Profiles" before the Healthcare Businesswomen's Association.

Here are the top three that I didn't find on any other lists online. (Go to: <http://www.yourwordsmith.com/wp-content/uploads/2018/02/10-Biggest-LinkedIn-Mistakes-List.pdf> for a one page list of them all.)

MISTAKE #1: NOT HAVING A GOAL FOR LINKEDIN

You need to know why you're there. "Because everybody else is" is not good enough.

Make your goal specific: to build my network, to find new clients, to attract a new position, etc. Know this may change over time -- which triggers a need to update your profile.

Action Steps: Write your goal to move it from your short-term into your long-term memory (it's neuroscience!). Use this to help you make decisions: Should I write an article? Should I share someone else's post? Should I connect with someone? When you have a clear goal, these decisions are easy.

MISTAKE #2: NOT THINKING ABOUT YOUR IDEAL CONNECTION

Develop an avatar (up to three) of your ideal connection(s). Make sure each one tracks back to your goal for being on LinkedIn. Keep this person in mind as you create your profile, post information and connect with people

Action Steps: Clearly describe the avatar's qualities to create a clear picture in your mind.:

- Woman or man
- Age
- Current position
- Type of organization
- Pains (s)he faces or gains (s)he wants
- The key words this person would use to search for you
- Family life
- Location
- Past positions
- Education
- Hobbies
- Other important facts

MISTAKE #3 TELLING RATHER THAN SHOWING

LinkedIn is *not* your online résumé. I call it "the conversation *before* the conversation." This is where people decide if they want to connect with you.

Start by *stripping the four most overused words from your profile*: motivated, passionate, creative, driven. Don't describe yourself (particularly with the same words everyone else uses) show us you in action.

Tell one good story about the value you created in each position: something that speaks to your ideal connection's pains or gains.

For example: "A CEO wanted to ask her board for money for acquisitions. She faced a big barrier: the company wasn't profitable now. We designed her formal remarks to address directors' concerns, and then practiced answering tough objections. She felt so prepared that the meeting was almost a non-event. After her presentation, the board deliberated for 15 minutes, called her back in, and gave her the dough."

In past positions, explain what you learned there that you still use today: "There's nothing like standing before a group of adults for eight hours -- who expect you to be boring -- to teach you how to grab an audience and hold its attention! This position taught me how to write good presentations, train executives and keep an audience engaged."

Action Steps: Brainstorm on good stories that show how you work and the value you added for each position. Then pick the one that would most appeal to your ideal connection.

MAKE NO MISTAKE: SET A TIMELINE FOR DOING THIS

If you don't block out time to make these three enhancements, they'll never happen. And you'll continue to have the same bland profile that doesn't attract the folks you want. I want *more* for you than that -- and *you* should, too!



Lynne Franklin is a corporate and marketing communications consultant and speaker. What she does best is create meaningful communications to help businesspeople solve their problems and get what they want. To learn about how she can help you, contact Lynne at 847-729-5716 or lynne@yourwordsmith.com

Technology Tidbits

The "Not Me!" Problem...And Why This Is Almost Guaranteed TO Happen To You

Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea. But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three

times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

7 Things Mentally Strong Leaders Never Do

Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1. They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.
2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.
3. They accept criticism with open

arms. Instead of protecting a fragile ego, mentally strong leaders take unfavorable feedback and use it to improve their processes.

4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.
 5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.
 6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.
 7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.
- *Inc.com* 12/12/2017

The Lighter Side....

Five surgeons from big cities are discussing who makes the best patients to operate on.

The first surgeon, from New York , says,

'I like to see accountants on my operating table because when you open them up, everything inside is numbered.'

The second, from Chicago , responds, 'Yeah, but you should try Electricians! Everything inside them is color coded.'

The third surgeon, from Dallas , says, 'No, I really think librarians are the best, everything inside them is in alphabetical order.'

The fourth surgeon, from Los Angeles chimes in:

'You know, I like Construction workers...Those guys always

understand when you have a few parts left over.'

But the fifth surgeon, from Washington , DC shut them all up when he observed:

'You're all wrong. Politicians are the easiest to operate on. There's no guts, no heart, no balls, no brains, and no spine.. Plus, the head and the ass are interchangeable.'

These great questions and answers are from the days when Hollywood Squares' game show responses were spontaneous, not scripted. These are the ones we can publish here.

Q. If you're going to make a parachute jump, at least how high should you be

A. Charley Weaver: Three days of steady drinking should do it.

Q. Which of your five senses tends to diminish as you get older?

A. Charley Weaver: My sense of decency.

Q. According to Ann Landers, is there anything wrong with getting into the habit of kissing a lot of people?

A. Charley Weaver: It got me out of the army.

Q. Who stays pregnant for a longer period of time, your wife or your elephant?

A. Paul Lynde: Who told you about my elephant?

Q. Jackie Gleason recently revealed that he firmly believes in them and has actually seen them on at least two occasions. What are they?

A. Charley Weaver: His feet.

Q. According to Ann Landers, what are two things you should never do in bed?

A. Paul Lynde: Point and laugh

March 2018



35 Aztec Court
South Barrington,
IL 60010

(312) 752-4679

www.bssi2.com

“We make all of your computer problems go away without the cost of a full-time I.T. staff”

New Help Desk Technician

We want to introduce the latest edition to the BSSi2 support team: meet Amani Emilio, first grandson to our president Scott Bernstein. While only 7 lbs 14 ounces and 20”, he has a mean set of lungs. For those who need IT support and want to cry to us about needing help, we will put you in touch with Amani and you can cry together.

© MARK ANDERSON

WWW.ANDERSTOONS.COM



“Here’s what you’re going to do. You’re going to give those 3 million people their credit card numbers back and you’re going to say you’re sorry.”



Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

- f www.facebook.com/NickAEsp
- t twitter.com/NickAEsp
- in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

- f www.facebook.com/bssi2
- t twitter.com/BSSi2llc