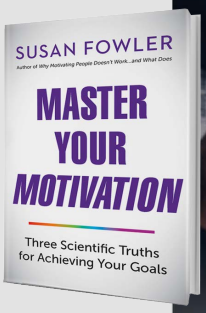
The tech chronicle

## Master Your Motivation

**By Susan Fowler**




"You have the power to change your behaviors," says Susan Fowler, "but to be successful in changing, you need an evidenced-based framework for motivation and techniques for applying it." In her 2019 book, *Master Your Motivation: Three Scientific Truths For Achieving Your Goals*, Fowler brings her decades of research into a guide that delivers such a framework.

*Master Your Motivation* is a refreshing look at what makes us strive for more. If you have team members who you feel lack motivation (or if you feel you lack motivation yourself), this is a book that can help identify why that is — and what you can do about it. It can help you put together a plan for your best next step.

**February 2020**

GRS TECHNOLOGY SOLUTIONS

### Our Mission:

To enable you to achieve your technology goals by being and integrated IT partner within your organization.

# If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybe criminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage.

Continued on page 2

... continued from Cover

They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

> **"The reality is that cyber security should be a normal, everyday part of any business."**

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – fi ewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

## News to Share

GRS is participating in the **Annual Review 2020: Hot Issues in Federal Contracting** on March 12, 2020 at the MGM National Harbor!


We will be discussing the CMMC Certification and how DoD contractors can make the shift easily and effectively.

The conference serves as a refresher on the developments in contracting over the past year, covering topics like GSA and VA Schedule updates, Trends in Bid Protests, Legal Compliance Issues, FAR Updates, and more.

## Cartoon of The Month


"Remember, once you get past my secretary, assistant, and security, my door is always open."

# 6 Time Management Tips For The Busy Entrepreneur

*Face it, there will never be enough hours in the day to accomplish everything you need to do. But if you methodically review how you spend your days and instill focus and discipline while completing daily priorities, you will soon find more time to work on the long-term success of your business. Here are six ways to do it.*

**1. CONDUCT A TIME AUDIT.**
Sit down and review three months of activity. The data from the analysis will show where you spent your time (which projects, tasks and priorities demanded your attention) and with whom you collaborated to get the work done. The audit will also shed light on areas where you were distracted, where you were the most productive and which tasks/projects took more (or less) time than anticipated.

**2. ELIMINATE TIME DRAINS.**
These are the kinds of things that sneak up on you and steal time and can be better put to use growing your business. Look for these time drains: not delegating tasks, not managing meetings efficiently (Tip: always have an agenda!) and spending too much time writing/responding to e-mails. If you've done your job as a leader, members of your team can handle a majority of meetings and e-mails. You hired great people. Now let them do their jobs.

**3. TAKE CONTROL OF YOUR CALENDAR.**
Remember: you drive your schedule; don't let others drive it. Block time throughout your day and guard against changing your schedule to work on tasks that are not important or urgent. The way you allocate your time has a direct correlation to your effectiveness as a leader and, ultimately, the performance of your business. Prudent calendar management will also send a strong signal to your team that you take this seriously.

**4. PLAN YOUR DAY.**
When you know your priorities for the day, you will be better prepared to reset your work schedule if the unexpected comes your way. Once your schedule is set, block off chunks of time to work on your priorities. I recommend 90-minute blocks so you can concentrate on big-picture items or work on a group of related tasks. Stay disciplined and don't allow yourself to go over that allotted time.

**5. LIMIT INTERRUPTIONS.**
Now comes the hard part. Once you start working on each priority, you need to remain focused. Close the door and don't answer the phone unless it's a critical issue. Avoid checking e-mail. Don't let distractions slow you down.

**6. HOLD YOURSELF ACCOUNTABLE.**
Share your tasks, priorities and deadlines with a colleague. Meet with that person at least monthly to review how well you managed your time. The probability of success increases when you have someone watching your progress and coaching you across the finish line.

*Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the* New York Times *best-selling book,* Who: A Method For Hiring, *and the author of the No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*

## Who Wants to Win A $10 Starbucks Gift Card?

The winner will receive a $10 gift card to Starbucks and has to be the first person to correctly answer our quiz question.

Why did Congress pass laws protecting civil rights during Reconstruction?

a) To reverse the Dred Scott decision

b) To abolish black codes in the South

c) To punish former Confederate soldiers

d) To help former slaves migrate to the North

Email Us Right Now!

newsletters@grstechnologysolutions.com

# Top 7 Things To Do So You DON'T Get Hacked When Shopping Online

**1. Verify the URL is safe.** Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

**2. Verify the URL is accurate.** Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

**3. Use a secure web browser.** Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

**4. Don't click suspicious links or attachments.** Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

**5. Always bookmark authentic websites.** When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

**6. Rely on a password manager.** It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

**7. Use the official mobile apps for online stores.** If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

**TOP TIPS FOR SCALING SECURITY FOR YOUR SMALL BUSINESS**

**Put a greater emphasis on passwords.** As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

**Rely on multi-factor authentication (MFA).** MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security. There are many MFA options available for different-sized businesses. Make it a part of your cyber security policy. *Small Business Trends, Nov. 1, 2019.*

## 4 Business Trends To Watch Out For In 2020

**Great Emphasis On Automation Software**
From accounting to data entry, more processes are becoming automated, and small-business owners love the time (and money) savings.

**Remote Work Becomes More Popular**
Research shows employees love the option to work remotely, and it can improve productivity.

**Generation Z Is Crucial To Small-Business Success**
Gen Z is coming into their own. Like millennials before them, they're a market that can't be ignored.

**Technology Improves Customer Service**
Thanks to numerous web apps and automated software, it's easier than ever to engage (and keep in contact) with your customers.

## Refer a Friend 250!

Know someone who has a slow computer network or bad IT? We can help! Simply enter their contact information in the form on the right. We will reach out to see how we can help.

**Once your referral becomes a GRS client, we will give you both $ 250! Visit www.grstechnologysolutions.com/referral-program or call 703.854.9559**

GRS
TECHNOLOGY SOLUTIONS

4114 Legato Road, Suite 250
Fairfax, VA 22033

## Inside This Issue:


- If You Think Your Business is Too Small to Be Hacked...You're a Cybercriminal's #1 Target
- GRS will attend to The Annual Review 2020: Hot Issues in Federal Contracting
- 6 Time Management Tips for The Busy Entrepreneur
- Top 7 Things to Do so You Don't Get Hacked When Shopping Online
- 4 Business Trends to Watch Out For in 2020