progressive computing
51 Smart Ave. Suite 200
Yonkers, NY, 10704

progressive computing

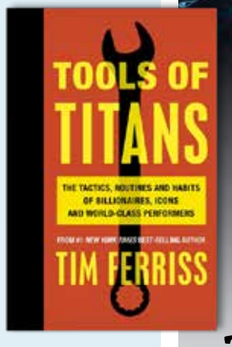
THE PROGRESS REPORT

Everything you need to know in a few minutes or less...

646-760-2071 • www.ProgressiveComputing.com

Inside This Issue

Tools Of Titans
By Tim Ferriss



Tim Ferriss has interviewed many successful people over the years and gained an incredible level of insight into how successful people operate day-to-day. In his book *Tools Of Titans: The Tactics, Routines And Habits Of Billionaires, Icons And World-Class Performers*, Ferriss puts that insight and wisdom to the page.

In *Tools Of Titans*, you'll find a curated selection of Ferriss's essays, along with "healthy, wealthy and wise" tips from the overachievers, including actor Kevin Costner, LinkedIn co-founder Reid Hoffman and political commentator Glenn Beck, to name a few.

3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security *once*. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years. Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up-to-date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand The Threats

It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cybercriminals rely on social engineering.

Continued on Page 2 ...

July 2020

This monthly publication provided courtesy of Ugo Chiulli, CEO & Co-Founder of Progressive Computing.

Our Mission:

We believe that our partners deserve the best possible service and support. We strive daily to improve our systems, processes and procedures to ensure that we can make a lasting relationship. Please don't hesitate to reach out if you have any questions or concerns about the service we provide.

3 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. *Inc., July 30, 2019*

HOW MALWARE CAN CRIPPLE YOUR BUSINESS

Every year, the number of malware attacks on small businesses increases. Semantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. *Small Business Trends, Oct. 12, 2019*

... continued from Cover

The most common form of social engineering is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file. Cybercriminals have gotten VERY sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. This helps keep your employees from becoming the weak link in your security setup.

> **"Proactive monitoring means your network is being watched 24/7."**

Update, Update And Update

From software to hardware, you must stay updated. There is no such thing as "one-and-done" when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software.

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring

When it comes to the security of your network and overall business, being proactive can make a huge difference. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, "How am I going to do all this?" You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

Help Us Out And We'll Give You A Brand-New Kindle Fire For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of July.

Simply refer any company with 15 or more computers to our office to receive a FREE computer network assessment (a $397 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Kindle Fire of your choice as a thank-you (or donate $100 to your favorite charity ... your choice!).

Simply call us at **646-760-2071** or e-mail us at **sales@progressivecomputing.com** with your referral's name and contact information today!

Cartoon Of The Month

"I used to be in advanced business platform solutions, now I just make stuff work."

SHINY NEW GADGET OF THE MONTH

FitTrack – A Smart Scale That Does More

The bathroom scale isn't always the most useful device in the home. FitTrack is a smart scale that aims to change that. It's a different kind of bathroom scale that gives you *much* more than a single number.

Traditional bathroom scales don't tell you anything about what's happening in your body. FitTrack *does*. It gives you an "inside look" into what's going on inside your body. It measures your weight, body fat percentage, body mass index, muscle and bone mass, hydration and more. In fact, it tracks 17 key health insights.

The advanced scale pairs with the FitTrack app, which you can download to your smartphone and connect to the smart scale. All you do is step on the scale with your bare feet – the scale actually reads electrical signals from your body – and it sends the results to your phone. Simple and useful. Learn more about FitTrack at **bit.ly/2VOg7Vs**.

Have You Received A 'Smishing' Text?

Smishing, or SMS phishing, is similar to phishing. With phishing, scammers send fraudulent e-mails with links or attachments. The goal is for the recipient to share sensitive details, like bank passwords, or to install malware on their computer so the scammer can ultimately steal or extort money from them.

With smishing, the scammer sends a text message instead. Scammers often pose as banks or government agencies (like the IRS or the Social Security Administration). The text may say your accounts have been compromised or that you're owed money — all you have to do is click the link in the text and share sensitive information.

The best thing to do is delete these types of text messages. Never respond and never click on anything in the message.

Building Confidence As A Business Leader

How can you build your confidence as a CEO, investor or entrepreneur?

My colleagues and I at ghSMART see many talented people work hard to build their confidence.

New CEOs have impostor syndrome. Private equity investors who just raised another $1 billion in funds read newspaper headlines about the coming recession and quietly gulp. Self-made billionaire entrepreneurs worry that their fortunes will take an embarrassing hit. Newly elected government leaders worry about whether their results will live up to their campaign promises.

We find that leaders are less confident when they obsess about things they can't control, rather than take action in the areas they can control.

Like what?

The *Wall Street Journal* reported the results of a Conference Board survey (Jan. 16, 2019) of what is on the mind of 800 CEOs.

External Hot-Button Issues

1. Recession
2. Global trade
3. Politics

Internal Hot-Button Issues

1. Attracting and retaining top talent
2. Disruptive technologies
3. Developing the next generation of leaders

What this survey says to me is this: it's good to be aware of issues that are outside of your control – recession, global trade and politics. But it's even more brilliant to master the things that are within your control – hiring and retaining top talent, developing digital capabilities and developing the next generation of leaders.

How much confidence do you have in your team?

If you have a high degree of confidence in your team, then keep doing what you are doing to hire and develop them.

But if you don't have a high degree of confidence in your team, then you should focus on hiring, developing and retaining more of the right people who fit your strategy and who can achieve the results you seek.

How?

There are three ways to build confidence in your team. You can invest the time to master the skills and best practices around hiring, developing and retaining top talent yourself. You can engage ghSMART to do it for you. *Or* (what most of our clients do) you can engage ghSMART to solve this problem immediately and build your skills in this area for your long-term success. (A quick side note: I'm very proud to report that my colleagues achieved 99% "high" client-reported satisfaction over the past 12 months. So, to go with this confidence theme, I have a very high degree of confidence that my team will help you solve your #1 problem!)

A great way to build confidence in yourself as a leader is to build your confidence in your team.

If you are the CEO of a company that generates over $1 billion in revenue (or has raised at least a $1 billion fund), then please reach out if you would like my team to help you build confidence in your team to deliver the results you want to achieve for customers, employees and shareholders.

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.*