

**Come See Us at the
2019 Annual Florida
Bar Convention!**

**Please stop by and see
us at booth #113 during
the upcoming 2019
Annual Florida Bar
Convention held at the
Boca Raton Resort and
Club June 26th - June
29th!**

**For more information,
visit here:**

www.palmtech.net/events/



Top 3 Leadership Strategies I Learned From Peyton Manning

Peyton Manning doesn't need much of an introduction. Whether you're a football fan or not, you've got to respect his hustle: Considered one of the greatest quarterbacks of all time, with a career spanning 18 seasons of play, he's the only quarterback in history with Super Bowl wins under his belt from two different franchises. Not only that, but he's been named MVP five times – more than any other NFL player – and holds the record for career touchdown passes. To top it off, he's a consummate philanthropist: His charity, the Payback Foundation, is dedicated to providing opportunities to disadvantaged and at-risk kids.

With so many accolades squirreled away in his trophy case, it'd be easy to assume that the friendly, easygoing Manning you see off the field is only a fabrication. As far as I could tell from seeing him speak at a recent boot camp, though, the man is

frustratingly faultless. Luckily, as a born leader, he is also eager to share his wealth of knowledge with others. Here are three of the top leadership strategies I learned from the retired football icon and how to implement them in your life and business.

1. THE 4 KEYS TO BEING A TOP PERFORMER

At his peak, Manning was one of the few individuals in the world to truly reach that lofty pinnacle of being the absolute best at what he did. Asked what got him there, he cited an attitude founded on four primary pillars for success.

Whatever field you're in, he says, "You certainly gotta have the ability." But, of course, that's far from enough. "You gotta combine that ability with a strong work ethic. You hear about it in sports all the time: 'hard worker, just not very talented' or 'super-talented, just not a very hard worker.'" If you cultivate *both* traits, he

continued on page 2



This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

**To equip small and midsize
businesses in the West Palm Beach
area with a smooth running and
seamless IT platform that enhances
productivity, improves efficiency,
and creates a competitive
advantage.**

argues, that's what will set you apart from the pack. And then, what will drive you a notch higher is your passion. "You gotta love your job. [My brother] Eli and I always used to kid – we'd never tell the owners this – we would play for free, 'cause we loved football that much." If you lack that fire for what you do, he adds, "it'll show up somewhere."

The final component, he says, is a sense of accountability. "That's what always kind of drove me, that people were counting on me – coaches, teammates, fans. You don't want to let them down."

2. DO YOUR HOMEWORK

Manning had a reputation for being one of the most consistently prepared quarterbacks in the NFL. By all accounts, the sheer level of detail he would put into his game plan was second to none.

When asked what steered him toward this habit, he has a pretty straightforward answer. "I always felt that preparation was where I could get an edge on the competition," he says. "I couldn't outthrow anybody, I couldn't throw at 75 to 80 yards down the field. If you've ever seen me play, you certainly know I couldn't outrun anybody; I had a coach tell me once that I couldn't run out of sight in a week – that was nice. But I thought that I could out-prepare anybody, and so that's what I based my

game plan on."

When he was growing up, he says, his dad was always providing him with the wisdom of sports leaders. When he was 14, his dad gave him a quote from Chuck Noll, then-coach of the Pittsburgh Steelers: "Pressure is something that you feel only when you don't know what you're doing." It's okay to get nervous and excited, Manning says – that just means you care about your work. "But *pressure* means you haven't done your homework." It's easy to get bored of the fundamentals, he says, but their mastery will be what leads you to victory.

3. LEARN FROM YOUR MENTOR'S EXAMPLE, AND THEN LEAD BY IT

Manning was fortunate to be coached for years by some of the most skilled sports leaders in the country. But one of his greatest influences was the legendary coach Tony Dungy of the Indianapolis Colts. "He had a very unique style of leadership," Manning says. "Never raised his voice. Never used any kind of language, but he treated you like such a professional that you just didn't want to let him down."

According to Manning, Dungy peppered his coaching with a lot of pithy little expressions, things like "Take care of the little things, and the big things will take care of themselves"; "Expectations, execution"; "No excuses, no explanations." "He was just as calm in the fourth quarter of the Super Bowl as he was out there at practice every day. When your leader is calm, the rest of your team following can be calm as well."

The best leaders, Manning says, walk the walk as well as they talk the talk. Pay attention to the habits and advice of those you admire, implement them into your own practice and success will always follow.

"The best leaders, Manning says, walk the walk as well as they talk the talk."

Shiny New Gadget: FlexSafe Will Protect Your Valuables

Beachgoers all know the security dilemma that comes with a stray wallet. When it comes time to put on your trunks and head into the sea, do you bury your valuables in the sand? Hide them under a towel? Or leave them be and hope for the best?

For all of those who find each of these options less than ideal, there's FlexSafe. It's a handy, personal, portable safe designed to stave off thieves, wherever you are. Water-resistant, slash-proof, RFID-blocking and equipped with a heavy-duty three-digit combination lock, it turns you from an easy target to a walking fortress. The bag-shaped design clips into itself, allowing you to secure it to a beach chair, umbrella or any other unwieldy surface and go on your merry way without worry. At \$59.99, it could be a sound investment for those of us finding ourselves leaving our valuables exposed on the regular.



4 Things You Should Do RIGHT NOW To Protect Your User Account In Case It Gets Hacked

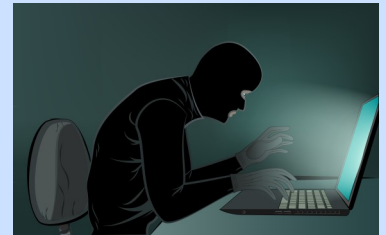
Last year, the top 15 hacks compromised more than 2.5 billion user accounts. You can safely assume that, even if you haven't been notified, it's likely your data is out there as well. So, get savvy and follow these simple tips.

1. Enlist in protection. In the wake of these high-profile breaches, many companies have extended free credit and identity monitoring as an olive branch to stave off lawsuits. Take advantage of it. Even if it's not free, it might be worth investing in.
2. Close loose ends. Only make an account for sites you actually visit regularly. Use guest accounts whenever possible, and delete accounts you never use.
3. Use a password manager. Seriously, most people's passwords are an absolute joke. A password manager allows you to use a different, powerful and unique password for every account you have while still being able to remember it.
4. Freeze your credit. If you have been notified of a breach and you're worried, you can take drastic action and set up a credit freeze with each credit agency you work with. Alternatively, you can just set up a free fraud alert. *Inc.com*, 12/11/2018

Top Tips To Protect Your Business From Social Engineering Attacks

Every year, millions of attacks are successfully carried out against businesses just like yours. It's important to know what you're up against and how to protect yourself.

The most common social engineering tactic is phishing, often coupled with a strategy called pretexting. By gaining the trust of the victim, hackers are able to lure them into giving out sensitive personal information. Also be on the lookout for baiting, in which attackers offer free downloads, such as movies or e-books, and demand personal information from the victim. The best tools against phishing are online filters that automatically detect phishing scams, security programs, antivirus programs and education on best online practices. It should be obvious to your employees that giving out personal or company information is something they should never ever do outside of trusted sites that they can confirm are genuine. *SmallBizTrends.com*, 2/28/2019



Are You Prepared For Hurricane Season?

Even if you feel your business is not likely to face the brunt of a hurricane's landfall, you should take steps to prepare for hurricane season. With talk of a busy hurricane season ahead, it is important that any business which might face heavy storms takes extra precautions. Extreme weather of any kind, from tropical depression and storms to Category 5 hurricanes and tornadoes, can not only cause structural damage to your business, but can also cause catastrophic data loss and network damages. Visit www.palmtech.net/hurricane-prep/ to download our [Extreme Weather Checklist!](#)



IT Terms You Need To Know

Jargon can be intimidating if you're dealing with IT issues and you're anything but techy. Running an anti-malware scan can generate auto pop-ups that leave you clueless with IT terms that sound Greek. Learning the basic concepts listed here will help you move on and not be surprised the next time that happens.

Malware: For a long time, the phrase "computer virus" was misappropriated as a term to define every type of attack that intended to harm or hurt your computers and networks. A virus is actually a specific type of attack, or malware. Whereas a virus is designed to replicate itself, any software created for the purpose of destroying or unfairly accessing networks and data should be referred to as malware.

Ransomware: Don't let all the other words ending in "ware" confuse you; they are all just subcategories of malware. Currently, one of the most popular of these is "ransomware," which is malware that encrypts valuable data until a ransom is paid for its return.

Intrusion protection system(IPS): There are several ways to safeguard your network from malware, but IPSs are quickly becoming one of the non-negotiables. IPSs sit inside of your company's firewall and look for suspicious and malicious activity that can be halted before it can exploit or take advantage of a known vulnerability.

Social engineering: Not all types of malware rely solely on fancy computer programming. Experts agree that the majority of attacks require some form of what is called "social engineering" to be successful. Social engineering is the act of tricking people, rather than computers, into revealing sensitive or guarded information. Complicated software is totally unnecessary if you can just convince potential victims that you're a security professional who needs their password to secure their account.

Phishing: Despite often relying on face-to-face interactions, social engineering does occasionally employ more technical methods. Phishing is the act of creating an application or website that impersonates a trustworthy and often well-known business in an attempt to elicit confidential information. Just because you received an email that says it's from the IRS doesn't mean it should be taken at face value — always verify the source of any service requesting your sensitive data.

Antivirus: Antivirus software is often misunderstood as a way to comprehensively secure your computers and workstations. These applications are just one piece of the cybersecurity puzzle and can only scan the drives on which they are installed for signs of well-known malware variants.

Zero-day attacks: Malware is most dangerous when it has been released but not yet discovered by cybersecurity experts. When a vulnerability is found within a piece of software, vendors will release an update to amend the gap in security. However, if cyberattackers release a piece of malware that has never been seen before, and if that malware exploits one of these holes before the vulnerability is addressed, it is called a zero-day attack.

Redundant data: When antivirus software, patches, and intrusion detection fail to keep your information secure, there's only one thing that will: quarantined off-site storage. Duplicating your data offline and storing it somewhere other than your business's workspace ensures that if there is a malware infection, you're equipped with backups.

We aren't just creating a glossary of cybersecurity terms; every day, we're writing a new chapter to the history of this ever-evolving industry. And no matter what you might think, we are available to impart that knowledge on anyone who comes knocking. Get in touch with us today and find out just how we can help you with your IT woes. -Techadvisory.org



**THE DARK WEB IS A
SCARY PLACE**

LET US GO THERE FOR YOU

CONTACT US TODAY FOR A FREE DARK WEB SCAN

PAI MTECH
IT SOLUTIONS FOR BUSINESS

(561) 969-1616

**Are Your Credentials
For Sale On **The**
Dark Web?**

Visit

**[www.palmtech.net/
darkweb/](http://www.palmtech.net/darkweb/)**

For A Free Scan!