

Technology Times



*"Insider Tips To Make Your Business Run Faster, Easier,
And More Profitably"*

What's New

Free Webinar Ransom Ware Defense System

Happy Spring 2018

Unified system is please to offer Ransomware free webinar.

This will show you managed service benefits and any promo with the current service. There will be a drawing of a free managed Antivirus license
Webinar on

15th May ,2018 at 4pm.

You can also sign up for our IT Security Tip of the Week to get a valuable security tip every Monday morning. Sign up for the tips at

<http://www.unified-system.com/securitytipoftheweek/>

Call us for more info

781 354 4929 or email

info@unified-system.com

March 2018



Tim Wilkins
President/Unified System, Inc.

This monthly publication is provided courtesy of Tim Wilkins, President of Unified System in Bedford, MA.

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine!* Call us and put an end to your IT problems finally and forever!"

- **Tim Wilkins, Unified System**

You can send us your Feedback, subscription requests or cancellations to: newsletter@unified-system.com.

We want to hear from YOU!



5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time - approximately 60% according to the *Harvard Business Review* - an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For

continued on pg2

Get More Free Tips, Tools, and Services At My Web Site: www.unified-system.com

this reason, most cyber-attacks come down to a lack of cyber security education.

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away,

"It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data... [b]ut there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."

you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, and personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entrepreneur.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE assessment or call our office at (781) 276-4567.

Shiny New Gadget Of



FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the \$59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

Cash In On Your Million-Dollar Idea

Nick Saban, head football coach at the University of Alabama, has won six national championships, one while he was head coach at LSU and five at Alabama. The five championships at the University of Alabama have happened in a span of only nine years – the biggest run in college football history.

In football, you can only put 11 men on the field at one time. It's your best against their best, and while talent is critical, it's far from everything. What is Alabama's magical formula for success, and why do so many teams have trouble duplicating it?

A few years ago, Coach Saban asked me to present a program on communication to his coaching staff. In his world, recruiting star athletes is paramount to their success, and he wanted his coaches to make the best presentation possible to the athletes they wanted to play for Alabama.

I learned a lot of things about Coach Saban and Alabama football preparing for my three-hour program. There are a lot of coaches, managers, bosses, and leaders out there who never mix with the people on the front lines. Not Coach Saban; he is all about being on the ground level, getting "dirty" in the details. In fact, I don't believe I have ever met anyone as detailed as he is. Meetings and practices are planned to the minute, and everyone understands what is expected of them and how



they are to accomplish it. In the football world, he's become famous for what most call "The Process." As he puts it, "The Process is much more important than the result."

The critical element of his success is a simple way of breaking everything down into manageable parts. He owes this technique to Dr. Lionel Rosen, a Michigan State University psychiatry professor he met when he coached there in the late 90s. Dr. Rosen studied cognitive therapy used in the Alcoholics Anonymous recovery program and found the best way to succeed was to deal with the moment, not the future or past. If you handle the moment correctly, the final result will work out.

Dr. Rosen pointed out to Coach Saban that the average play in a football game lasts only about seven seconds, and that is where he needed to concentrate. The last play is done – it's the next play, the next seven seconds, that counts. Ensuring that his players know exactly what they have



MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Proventus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small-business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book *The Toilet Paper Entrepreneur*. His newest book, *The Pumpkin Plan*, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.

Riddle Me This

What time do ducks wake up?

Answer to Previous Issue's Riddle: A Mailbox.

The pain that you've been feeling can't compare to the joy that's coming.
Romans 8:18

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.

Who Else Wants To Win A \$25 Gift Card?

Be the first person to call us with the correct answer to this month's trivia question and we will send you a \$25 gift card to Panera Bread!

The correct answer for last month trivia was c) IBM Selectric

Now, here's this month's trivia question.

The next major step in the automated computer was the development of something that was widely used for nearly a hundred years.

What did Herman Hollerith and James Power develop in 1890?

A) Punched cards B) Confetti C) Ticker tape D) Papier mache

*Call us or email us right now with your answer!
781-276-4567*

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