two river™
TECHNOLOGY TIMES

What's New

Authorities Seize Largest Stolen-Login Marketplace Site On The Dark Web

Earlier this year, the Department of Justice announced that they, along with other international authorities, had seized Slilpp, the largest site for stolen login credentials on the Dark Web. The site had over 80 million user credentials lifted from 1,400 service providers.

Authorities from four different countries all helped the FBI seize servers that hosted Slilpp. They also arrested and/or charged 12 people involved with operating the site.

Eighty million user credentials from 1,400 sites is a lot of sensitive information. That said, though, the Department of Justice still hasn't ascertained the full impact of the illegal activity on Slilpp. In the U.S., activity on the site led to almost $200 million in losses–and that's just a tiny fraction of the total activity.

The fight isn't over, but this case is a big win against illegal login sale marketplaces. The Department of Justice hopes for more seizures like this one in the future.

September 2021

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

"As a business owner, 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!"

How Co-Managed IT Could Save Your Company From Financial Disaster

When you consider the investments in your business that you can make as a CEO, you probably think to yourself, "Which investments will give my company the best ROI?" With that in mind, would you think of making a significant investment in bolstering your IT department?

Many CEOs are understandably hesitant to throw a lot of money into their IT department because the ROI is more difficult to estimate. That said, though, consistently updating your company's IT services is becoming increasingly crucial to the continued success, and indeed safety, of your company. Ransomware and other cyber-attacks that steal company data are becoming more frequent and more costly, while IT departments continually get the short end of the budgetary stick.

While that all undoubtedly sounds horrible, you might be wondering just what you can do about it. After all, you only have so much money you can invest back into your company's IT department, and it might not be sufficient for keeping your IT staff from getting burned out, disgruntled or making costly mistakes – even when they're performing their responsibilities to the best of their abilities.

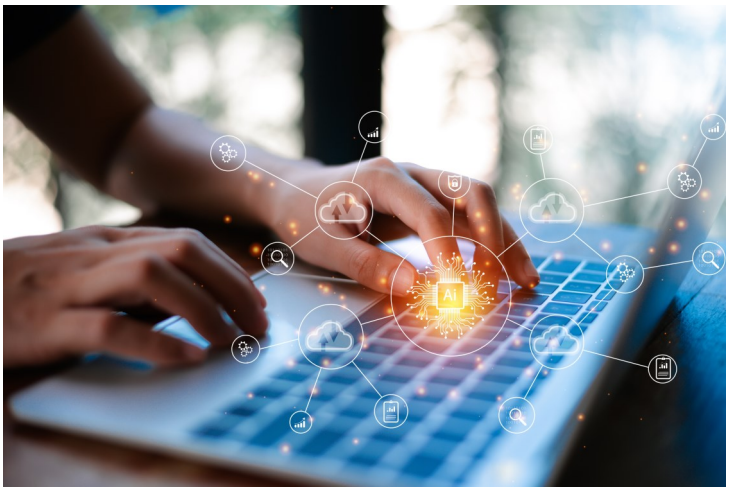
What if there were a way that you could have access to the most up-to-date IT knowledge and software while also not having to shell out the funds necessary to update your systems and hire more knowledgeable employees? Well, that's where co-managed IT can be your company's life preserver.

Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks as well as assisting in your daily operations where needed. Think of it as "filling in the gaps" that your current IT department (try as they might) struggle to fill.

Continued on pg.2

Continued from pg.1

For instance, say your current IT department is great at taking care of the day-to-day fires that inevitably come up in a normal workday, but they struggle to get to the "important but not urgent" task of updating your company's cyber security and creating data backups. Maybe it's the other way around, where your IT department is very focused on security, but they struggle to find time to assist employees with password resets and buggy programs. Maybe neither of these cases describes your IT department, but they still need better access to the tools and software that would allow them to reach their full potential in protecting the company's sensitive information. Or maybe your company is going through a period of rapid expansion, and you just don't have time to build the kind of IT infrastructure that would best serve your needs.



Regardless of what your IT department's current needs are, co-managed IT is the solution. We're here to do the tasks and provide the tools that your current IT department just can't provide. Make no mistake, however: our intent is not to replace your current IT leader or team. In fact, we rely on the expertise that your IT department has about your systems. That's what makes up the "co" in "co-managed IT."

"Co-managed IT is a flexible system for keeping data for your company, employees and clients safe from cyber-attacks, as well as assisting in your daily operations where needed."

In order for co-managed IT to work, your company's IT department will need to see us as an ally in doing their job, not as an adversary. At the same time, they'll also need to be open to new ways of doing things. The world of cyber security is constantly changing, and if your IT department is set in their ways and unwilling to budge, your company will be left with an antiquated system, chock-full of valuable data that hackers and cybercriminals can easily exploit.

Finally, however, in order for co-managed IT to work, your company still must be willing to invest in its IT department. We know that the ROI might not be as clear as it is for some other investments, but trust us, the consequences of not having up-to-date IT services if (or when) hackers steal your sensitive data could financially devastate your company – or even end it altogether.

So, with that in mind, we hope you'll consider the benefits of co-managed IT and how it can make your company safe from cyber-attacks and bring you peace of mind.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

To claim your free Report send your request to kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

'Peep' The World Around You

Peeps by CarbonKlean is the ultimate cleaning tool for glasses – far better than your traditional rag, spray or T-shirt. It's compact, easy to use and, most importantly, revolutionary in its ability to not only clean smudges off your glasses but also protect them from the next smudge.

Peeps uses state-of-the-art carbon molecular technology to remove smudges and dirt at a microscopic level as well as keep your lenses clear of contaminants long after you use it.

To clean your lenses with Peeps, simply brush them to remove dust and particles, wipe them between the heads of the tongs and enjoy your crystal-clear vision!

How To Succeed In Business And Life In Just 8 Hours Per Week

Do you want to know my secret to success – how I'm able to live the way I do after growing up in a dysfunctional family, lasting half a semester in college and possessing no special skills, talents or intelligence? Well, I do two things that most people don't do: I study and I plan.

I pull these two levers once every day (and twice on Sunday), and that's what has led to three decades of success. You can follow my example. Like all fundamentals of success, the daily disciplines of studying and planning are easy to understand, but hard to maintain in practice. Most people don't have discipline, and, therefore, they do not succeed. What's more is that in total, you only have to study and plan for eight hours every week! Curious about how that works? Let me break it down for you.

Early each morning, I give myself an hour to study and plan as needed. No matter how early the rest of my day starts, I always start with this hour – no exceptions. I devote the first 30 minutes to studying. When I say "studying," what that basically means is that I'm reading a book to grow one of my core skills. Don't spend that first 30 minutes reading useless crap; only focus on books that will help you grow in some way.

If your response to that idea of studying was that you don't have time to read, then I would say you're lying. Bill Gates, Warren Buffett, Oprah Winfrey, Elon Musk and Jack Ma are all voracious readers. Do you think you're busier than them? Yeah, thought not. They're not the only ones either – the average multimillionaire reads at least two books a month. And guess what? I can get through that many books in a month by reading just 30 minutes a day.

I spend the remaining half of the first hour of my day planning. That means I review my MVPs (most valuable priorities) and walk through my day in my head. Thinking about how I might interact and empathize with people helps me grow my emotional intelligence.

It's also during my planning time that I identify my spotlight moments – the moments when I know my example is on display, where I need to maximize my excellence. Want to know a little secret? Being excellent isn't about trying to be incredible at everything all the time – it's about picking the right moments to maximize your effort and be disproportionately excellent.

So, altogether, if you do those two things for an hour each day, that's seven hours. The eighth hour happens on Sunday afternoon, when I plan out my week. And that's it. That's how you get a massive edge over your peers in whatever you're doing. Too few do it and stick with it, and that will make it all the easier for anyone who does stick with it to succeed.

Darren Hardy is the former publisher of SUCCESS Magazine, *and he has written several best-sellers, including* The Entrepreneur Roller Coaster, Living Your Best Year Ever *and* The Compound Effect. *He is also the recipient of the "Master of Influence" designation from the National Speakers Association (NSA), which honors his professionalism and public speaking ability.*

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

TRTG Happenings

In Memoriam-Lucille Christianson

It is with great sadness that we announce the passing of one of our long time clients, Lucille M. Christianson. Lucille was a wonderful person and an important member of the staff at Garmany in Red Bank. Lucille´s attention to detail was respected and her sincere personality was beloved by everyone who met her. We will dearly miss her positivity, cheerfulness and generosity. Our thoughts and prayers are with her family and the rest of the Garmany Team. For more information about Lucille's life and to pay your respects to her family please visit her memorial page here.

Beware of Back-To-School Scams

As if back-to-school shopping wasn't already a nightmare, experts are warning parents to look out for online shopping scams for school supplies.

With more schools resuming in-person learning this fall, the Better Business Bureau expects a surge in demand and a sharp decline in supply.

The agency is urging shoppers to verify third-party vendors found through ads on social media. "If you see those pop-up ads, use some hesitation and caution with those and double-check the name of the business to make sure they're legitimate," said Sandra Guile, with the Better Business Bureau.

The Better Business Bureau recommends using a credit card when buying online for the additional protections to dispute and resolve charges.

It's OK to lie and you should!

Social engineering is big business. What is it? Figuring out who you are and then using that information to make money off of it. People list password challenge and identity verification publicly or at least freely on their Instagram, Twitter and Facebook pages and feeds without giving it a second thought. Maiden name? Check. Favorite pet? Check. High school? Check. Town they grew up in? Check. Favorite or first car? Check. Throwback Thursday is a social engineer's dream! They love this stuff. Combat it by always giving false password and identity challenge and verification information to the sites and services that require it. Keep the answer file off-line or at least in a format that's not easily guessed. Remember, if it's a handwritten list, you can still take a photo of it.

How to foil ransomware

Not too long ago, the CryptoLocker ransomware virus was all over the news, infecting over 250,000 computers in its first 100 days of release (at least that's the number reported – the real numbers are probably MUCH higher). The threat was fairly straightforward: Pay us or we'll delete all your data.

Ransomware, like the CryptoLocker attack, works by encrypting your files to prevent you from using or accessing them. After your files are compromised, the hackers behind the attack then pop up a demand screen asking for payment ($400 to $2,000) within a set time frame (e.g., 72 hours or three days) in order to get the key to decrypt your files. The last CryptoLocker virus forced many business owners to lose data or pay up since there was no other way to decrypt the files.

Obviously the best way to foil a ransomware attack is to be incredibly diligent about IT security; but with hundreds of thousands of new attacks being created daily, there are no guarantees that you won't get infected. Therefore, it's critical to maintain a full, daily backup of your data OFF-SITE so that IF you do get whacked with ransomware, you can recover all your files without having to pay a thin dime; and don't forget to back up off-site PCs, laptops, remote offices and third-party software data stored in cloud apps as well!