The OnPar Report

"Insider Tips to Make Your Business Run Faster, Easier and More Profitably"

Offer Expiring Soon!

OnPar's Free Telecommunications Bill Analysis

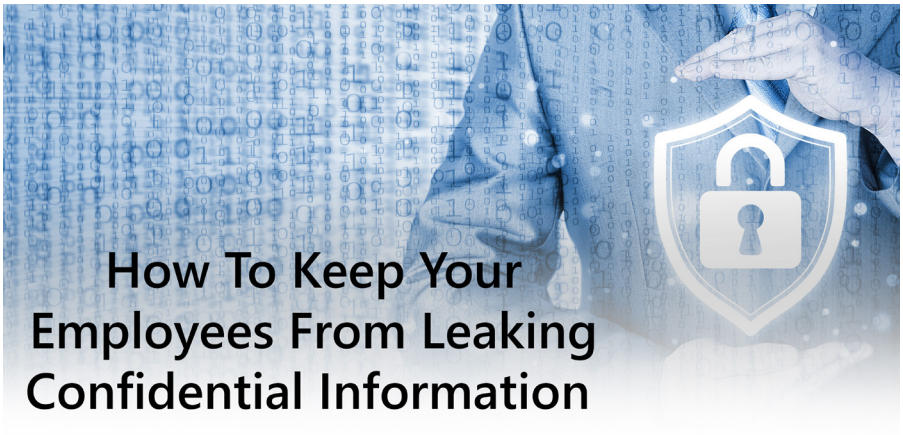
Stop paying tons of money for your phone and data service! This assessment will analyze your current bill to identify areas to cut costs, highlight any potential billing errors, provide tools to better understand your bill, and better understand your company's needs to offer a better solution.

Offer is valid through June 30, 2016. Sign up at: www.onpartech.com/telecommunicationsbill/ or call us at: 919-926-9619

June 2017

This monthly publication provided courtesy of Jeremy McParlan, President of OnPar Technologies

Our Mission: To help our partners unleash opportunities by implementing innovative technology that is simple, lean and integrated, provide a service and support experience second to none, and build a company that employees are proud to work for and one in which customers trust and enjoy doing business with.



How To Keep Your Employees From Leaking Confidential Information

Back in 2014, Code Spaces was murdered. The company offered tools for source code management, but they didn't have solid control over sensitive information — including their backups.

One cyberattack later, and Code Spaces was out of business. Their killer had used some standard techniques, but the most effective was getting an unwitting Code Space employee to help — likely via a phishing attack.

When it comes to cybercrime that targets businesses, employees are the largest risks. Sure, your IT guys and gals are trained to recognize phishing attempts, funky websites, and other things that just don't seem right. But can you say the same thing about the people in reception, or the folks over in sales?

Sure, those employees might know that clicking on links or opening attachments in strange emails can cause issues. But things have become pretty sophisticated; cybercriminals can make it look like someone in your office is sending the email, even if the content looks funny. It only takes a click to compromise the system. It also only takes a click to Google a funny-looking link or ask IT about a weird download you don't recognize.

Just as you can't trust people to be email-savvy, you also can't trust them to come up with good passwords, people still use birthdays, pet names, or even "password" as their passcodes — or they meet the bare-minimum standards for required passcode complexity. Randomly generated passcodes are always better, and requiring multiple levels of authentication for secure data access is a must-do.

Remember, that's just for the office. Once employees start working outside of your network, even more issues pop up. It's not always possible to keep them

Continued on page 2

from working from home, or from a coffee shop on the road. But it is possible to invest in security tools, like email encryption, that keep data more secure if they have to work outside your network.

And if people are working remotely, remind them that walking away from the computer is a no-no. Anybody could lean over and see what they're working on, download malware or spyware, or even swipe the entire device and walk out — all of which are cybersecurity disasters.

Last but not least, you need to consider the possibility of a deliberate security compromise.

When it comes to cybercrime that targets businesses, employees are the largest risks

Whether they're setting themselves up for a future job or setting you up for a vengeful fall, this common occurrence is hard to prevent.

It's possible that Code Space's demise was the result of malice, so let it be a warning to you as well!

Whenever an employee leaves the company for any reason, remove their accounts and access to your data. And make it clear to employees that this behavior is considered stealing, or worse, and will be treated as such in criminal and civil court.

You really have your work cut out for you, huh? Fortunately, it's still possible to run a secure-enough company in today's world. Keep an eye on your data and on your employees. And foster an open communication that allows you to spot potential — or developing — compromises as soon as possible.

FBI: Building A Digital Defense With An Email Fortress

The Best Way To Protect Your Business Is With Advanced Threat Protection and Multi-Factor Authentication

With fraudsters wanting to cash in your business by utilizing phishing schemes and various other tactics to get into your network, it is imperative that you have the right precautions in place to protect your company and employees. Here are some of the things you could experience with Office 365 Advanced Threat Protection and Multi-Factor Authorization.

- **Securing your mailboxes against threats.** New malware campaigns are launched everyday and you need to protect your mailboxes against new and sophisticated attacks in real time.
- **Protect against unsafe attachments.** With safe attachments, you can prevent malicious attachments from impacting your messaging environment.
- **Get rich reporting and track links in messages.** Gain critical insights into who is being targeted in your organization and the category of attacks you are facing.
- **Get more security with fewer hoops.** Get strong authentication with a range of easy verification options to allow customers to choose the method they prefer.
- **Mitigate threats with real time monitoring and alerts.** To help mitigate potential threats, real-time alerts notify your IT department of suspicious account credentials.

To learn more and how to acquire them, go to: www.onpartech.com/defense/
or call us at: 919-926-9619

Our Featured Case Study: MedSource

MEDSOURCE
Taking Relationships as Seriously as Science

MedSource is a full-service niche CRO comprised of over 170 employees that specialize in oncology programs and other complex clinical trials. Their efforts support biopharmaceutical clients who conduct complex trials in the most challenging disease states.

MedSource was using an unreliable on-site Exchange Server. The server was creating a single point of failure due to an outdated design and lack of redundancy. The server was never designed to scale to the number of mailboxes needed, therefore it could have impacted MedSource growth pattern.

OnPar Technologies was then tasked with migrating MedSource's email from their current Exchange 2011 solution to Office 365 Hosted Exchange. Overall, OnPar migrated 177 email inboxes including calendars and contacts. Once the migration was complete, staff members received Microsoft O365 administrative training.

To read more, go to: www.onpartech.com/resources/case-studies/medsource/

Free Upgrade to Windows 10 Enterprise With OnPar Technologies

Powerful Collaboration, Advanced Security and Control, and All The Space You Need. ***Now Through June 30th OnPar is Offering Free Upgrade Assistance to Windows 10* With The Purchase of Windows 10 Enterprise.*** As a customer, you could enjoy the following benefits:

- The Most Secure Windows Ever. Safeguard your sensitive data and devices with advanced security and control features that protect against malware, untrusted apps, and executables.
- Managed by a Trusted Partner. Windows 10 Enterprise is designed to be delivered as a cloud service and managed by a trusted partner, so you get comprehensive management and support for all aspects of implementation and configuration of services and devices.
- Easy Pricing for Small Businesses with Per-User, Per-Month Pricing. Save on up-front costs by paying monthly, only for the users you need. Spend less time managing devices and licenses and get a simpler process for staying compliant by eliminating the need for device counting and audits.

Learn more at: www.onpartech.com/windows10/ or e-mail us at: win10@onpartech.com, or call us at: 919-926-9619

Monthly Security Tech Tip

How To Spot A Phishing E-Mail! A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular website or to click and download a virus. Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail. So how can you tell a phishing e-mail from a legitimate one? Here are a few telltale signs…

First, hover over the URL in the e-mail (but DON'T CLICK!) to see the ACTUAL website you'll be directed to. If there's a mismatched or suspicious URL, delete the e-mail immediately. In fact, it's a good practice to just go to the site direct (typing it into your browser) rather than clicking on the link to get to a particular site. Another telltale sign is poor grammar and spelling errors. Another warning sign is that the e-mail is asking you to "verify" or "validate" your login or asking for personal information. Why would your bank need you to verify your account number? They should already have that information. And finally, if the offer seems too good to be true, it probably is.

It's Simple. Refer A Business To OnPar. Get $200.

Here's how it works:

- Refer a business to OnPar
- If we schedule a consultation with your referral, you will recieve $100.
- If your referral goes on to become our client, you will recieve another $100

To get started go to: www.onpartech.com/refer-a-friend/

Could The Dog Days of Summer Be A Threat To Your Business?

Don't let the summer heat get you down. Protect your server and computer equipment from frying with our FREE "Beat The Heat" Network Audit. For free we will:

- Check your computer network's security settings to make sure you are protected from the latest hacker attacks, worms and viruses.
- Check your data back-up system to ensure it is working properly and accurately backing up all of the critical files and information you never want to lose.
- Verify that you have the most up-to-date security patches installed properly; miss one critical update and you're a "sitting duck."
- Diagnose slow, unstable computers

To Schedule Your FREE "Beat The Heat" Network Audit Today, go to: www.onpartech.com/beat-the-heat/ or call us at: 919-926-9619

**Offer is valid for new customers only. This is a server scan only, or an Active Directory domain is required to complete the audit.*