The OnPar Report

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

Happy Fourth Of July!

The staff at OnPar Technologies would like to wish you, your employees, and your families a happy and safe Fourth of July this summer!

To all current clients: we would like to let you know that we have created a one page quick reference guide for submitting a service a ticket to OnPar Technologies. If you are interested in receiving this document and distributing it within your company to your employees, please email our service manager Andrea Slezak.

July 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.

The Loophole That Lets Insurance Companies Refuse to Cover a Cybercrime Theft in Your Business

As hacking hit the headlines in the last few years -- most recently the global hack in May that targeted companies both large and small -- insurance policies to protect businesses against damage and lawsuits have become a very lucrative market.

Your company may already have cyber insurance, and that's a good thing. But that doesn't mean that you don't have a job to do -- or that the insurance will cover you no matter what.

When you buy a car, you get the warranty. But in order to keep that warranty valid, you have to perform regular maintenance at regularly scheduled times. If you neglect the car, and something fails, the warranty won't cover it. You didn't do your job, and the warranty only covers cars that have been taken care of.

Cyber insurance works the same way. If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain that car. And when something

bad happens, like a cyber attack, the cyber insurance won't be able to help you, just as a warranty policy won't cover a neglected car.

Check out this real life policy exclusion we recently uncovered which doesn't cover damages "arising out of or resulting from the failure to, within a reasonable period of time, install customary software product updates and releases, or apply customary security-related software patches, to computers and other components of computer systems."

If your cyber insurance policy has a clause like that -- and we guarantee that it does -- then you're only going to be able to collect if you take reasonable steps to prevent the crime in the first place. That doesn't just mean you will have

"If your company's IT team isn't keeping systems patched and up to date, taking active measures to prevent ransomware and other cybercrime attacks, and backing everything up in duplicate, it's a lot like neglecting to maintain a car."

to pay a ransom out of pocket, by the way. If your security breach leaves client and partner data vulnerable, you could be sued for failing to protect that data. When your cyber insurance policy is voided because of IT security negligence, you won't be covered against legal damages, either. This is not the kind of position you want to be in.

All of this is not to say that you shouldn't have cyber insurance, or that it's not going to pay out in the case of an unfortunate cyber event. It's just a reminder that your job doesn't end when you sign that insurance policy.

You still have to make a reasonable effort to keep your systems secure -- an effort you should probably be making anyway.

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

Join The OnPar Cash Club!

Here is how you can earn some summer cash:

- Fill out our referral form at www.onpartech.com/refer-a-friend or call us at: 919-926-9619 with your referral information.

- We will call to schedule a consultation with your referral. If we schedule a consultation, we will send you $100 the same day we meet!

- If your referral becomes our client, we will send you a check for another $100.

*Referrals must have between 15-150 PCs and not be an active prospect.

Welcome To The Cash Club, Good Friend!

Beware of Netflix Phishing Scam!

Beware of this Netflix phishing scam that is currently affecting many individuals. Criminals have found a way to send notifications to some of the streaming service's account holders asking them to reveal personal information.

The scam is very sophisticated and states that the company is having trouble authorizing your credit card, then asks you to click on a link within the email to enter your payment information again or use a different payment. If you click on the link you will be taken to a fake site, and asked to enter your credit card information. If you enter this information the cyber criminal will be able to access your bank account.

How should you know if it is fake? The real Netflix never asks subscribers to enter their billing and payment information from an email. Instead they require that the information is filled out via their website or app itself.

OnPar

Recent Ransomware Attacks
The Cyber Attacks You and Your Employees Need to be Aware of

In early May a major ransomware attack known as WannaCry spread acorss 150 countries and began taking over user files and demanding $300 to restore access. In late June another form of Ransomware known as Petrwrap infected airlines, banks, and utilities across Europe causing many to close. Both viruses encrypt users computers and files, rendering them unusable, and then demanding a bitcoin payout for decrypting the files. If you have been attacked:

- DO NOT pay the ransom demanded by the cyber criminals. There is no evidence of hackers giving people their files back

- For individuals - you should contact your local IT Support services

- Restore all backups

How OnPar ensures safety for our customers: OnPar utilizes various technologies for our customers to ensure safety from these potential threats. These technologies include- Automated Patch Management, Bitdefender, and SonicWall. OnPar Technologies is also a Datto Partner. Datto protects essential business data for tens of thousands of the world's fastest growing companies, delivering uninterrupted access to data on site, in transit, and in the cloud. In addition, OnPar offers current customers various solutions against ransomware that include: protecting all data with a backup solution, providing anti-virus/anti-malware and spam filtering, removing local admin access from PC's, integrating PC's with O365 active directory, enabling two-factor authentication sign on, and much more.

To prevent a ransomware attack on your business, make sure all anti-virus is up to date, back up all copies of your data, scrutinize links and files in emails, and only download software from trusted sources.

If you are interested in adopting other solutions to ensure your data is protected, contact OnPar Technologies at 919-926-9619

Enjoy 10% Off Managed Services and Office 365 Applications Through December 31, 2017

We're celebrating our 10th Year Anniversary all throughout 2017! So we want to give you 10% off managed service contracts and Office 365 throughout the year!

Simply go to: www.onpartech.com/10-percent-off-promo and fill out the form or call us at: 919-926-9619

This offer is only valid for new customers with 10 PC's or more. Must sign a 1 year contract to receive the full discount.