MAY 2022 | VOL. 8

THE ACCOUNTING NOTE

OFFICIAL COMPANY NEWSLETTER OF
PLUS 1 TECHNOLOGY

INSIDE THIS MONTH'S ISSUE:

HOW REPLACING YOUR PC CAN SAVE YOU 3 DAYS OF DOWNTIME - 1

WHAT IS BEC AND WHY SHOULD I BE WORRIED- 3

The technology newsletter for Accountants

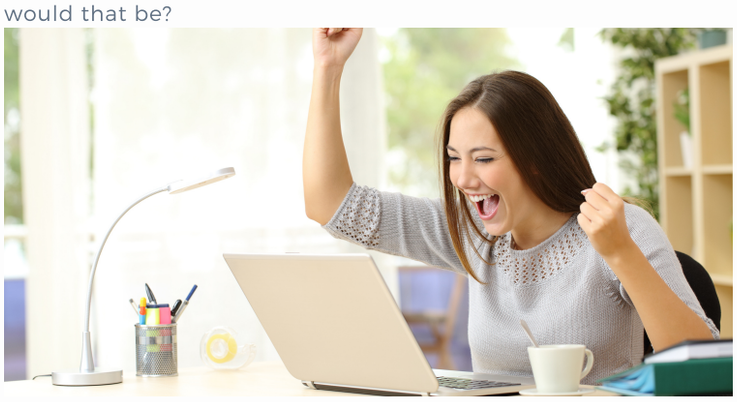
This monthly publication is provided courtesy of Marc Umstead, President of Plus 1 Technology.

Our Mission:
Plus 1 aims to help empower accounting firms with tools that boost productivity, efficiency, and reliability. Our goal is to take the stress out of IT through innovative solutions and services.

How replacing your PC can save you 3 days of downtime

WRITTEN BY MARC UMSTEAD

We have all been through the process of getting new equipment. Many cringe at the thought of replacing their work desktop or laptop. Installing software, arranging desktop icons, and customizing your browser are all things most of us don't even want to think about. How would you like to be doing all of that during the most stressful time of the year? What if your computer crashes on April 10th, 12th, or 14th? How terrible would that be?



We recommend that our customers replace equipment every five years. It isn't because on it's 5th birthday it stops working or you are at anymore of a security risk than 2 days before it turned 5, but as a risk mitigation step. The truth is computers, much like us, age with time. They get slower, have new aches and pains, and start to break down. MSPs are essentially your technology risk mitigator. It is our job to lower, mitigate, and eliminate as many risks as possible. We recommend replacing computers around the 5 year mark because they have a much higher rate of failure when they get much older than that. The last thing we would want would be for a client of ours, especially during a busy time, is to have to replace their computer in a rush. Replacing/upgrading computers can already be a shock even with the best planning and it is much harder when done in a hurry because speed takes precedent over process.

When your MSP provides you a replacement schedule during a meeting (and they should be) we suggest that you make every attempt to adhere to the schedule. Replacing your computer in June or July is a much better idea than trying to do it in the throws of tax season. Replacing computers under a schedule also gives plenty of time for the replacement to be executed properly, ensuring there is less work you have to do when the new computer is installed and you can schedule your work accordingly.

After Tax Season Technology Checklist

WRITTEN BY MARC UMSTEAD

After Tax Season Technology Checklist:

1. **Review hardware replacement schedule and schedule replacements**

Your IT provider should be providing you with a list of all your equipment with a 5 year replacement schedule and budget. Review this plan and schedule this year's replacements.

2. Schedule any application updates (QuickBooks, Sage, and etc.)

Do you need to update your QuickBooks, Sage or other applications or install the new versions?

3. Review tax season technology frustrations and address

What were the company's biggest technology issues during tax season and how should they be addressed

4. Any software replacement or needs?

Are you looking to switch Tax prep software, add a CRM, add a file upload portal or online scheduling?

5. Any infrastructure changes?

Need to add better WIFI? Enable more robust work from home technologies?

"Plus 1 Technology has the specialized knowledge required to keep our infrastructure running so we can run our business. Our past providers were not as responsive to our support concerns. Plus 1 Technology provides quick resolutions. Plus 1 has the personal feel of a small business but the responsiveness of a large firm. "
- Patrick McDonnell, Partner, WSM Law

Account Monitoring

Does someone already have access to your e-mail account?

Does someone already have access to your email account? If you answered no, are you sure? We have seen an increase in complex BEC (Business E-mail Compromise) attacks. Often these malicious actors have access to the account for days, weeks or even months before they do anything to tip off the user. These type of attacks is why we use a SOC (Security Operations Center) to constantly monitor all e-mail account activities such as logins, email rules, and ip addresses accounts are accessed from. This helps us ensure the only people accessing the account are the rightful owners.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.
After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide
a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, visit www.IT4MyBusiness.com/csra

What is BEC and why should I be worried?

WRITTEN BY MARC UMSTEAD

What is BEC? BEC is a Business Email Compromise. This basically means that a malicious actor (MA) has gained access to an email account. These attacks are typically the result of a credential being leaked on the dark web or a user falling for a phishing email and providing their credentials. In years past these attacks were easy to spot. A malicious actor would gain access to an account and spam everyone in that users account. Today's attacks are becoming much more complex. Now when a malicious actor gains access to an account they quite often, do nothing. They will monitor emails and content in the account and wait till an opportune moment to perpetuate a scam. This may be creating an email address for a contact that would be a single letter off. So, if a user is working on a real estate transaction and working with robert@bobstitleservice.com the bad actor will create an email robert@bobtitleservice.com. The MA will copy Robert's signature and at the same time create a rule on the user's mailbox to redirect mail coming from the real Robert to the junk mail folder so the user can only see emails coming from the fake Robert. I have seen many users fall for these types of attacks and lose large sums of money.

4 ways to Protect from BEC

How can you protect your company?
Here are four ways we recommend you protect your company from these types of attacks:

Training

Providing cyber security awareness training to your employees is a great way to stop these types of attacks. Users will be better able to spot phishing emails and avoid giving away their credentials

E-mail Protection Tools

There are many products available to assist users with being able to spot phishing and impersonation attempts. We use a protection suite from Barracuda that lets users know if the person is a "first time sender" or an "external sender". These classifications can help users spot impersonation attempts.

Proper policies and procedures

Employees should have clear instructions on how to verify senders for financial transactions. We recommend that every company build some "analog" verification into any workflow involving financial transactions. The best method is using a phone call to the number on file to verify any changes in financial instructions.

Account Login Monitoring

Do you know if a malicious actor has access to one of your accounts right now? Using a monitoring service typically provided by a "SOC" (Security Operations Center) is a great tool to verify that every login to your accounts is from a verified location. These services can spot anomalies in login activity and lock down accounts before a compromise can take place.

Business E-mail Compromise (BEC) attacks are quickly becoming one of the largest threats to a company's cyber security. We recommend all companies take the steps above to minimize this risk.

Using a Secure File portal?

The "offseason" is a great time to drive adoption for your secure file portal. We recommend holding a lunch and learn or webinar to train your clients on how to use your web portals to upload their documentation and pull down their prepared documents.

If you use an online schedule tool, this is also a great time to teach your clients how to use this tool. The of your technology your clients adopt the more productive and efficient your company will run. You have to make the investment in educating your clients to ensure they are comfortable with the tools you provide.

PLUS ONE TECHNOLOGY

Splice data easily

Slicing allows you to filter data easily.
To do so, select any range in a table or PivotTable and then go to Insert > “Slicer,” in the top right corner. Then, select the column you want to filter by.

HAPPY HOUR

BROWN DERBY

That trio of simple ingredients belies the complex taste of the drink, as the honey bridges the gap between the tart citrus and the spicy bourbon to produce an intricate combination that has stood the test of time.

- **1 1/2 oz, bourbon**
- **1 ounce grapefruit juice**
- **1/2 ounce honey syrup**
- **Grapefruit Twist**

- **Add the bourbon, grapefruit juice and honey syrup into a shaker with ice and shake until well-chilled.**
- **Fine-strain into a cocktail glass.**
- **Express the oil from a grapefruit twist over the drink and drop the twist into the drink to garnish.**

PLUS ONE TECHNOLOGY

3277 W Ridge Pike Suite B201
Pottstown PA 19464

Inside This Issue

How Replacing your PC can save you 3 days of downtime - 1

After Tax Season Technology Checklist - 2

What is BEC and why should i be worried- - 3

Tips & Tricks - 4