Issue 43

August 2014

Page 1 of 2

M&H CONSULTING

THE M&H MONITOR

Getting the Most From Your "Tech For A Day" Visits

Scott McDonald

At M&H Consulting, we offer a program called "Tech For a Day," which the majority of our clients take advantage of already. On our Tech For a Day (TFaD) program, M&H clients get regularly scheduled maintenance visits with our technicians, at a discounted rate, where we perform important maintenance on their systems. The system maintenance we provide helps to prevent unnecessary costs & downtime, while optimizing system performance.

Your organization is already on our TFaD program? That's great! But how can you be sure you are getting the most possible value for your money? We wanted to help our clients in this regard, so we decided to put together this simple, easy-to-follow list of things you can do to help get the most 'bang for your buck' from TFaD.

Have an "IT To Do" list ready. One of the great advantages of our TFaD program is that we can also do additional troubleshooting or setup work during TFaD visits after performing maintenance, still at the reduced rates. It can be very helpful to have one person in charge of maintaining the "IT To Do" list, so that our technicians have an organized, prioritized list at the beginning of the day. This can save time during the visit, and can also help to make sure we work on the most crucial items first.

Plan for the maintenance time. Our technicians are very good at minimizing downtime for users during maintenance; however, there will inevitably be a small amount of time when users cannot work due to the server being rebooted, or their particular workstation receiving maintenance. It is best to have users plan for this, and inform the technician if there is a desired time for reboots. This will help to minimize work interruption, and can also help our technicians to work more efficiently for you.

Leave your computers on the night before. Our technicians will schedule some automated maintenance tasks to run on your PC's every night during overnight hours. While not all maintenance tasks can be automated, having these run automatically the night before a visit can save some time during the visit. It can also be helpful to restart computers the night before we visit, if they have been running for more than 24 hours.

Allow your technician to work on multiple machines at a time. While it may take 30 to 45 minutes or more for maintenance to be completed on a workstation, there is generally only about 20 - 25 minutes of actual work to do. The rest of the time involves waiting for updates to install and scans/cleanup utilities to finish. Why not let your technician work on 2 or 3 machines at a time to maximize efficiency? Our technicians will always try to do this, but when a lot of restrictions are placed on the timing for maintaining machines, efficiency is reduced. Try to minimize these restrictions as much as possible, and inform the technician of them as early in the day as possible.

Make time to talk with your technician. Did you know that your M&H technician is not only a great computer tech, but also a great consultant? Our technicians can provide you with a wealth of relevant knowledge about technology to help you make informed decisions about how to spend your budget, what systems to replace/upgrade, and how to avoid problems in the future. Make use of that resource! We recommend setting aside at least 10 minutes during each visit to meet with us and review your plans and questions.

If you have any questions about our Tech For a Day program, please contact us at **866-9MH-TECH** or **support@mhconsults.com**.

TECH TIPS: Securing Your Smartphone

These days, employees are more mobile than ever. One of the ways that employees and business owners stay connected when away from the office is by setting up smartphones and tablet devices to access email and other company resources. This can be an incredibly convenient and helpful business tool, but it can also present security dangers.

Here are some tips from M&H and Sophos on things that you can do to help protect your confidential and proprietary information from being compromised on a mobile device:

- **Always secure access to your device.** A 4-digit PIN or swipe pattern is better than nothing, but not nearly as good as a complex passcode (a PIN is far more susceptible to guessing, and finger-trails left on your screen might reveal your swipe pattern).
- **Check that your device locks automatically.** It is recommended to set your device to lock automatically after 5 minutes or less.
- **Install security software on your phone**, such as Sophos Mobile Security (free). Security software can help protect your device against viruses and malware, and also provide easy ways to remotely lock or wipe your device if it is lost or stolen.
- **Be wary of open/public wifi networks.** When you connect to an open wifi network, such as those you find in cafes and restaurants, your device becomes searchable on the network and potentially open to hackers. Be careful what data you transmit on open networks. If your company has a VPN, using your VPN connection over the public network dramatically reduces the risk.
- **Limit access to only what is required.** For example, if your company has a VPN but a particular user's job doesn't require VPN access from their mobile device, don't set it up unnecessarily. Give their device email access only, or whatever access they actually need to do their job, and not more.
- **Do not save passwords in applications where it isn't required.** For example, a VPN or Remote Desktop app might present the option to save your password into a saved connection. Don't do this! The security benefits of requiring manual password entry far outweigh the inconvenience of 5 seconds spent entering a password.

Issue 43

August 2014

Page 2 of 2

THE M&H MONITOR

M&H CONSULTING

Securing Your Data Before Discarding Your Devices

Justin Bowden

One inconvenience that all users inevitably face occurs when their favorite piece of technology reaches the end of its lifespan. Most users will take the initiative and replace the device before it completely fails, but then are left with the decision of "What to do with the old one?" Laptops and desktops can be brought to a recycling center, while smartphones and tablets are usually either recycled or traded in for an upgrade. Whatever the decision, one factor should not be overlooked: What will happen to the data on your device?

Identity theft is one of the fastest-growing areas of crime, and can negatively affect an individual for

years. For businesses, the effects of compromised data can be even more serious. Data stored on computers and mobile devices can include business information such as email accounts, network passwords, and client data; as well as personal information such as phone number, address, and photos. The good news is that there are steps that you can take to ensure that your data is secure when it is time to part with your electronic device.

In laptops and desktops, all data is stored on an internal hard drive. Before discarding a PC, you should remove all of this data, and there are different options for this. There is software that can be used to erase all of the data on a drive, but this may not be completely effective. There are devices and services that will magnetically remove all data from a hard drive, but these can be very costly. The most effective method is always to simply destroy the hard drive. There are many guides and videos available online for this, and this is also a service that M&H can provide for you. Once the internal components of a hard drive have been destroyed, you can be confident that the data is no longer accessible.

For smartphones and tablets, destruction is often not a desirable option because most users prefer to sell, trade in, or recycle them. While these options make sense economically, there is always a risk in turning over your device. Most smartphones and tablets have options that allow you to reset the device and wipe your data, but these may not all be 100% effective. A recent case study performed on discarded

mobile devices found large amounts of data that had been unintentionally left behind by their owners. It is recommended to run the device's data wipe function multiple times, and also to remove or manually delete the contents of SIM cards or any add-on storage cards. Ultimately, the most effective way to keep your data secure is to keep or destroy the device, but if you do decide to give up your device, be sure to take proper safety precautions first.

If you have questions about what to do with your old devices, or need assistance in securing your data, contact us at any time at **866-9MH-TECH** or email us at **support@mhconsults.com.**

TAKE $$$CASH$$$ FROM M&H CONSULTING

Refer a new Tech-For-A-Day client to M&H Consulting and mention this offer to us, and you will receive $25 for each PC the new client has. Call for details.

"The computer says I need to upgrade my brain to be compatible with the new software."