E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

October 2018

In this issue...

Simple tips to increase cloud affordability

Moving to the cloud can save you a considerable amount of money, which explains its rise in popularity over the years. What many business owners fail to realize is that some cloud services come with hidden costs. And while they might seem insignificant at first, they can add up to a staggering amount if left unchecked. Minimize your cloud expenditures with these five tips:

No standalones

Cloud services come in various shapes and sizes, many of which are standalone platforms with rates that increase over time. Opt for a service provider that offers a suite of products that all work together. They are often less expensive than a group of standalone products. Another benefit of working with a cloud provider is that you receive a single point of contact to resolve your issues quickly and effectively.

Experience matters

If you plan on integrating a standalone cloud service into your system, make sure you hire an experienced integration consultant to facilitate a smooth transition. Integration mishaps can cause serious downtime and cost a lot of money.

Backups are important

Unnecessary or inefficient backups will waste cloud storage space. Examine your cloud storage data by asking the following questions:

- How many versions of this data do I need to store long-term? The more versions you store, the more it costs.
- What regulatory demands do I need to meet? Some data may need to be accessible for up to three years, whereas other data can be deleted after 30 days.
- How quickly do I need to access my backups? If it can wait for a day or two, archive that data to a less expensive service or offline at the provider's data center.

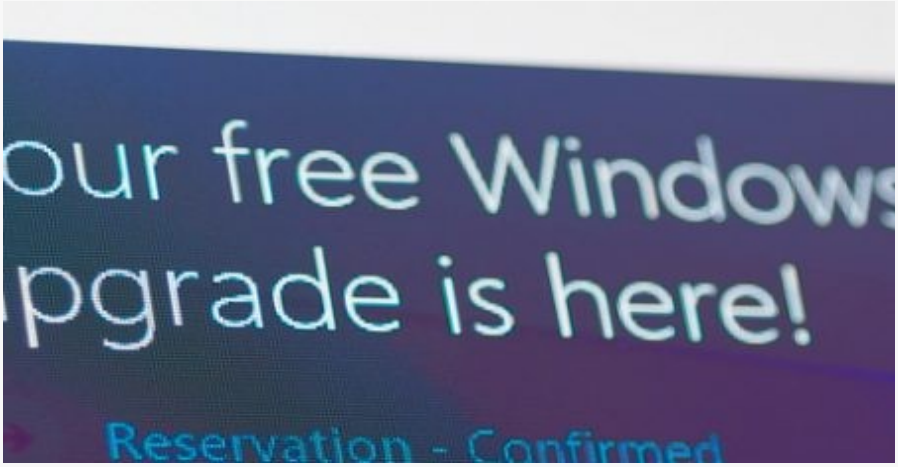
Remove users

Many cloud service providers charge by the number of users in your system. By neglecting to manage the list of users, you could end up paying for people who no longer work for you. Implement processes that remove users when they are terminated and consider scheduling a regular audit. Ideally, this should be once every six months to a year, to ensure your cloud user list is up-to-date.

Monitor proactively

Ask your cloud provider whether they can proactively monitor your account and notify you of potential issues before they cause problems. This is especially important if you have a pay-as-you-go license that charges based on resource or storage consumption.

Utilizing the right technology resources is vital to your business's success, and so is knowing how to prevent them from racking up an overwhelming monthly bill. If you wish to enjoy all the benefits of cloud computing without breaking the bank, give us a call and we'll be happy to help.



Fix these five problems in Windows 10 now

Although Windows 10 is packed with wonderful new features, it's far from perfect. Users have complained about storage, connectivity, and update issues, among other things. If you've encountered any of these issues, no need to panic. We have listed down five simple fixes to the most common Windows 10 problems.

1. Less storage space

When you upgrade to Windows 10, your old software is not actually deleted but stored in your hard drive as "windows.old". While this is a smart move that allows users to downgrade their software if they want, it also consumes a lot of space that you can use to store more important files.

If you want to delete this previous version to free your storage space, first type "cleanup" on the Windows search bar to pull up the Disk Cleanup app. From there, you can either click on *OK* right away, or you can choose *Clean up system files* to ask Windows to scan your system. Either of these options will open a pop-up box that will ask whether you would like to delete previous Windows installations.Then, select the files you want to delete and click *OK*.

2. System Restore isn't enabled

In Windows 10, System Restore isn't enabled by default. To turn it on, go to the Start Menu and type "Create a restore point." Next, choose the system drive and click the *Configure* button, then select *Turn on system protection*. Use the slider to set an appropriate amount of maximum disk space to be used for restoring the system (about 5 GB should be enough).

3. Updates won't work

First off, check if you've upgraded to the most recent stable update. Users should hold off on installing the Fall 2018 update until issues are resolved. If your updates still don't work, download and run Windows Update Troubleshooter and try to update again.

4. Privacy violations

Windows 10 faces a lot of criticism over data privacy settings. We recommend you review them from time to time, especially after every update is released. To change the privacy settings, go to *Start Menu* > *Settings* > *Privacy*. On the left-hand side, you'll see a list of features and data Windows has access to that you can disable, including the computer's camera, microphone, account information, and so on. Turn off the ones that you don't want Windows to have access to.

If you use Windows Defender, go to *Update & Security*, and decide whether you want to enable cloud-based detection and automatic sample submission, which uploads suspicious files to Microsoft Servers for analysis.

5. Windows 10 uses up all the 4G data

Windows 10 allows you to connect to the internet via cellular data, just in case the Wi-Fi is slow or unavailable. However, it can use up all your data if you're not careful. To avoid this, go to *Settings* > *Network & Internet* > *Data Usage*. Select *Cellular Data* from connection options, and then click on *Set Limit* where you can adjust how much data your computer uses.

Break a Hacker's Heart

Our security experts are ready to teach you how to Break a Hacker's Heart in 2018 and beyond.

Join E-Safe Technologies and Sophos **Tuesday, December 4th at 11:30 a.m. for this free event.**

Learn how to ruin a hacker's day by leveraging the power of deep learning and more to fight the most dangerous threats aimed at your network. Plus, we will arm you with the latest cybersecurity news and practical methods to fight targeted, coordinated attacks.

Fogo de Chão Pittsburgh
525 Smithfield Street,
Pittsburgh, PA 15222, USA

REGISTER HERE

BE SURE TO SIGN UP TODAY!

4 types of hackers that may target SMBs

When it comes to cyberattacks, most business owners get hung up on the technical and logistical details, forgetting another important aspect: motive. Why are hackers attacking people and organizations? And whom are they targeting? By answering these questions, you'll have a better understanding of which of your business's resources need the most protection.

Script Kiddies

Skill-wise, script kiddies (or skids, for short) are at the bottom of the hacker totem pole. Their name comes from the fact that they use scripts or other automated tools written by others. Most of the time, script kiddies are young people on a quest for internet notoriety. Or, more often than not, they're simply bored and in search of a thrill. Many never become full-time hackers; in fact, many script kiddies end up using their skills for the greater good, working in the security industry.

Though lacking in hacking know-how, script kiddies shouldn't be dismissed so easily, as they can cause businesses much damage. In May 2000, for instance, a couple of skids sent out an email with the subject line "ILOVEYOU" and ended up causing a reported $10 billion in lost productivity and digital damage.

Hacktivists

Hacktivists are primarily politically motivated, and they often hack into businesses and government systems to promote a particular political agenda or to effect social change. These so-called "hackers with a cause" steal confidential information to expose or simply disrupt their target's operations.

If you're a small- or medium-sized (SMB) owner, don't think for a second that you're immune to hacktivist attacks. This is especially true if your company is associated or partnered with organizations that are prime hacktivist targets. Or, if your business provides services that can be seen as unethical, you may targeted by hacktivists as well.

Cybercriminals

When a hacker breaks into digital systems or networks with malicious intent, they are considered a cybercriminal. Cybercriminals target everyone from individuals to SMBs to large enterprises and banks that either have a very valuable resource to steal or security that is easy to exploit, or a combination of both.

They can attack in a number of ways, including using social engineering to trick users into volunteering sensitive personal or company data, which they can then sell in underground markets in the dark web. They can also infect computers with ransomware and other malware, or use digital technology to carry out "conventional crimes" like fraud and illegal gambling.

Insiders

Perhaps the scariest type of hacker is the one that lurks within your own organization. An insider can be anyone from current and former employees to contractors to business associates. Oftentimes their mission is payback: to right a wrong they believe a company has done them, they'll steal sensitive documents or try to disrupt the organization somehow. Edward Snowden is a prime example of an insider who hacked his own organization — the US government.