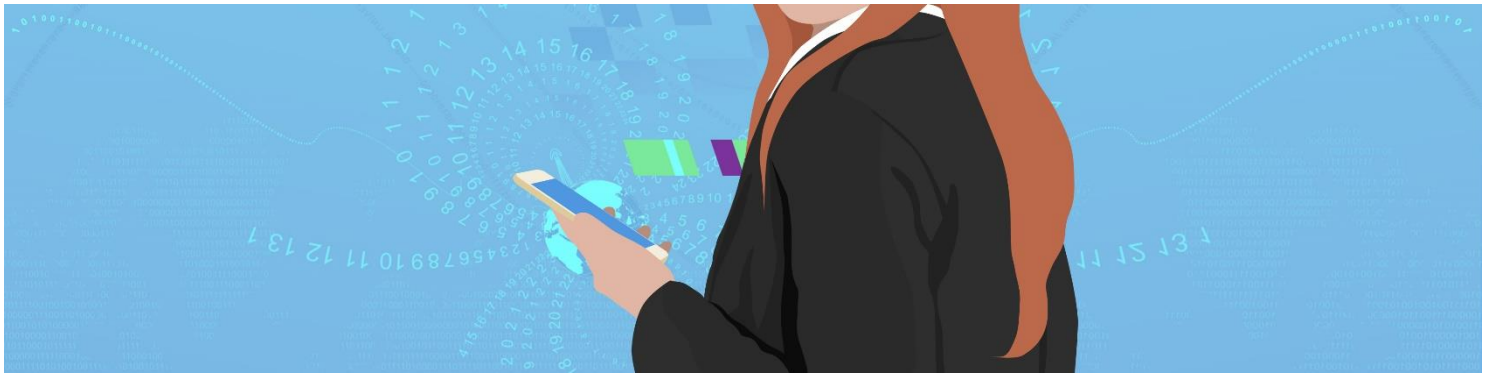
November 2018
http://www.ctsioutsourcing.com
229-446-9641

NEWSLETTER



Business Tools to Take Your Business Out of The Office

Being engaged in business used to mean staying wired in at the office eight to twelve hours a day. In the modern day, this is completely untrue. Often the most efficient workplace is spread far and wide and always on the go.

Today you can completely unplug from your desk with just your laptop computer and 4G modem. The freedom to work out of the office and even on the move is a huge advantage gifted to modern business. A simple mobile phone tether is enough to work from anywhere in the world.

The Right Tools for the Job

The most important part of working on the go is ensuring you don't lose touch with your team. Maintaining total collaboration between team members can be tricky. Luckily, there are tools that will help you to stay on top.

Microsoft Office 365 provides the traditional tools and support of Microsoft office, but adds remote team collaboration and cloud support too. Files can be saved into the cloud, worked on, and accessed anywhere for review. At one time, remote working meant taking a copy of a file somewhere else to work. Changes to the original weren't reflected in the remote copy and at least one version was destined to be lost forever.

Software packages such as OneDrive allow the entire team to work on a single centralized file saved to the cloud. Whether you edit on a beach, plane, or train; your team in the office gets the same version you do, at the same time.

Collaborative Working

The key to remote working is the ability to collaborate in a digital space with everyone at once. Modern software such as Office 365 allows all team members to be working on a single document at the same time.

Whether the project calls for killer spreadsheets, expertly crafted documentation, or a knockout presentation; everyone can pull together and hit it out of the park.

Even when you're not working out of the office or busy on the road, collaborative software can help to power your team working locally too.

Admin Done Remotely

Modern software has impacted the way in which we do bookkeeping and accounts too.

Similar to being tied to your desk in years gone past; accounting software was once stuck solidly in the desktop too. Previously, batch runs of calculations were required to provide reports on a weekly, bi-weekly, or monthly basis. Today, cloud computing has opened up ways to speed up business in ways we couldn't have imagined.

Cloud-based accounting packages such as Xero or Quickbooks Online allow for your accounts to be done remotely. Moving the resource and strain out of your firm takes it out of sight and out of mind.

Security and maintenance of your accounts databases, for example, falls to cloud professionals instead of your business. Rather than waste company time on submitting documents and calculating taxes they are done in the cloud and submitted to you instead.

Make your Accounts Work for You

Maintaining your accounts is made as simple as logging into a single portal. This tool allows you to take both your admin and your work out of the office and keep it on the go.

By the time your accounts are due, your accountant simply has to log in remotely and pick up where you left off. By the time taxes are due the work is done, and you can get on with the important things.

Getting work done out of the office and on the go is a huge boost to productivity. Modern technology enables you to keep team members up to speed, continue collaborating, and even stay on top of your accounts from anywhere in the world.

Give us a call today at 229-446-9641 to talk about how we can help you unwire from the office.

It is important to first distinguish the type of dangerous employee we want to defend against.

Protecting A Business from Internal Threats

When considering IT threats to your business many articles focus on hackers, viruses, and attacks from external threats. These dangers are real, constant, and easily identifiable. In many cases, however, the largest threat to a firm comes from inside the business itself.

People inside the firm often pose the largest single threat to systems and security. These individuals often have trusted access and a detailed working knowledge of the organization from the inside. Employees therefore deserve the largest security consideration when designing a safe business system.

It is important to first distinguish the type of dangerous employee we want to defend against. We're not talking about an otherwise model employee accidentally opening a malicious email or attachment. Rather, a disgruntled employee seeking to do damage to your business. An employee who may wish to destroy services or steal clients and files from your firm.

Security Policy

Some firms, particularly young businesses, grant employees' system-wide permissions from day one. This can make administration appear simple, preventing further IT requests in future. Granting system-wide access is an inherently risky strategy.

Private information relating to the business should be restricted access information. Many types of files need to remain confidential, often as a legal requirement. Human resource files, salary information, and employee documents should be limited to only a select few employees. Yet, businesses often keep confidential information in public places on the network.

Granting system-wide read and write access can appear to save time short term. It is, however, a security policy which only serves to cause security, administration, and potentially legal troubles in the future.

The Principle of Least Privilege

The principle of least privilege is a vital tool, helping you to handle internal IT security. It defines a security policy which ensures staff can access only the resources, systems and data they require to carry out their job.

The policy protects the business from many different types of threat in day-to-day operations. Even where malicious attachments have been opened by accident, the damage is limited only to the work area of a single employee. This results in contained damage, less time needed to restore from backup, and drastically reduced downtime for the firm.

Along with limiting accidental damage, malicious employees looking to destroy or steal data are limited too. With restricted access, an employee with a grudge or profit motivation can only damage or steal from their own area of operation. This helps to ensure that no single employee can damage the entire firm's operations.

Security Policy in Practice

A member of staff within Human Resources, for example, may have read and write access to the employee database. This will likely include payroll information and sensitive data. This same member of staff would have no need to access sensitive client data, such as sales information, in normal working conditions.

Likewise, a staff member from the sales department should have no need for accessing sensitive HR records.

Using the principle of least privilege, each employee may only have full access to systems that are directly related to their role. Similarly, some systems may be visible to a wider group of staff members even if they can only be edited or removed by one or two people.

In some cases, a security policy may be defined by even finer details than a person's role within the organization. An HR employee should not be able to edit their own file to change salary information for example. An employee file might only be edited by their superiors in such a case.

Additional parameters can be used to assign privileges to enable the business hierarchy to work within the IT network. Seniority, physical location, and time are all examples of factors that can restrict access to critical systems and secure data.

We can tailor your network to your business, locking down your data to ensure data is only accessed on an "as needed" basis. Call us at 229-446-9641 now.

Increase Your Productivity with Dual Monitors

"While most tasks can be tackled feasibly with a single monitor; two makes the same tasks faster"

Conventional wisdom states that cluttered workspaces lead to a disorganized mind. Mess prevents productivity and begins to hamper professionalism. Shouldn't that apply to the computer desktop too?

The simplest way to clean and organize your digital desktop is to add more space. Just adding a second screen doubles the available room and makes organization a breeze.

Getting work done with a single-monitor setup is a balance of poor compromises. There never seems to be enough space and the little space available is full of clutter and mess. Switching between windows or tabs wastes time and distracts from work to be done. Stacking windows together, side-by-side, or top and bottom wastes valuable screen real estate. The resulting clutter of windows makes it hard to focus on what is important.

While most tasks can be tackled feasibly with a single monitor; two makes the same tasks faster, simpler, and much more enjoyable.

Two Monitors, Many Uses

Data entry with two monitors is far easier than data entry with one. Having source data on one screen, laid out in large type, and the destination on another makes the job a breeze. By eliminating the need to scroll tiny windows or switch tabs, forget and repeat; the same job can be done in a fraction of the time.

Graphic design, image manipulation, and editing are key areas that make the most of a dual screen setup.

Stacking one image on each screen allows you to make quick comparisons to make sure your work is going in the right direction. Organizing your editing space is made simple too. Stacking your tools, menus, and options on one monitor with your image maximized on the other helps to stay focused and finish the task.

Beyond Just Two

Having more than a single screen helps you to track tasks you need to keep on the back burner. A team chat window to keep on top of collaboration, status updates for business-critical services, or the latest stock price. These windows and dialogues can remain open and serving updates on a secondary screen while you keep your work focused on your first.

It is not uncommon for stock traders or financial analysts to maintain 6 or more screens running from a single computer. Many uses this to track various stocks or indices so they don't miss a beat.

Setup How You Like It

Multiple monitors can be arranged in almost any practical configuration imaginable. While traditionally positioned in landscape orientation, second, third, or fourth monitors are often rotated 90 degrees to portrait orientation.

This setup is used often by software engineers, editors, and users reviewing large amounts of text. The lengthwise orientation allows multiple pages to be read from the screen at any one time.

Multi-screen setups, no matter how they are arranged, behave the same as if all the monitors were just a single screen. Mouse input moves from one monitor to another as if there was no difference between them. From the user's perspective, there is no difference to how they interact at all.

A Boost to Productivity

There is a scientific advantage to multi-monitor setups too. A survey by Jon Peddie research found that adding an extra monitor boosted a user's output by as much as 20 to 30 percent.

A productivity advantage of even 10 percent is prized and very hard to come by in the business world. Receiving a productivity reward of over 20 percent for just the cost of adding a second monitor is something few firms can afford to pass up.

The satisfaction of de-cluttering your digital desktop and keeping your focus in the zone is worth it alone.

Give us a call at 229-446-9641 if you would like us to boost your setup by adding a second monitor.

Celebrating 20 years

Protect Your Firm Against Zero-Day Attacks

Protecting your business against the latest IT threats should always be a top priority. Updating antivirus and patching your operating system is a great way to start. What happens, however, when a threat appears at your door before security firms have had a chance to catch it?

A security threat that exploits a previously undiscovered vulnerability in the computer is known as a zero-day threat. The name "zero-day" is designed to imply how long since the vulnerability was discovered. The term also indicates that system developers have had zero days to fix it.

A newly discovered attack might be packaged into a computer virus or worm. This will allow it to spread far and wide while inflicting the maximum amount of damage possible. When spread successfully, a new exploit has the potential to reach hundreds of thousands of computers before an operating system or anti-virus update can even be issued.

There are a number of ways we can protect your business or lessen the damage from a zero-day attack.

Preventative security

The number one way to mitigate the damage from any attack to your system is to prevent it from happening in the first place. Maintaining a good firewall and up-to-date antivirus is the best step you can take to ensure the security of your system.

A firewall, monitoring traffic in and out of your network, reduces unauthorized entry over the network. Even without knowing the exact nature of the attack, suspicious activity travelling in and out of the system can be stopped.

The same is true of modern Antivirus. Even when it cannot identify the specific zero-day threat from its virus database; it can often identify malicious intent from learned behavior in the system.

A Locked Down Network

Should a zero-day threat make it into your network, our next goal should be to limit its effects. By restricting user access to only essential files and systems we can limit the damage done to the smallest number of systems. Good security policy dictates that each account should only have full access to the systems needed to complete the user's job. For example, users from the accounts department shouldn't have access to sales department databases.

In this way, the damage of a single compromised account is limited to only the network area it operates in. Such limited impact should be easy to control and can be reversed with regular backups.

Good Data backup

Whether your entire network has been exploited or only a small area has been affected; good data backups are your protection against major lasting damage. Having a good backup means having the procedures in place to both create regular backup copies and make sure they can be restored at a later date.

Reliable and well-tested backups are worth their weight in gold. Knowing your data is safe and your system can be recovered is peace of mind against even the most highly destructive zero-day attacks.

Intrusion Protection

While the precise methods of a zero-day exploit can't be known in advance, a network intrusion protection system (NIPS) can monitor the firms' network for unusual activity.

The advantage of NIPS over a traditional antivirus only system is it does not rely on checking software against a known database of threats. This means it does not need updates or patches to learn about the latest attacks. NIPS works by monitoring the day-to-day patterns of network activity across the network.

When traffic or events far out of the ordinary are detected action can be taken to alert system administrators and lock down the firewall. Devices such as USB drives and mobile devices can all introduce threats to the network. They can often make it past the firewall because they are physically introduced to the system.

Comnet Technical Solutions, Inc.
CTSI
CTSIoutsourcing.com
229-446-9641

235 Cedric Street
Leesburg, GA 31763

HOURS OPEN
Monday to Friday
8:30am - 5:00pm

CTSI Facebook

NIPS protects against threats introduced to the network from both external and internal sources.

Full Cover Protection

Used in combination these techniques can prevent, protect, and mitigate against the kinds of threats that even the top security firms haven't patched yet. We think it's important to keep your firm secure whatever it might come up against in the future.

If you could use help protect your business against online threats, give us a call today at 229-446-9641.