August 2017

TechTidbit.com

brought to you by Tech Experts

Improve Your Staff's Productivity Using These Five Tips

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Increasing employee productivity is a positive approach for companies, regardless of the industry; however, the concept can be rather vague.

Productivity means more than just working to meet a given quality standard, therefore, it isn't always immediately clear how to achieve optimum outcomes while maintaining standards and keeping your employees happy.

Here are a few concrete methods that can help your staff be more productive:

Block Certain Internet Sites

With the rise of social media, online gaming, and entertainment websites, there are many potential distractions on the web. Even if an employee is well-intentioned, there are plenty of well-designed trappings to keep them there, wasting your company's time, Internet bandwidth, and, ultimately, money.

Consider placing a block on potentially productivity sapping sites to remove the temptation to linger online.

Try Mobile App Blocking

Just as employees can get distracted while on computers, they can also waste time piddling away with apps on their smartphones.

While there is no way to completely solve this problem, you can at least block the use of certain applications when connected to the corporate network with technology such as firewalls.

Revamp Technology

It isn't necessary to invest a fortune in buying new equipment to upgrade your IT infrastructure and increase your staff's productivity.

Get rid of any obsolete technology that just takes up space, update your software, and consider investing in one or two pieces of newer equipment that can benefit multiple staff members or perhaps the whole company.

Save Files on the Company's Server

Get rid of clutter on individual computers while promoting collaborations between members by using server-based storage. This frees up space on each computer station for optimum speed, and you can set permissions on files to share between certain staff members while restricting access to others.

Track Production

There is a wide array of tracking methods to measure how many tasks an employee undertakes during a work day, how long it takes to complete, and which client they worked on.

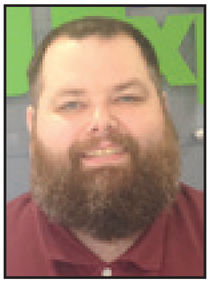
Many industries have developed tools and established best practices to manage and track production times and quality.

If you're having trouble finding the best tools to use for your business, give us a call and we'll work with you to find the solutions that will work for you.

With the rise of social media, online gaming, and entertainment websites, there are many potential distractions on the web. Even if an employee is well-intentioned, there are plenty of well-designed trappings to keep them there, wasting your company's time, Internet bandwidth, and, ultimately, money.

What Is Credential Management And Should I Have It?

> *"With Passportal, once you have your account set up – and have entered your websites, usernames, passwords, and passphrases – you will only need to remember one password to sign into anything. There is also an extension for one of the most popular web browsers."*



Ron Cochran is a Field Service Engineer at Tech Experts.

In the world today, we have many things to remember and passwords are one of those. We have alarm codes, website logins, usernames, passwords, passphrases, bank account information, and everything in between.

However, if you're on top of your password game, then none of your passwords match and that can be quite the chore to keep up on.

This brings me to a product called Passportal.

Passportal eliminates the need to remember all those different passwords, websites, and passphrases.

With Passportal, once you have your account set up – and have entered your websites, usernames, passwords, and passphrases – you will only need to remember one password to sign into anything. There is also an extension for one of the most popular web browsers.

Once you create your account with Passportal, you'll be able to enter your website of choice, username, and password; then, when you revisit that site, you will be notified that Passportal has saved your credentials for that site.

You'll click one button and Passportal will automatically enter your information in, then you're logged in to your favorite websites, social media, or message boards.

While it may sound like you're putting all of your eggs in one basket, Passportal's main focus is password security. The website, application, and process was created with military-grade password data security in mind while maintaining ease of use for the end user.

In the event of a mugging or break-in, you can lock your Passportal account and disable your usernames and passwords, instead of trying to remember everything you need to change. It's one less thing to worry about when recovering from identity theft.

Let's say your credit card and bank information have been compromised. Once you receive your new card and password, you revisit the website. Passportal remembers your password, but it doesn't work. You will be able to seamlessly add the new password to the Passportal extension with just a couple clicks and keystrokes.

Passportal has saved many users countless extra clicks, time, and hassle by keeping their valuable personal information secure.

If you are the owner of a company, you can utilize Passportal and have control over the passwords and when/if they expire.

If you have an employee that quits or is terminated, you can lock that username out of your company information with just ONE click of a button.

This feature saves valuable time that a human resource manager would have used to track down all the user information, gain access to their workstation or laptop, and remove their profile, or gain access to the server to remove their Active Directory profile.

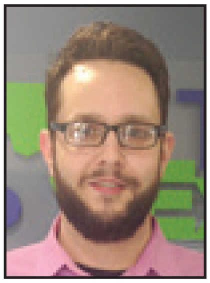
Passportal also has two-way syncing with Active Directory for Windows Server. With Passportal, there is even a mobile app and phone number you can text to get a password reset.

This feature will save employees who are locked out of their accounts – and allow your IT department to focus on more in-depth issues.

If you're the human resource manager, general manager, or owner of a company, your company will most likely be able to benefit.

Give us a call to find out how you can implement Passportal within your company.

Gone Phishing! How To Spot A Phishing Scam



Jason Cooley is a Network Technician at Tech Experts.

If you are a user that has been around for a while, there is a pretty good chance you've been targeted with a phishing scam. You may have a long lost relative in another country who left you millions – and all the executor of the estate needs is your banking information to send you your inheritance! Or a prince of a small country is trying to move some of his fortune and escape to America – and if you can help, you will be rewarded!

These are some oldies-but-goodies, however phishing scams have and will continue to get better and smarter. There was a time when phishing scams almost always came filled with poor grammar, spelling errors, and writing that just seemed a little off. While these still exist, things have become harder to detect.

These scammers are always looking for your personal information. There are a few ways they can do this, but most of them begin with email spoofing, where a sender will mask their actual email address with a familiar one.

If it isn't a spoofed email, it may come from an address that is very close to that of a known and trusted sender. This could have an extra letter or even just a period to try to trick you into completing whatever task they are using in an attempt to get your information. This could be something as simple as a link to "family photo" or video and it could very well open your system to different vulnerabilities.

Something like a keylogger, a program that tracks your keystrokes, can be almost undetected while also gathering your online banking or credit card information. Lately, phishers and scammers have pulled out all the stops. There have been cases where phishers will not only spoof an email, but also documents. These can look pretty real, so take a close look.

A new long-shot, big-payoff scam is to spoof an email address of a financial institution to try to intercept money from home purchases. This is done with forged documents and a fake email. While it's a long shot for something that big to happen, do big business in-person or through trusted secure communications.

What to watch for

When you have email communication from a known sender that doesn't quite add up (or doesn't sound like them), don't assume they're just having an off day. One example: if you know your family member shares all of their photos on Facebook, would they really email you a link with little to no writing in the email?

> *"When you have email communication from a known sender that doesn't quite add up (or doesn't sound like them), don't assume they're just having an off day. One example: if you know your family member shares all of their photos on Facebook, would they really email you a link with little to no writing in the email?"*

Any "company" asking for any personal information or passwords through email should also raise red flags. While this might seem obvious if the email address doesn't match, a spoofed email address can make this trick easier to fall victim to.

Also, be wary of anyone asking for your bank account number via email. Even if it is legitimate, there are other ways to send this information. Protect yourself by choosing a more secure method of communication.

What to do

If something seems off, research it. If you get a weird email requesting something or asking you to click on a link, don't assume it's safe. If it's from someone you know, ask them if they did send it.

If you are the one "sending," check your Outbox or Sent folder. This is a good indication if the email came from you or someone you know.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

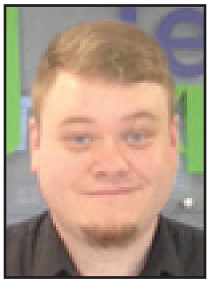
Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Win10 Creator's Fall Update Brings Hardened Ransomware Protection



Jared Stemeye is a help desk specialist at Tech Experts.

2017 has seen some of the most high-profile ransomware and cryptoware attacks to date. These incidents have demonstrated that these types of attacks can have catastrophic effects that reach far beyond the ransom demands paid to these attackers.

The cost of downtime and damage control multiplies quickly. Even more damaging is being impacted because critical infrastructure or health care services are unexpectedly unavailable for extended periods of time, consequently costing much more than any monetary value.

Microsoft has stated that they recognize the threat that these cybercrimes represent and have since invested significant yet simple strategies that are proving to be extremely effective as new attacks emerge.

These new security features are now coming to all businesses and consumers using Windows 10 with the Creators Fall Update.

These advanced security features are focusing on three primary objectives:

1. Protecting your Windows 10 system by strengthening both software and hardware jointly, improving hardware-based security and mitigating vulnerabilities to significantly raise the cost of an attack on Windows 10 systems. Hackers will need to spend a lot of time and money to keep up with these security features.

2. Recognizing that history has revealed vastly capable and well-funded attackers can find unexpected routes to their objectives. These latest security updates detect and help prevent against these threats with new advances in protection services like Windows Defender Antivirus and Windows Defender Advanced Threat Protection.

3. Enabling customers and security experts to respond to threats that may have impacted them with newly updated tools like Windows Defender ATP. This will provide security operations personnel the tools to act swiftly with completeness of information to remediate an attack that may have impacted them.

4. Microsoft states this is a proven strategy that has remained 100% successful on Windows 10 S, the new secure version of Microsoft's flagship operating system. Albeit, this version of the operating system does not allow any software from outside the Microsoft App Store to be installed.

Further, Microsoft states that even prior to the fall security updates rolling out, no Windows 10 customers were known to be compromised by the recent WannaCry global cyberattack.

Despite this, Microsoft knows that there will always be unforeseeable exploits within their systems.

This is why the Windows 10 Creator's Fall Update benefits from new security investments to stop malicious code via features like Kernel Control Flow Guard (kCFG) and Arbitrary Code Guard (ACG) for Microsoft Edge.

These kinds of investments allow Windows 10 to mitigate potential criminal attacks by targeting the techniques hackers use, instead of reacting to specific threats after they emerge.

Most importantly, Windows Defender security updates coming in this Fall will begin to leverage the power of the cloud and artificial intelligence built on top of the Microsoft Intelligent Security Graph (ISG) to promptly identify new threats, including ransomware, as they are first seen anywhere around the globe.

Though no exact date is set in stone, all of the amazing security updates detailed above will be available this Fall 2017 for free.

For more information about the Creator's Fall update beyond the security features, visit https://www.microsoft.com/en-us/windows/upcoming-features.

Create new service requests, check ticket status, and review invoices in our client portal: *http://www.TechSupportRequest.com*