Ashton
TECHNOLOGY SOLUTIONS

TECHMinutes
October 2018

Your Small Business Technology Information Source!

This Issue:

Our Top Tweets

@AshtonSolutions David Fisher, Ashton Pres Jim Millican, and Ashton Service Coord Laura Fisher were part of the team at this morning's Pals in Motion walk for Parkinson's Disease. Perfect day for it!

@AshtonSolutions Hard to see, but that's an Ashton fishing shirt being put to good use on Biscayne Bay. Learned a lot at Taylor Business Group #BigBIG and then got to have fun.

@AshtonSolutions Considering an acquisition? Or just want to make sure your current IT network is properly configured? Download Ashton's IT Due Diligence white paper to learn more. https://t.co/XQtxlAA82W

Our Sales Team Contact Info

Jim Abbott
jabbott@ashtonsolutions.com
216-539-3685

Peter Bunevich
pbunevich@ashtonsolutions.com
216-223-7010

Visit us **online** at:
newsletter.ashtonsolutions.com

In October, we join IT professionals from all over the U.S. to celebrate National Cybersecurity Awareness Month.

In promoting the strategies and practices that individuals, businesses, and other organizations utilize to protect their interests from the ever-growing number of threats found on the Internet, we work to advance the pervasive protection of data and information systems.

Your Employees Are Your Biggest Cybersecurity Risk

If we asked you to identify the biggest risk to your business' network security, what would you think it would be? Some might think that the countless threats on the Internet are the biggest issues your organization will have to deal with, while others might think natural disasters represent the biggest problem for your business. Many others, however, see the end user as the biggest threat to their business, and they are right… to an extent.

That's right. The same employees who are dedicated to keeping your business functioning as intended are also its biggest achilles heel. The reason for this is simple, even though it may not be clear right off the bat. They are using your technology solutions and working directly with clients, meaning that they are usually the first point of contact people would have in the dissemination of your business' responsibility for your business' operations, whatever they happen to be. An attack against them is an attack against the lifeblood of your business.

Of course, employees generally don't know when they are the source of your business' security problems, and most of the time they certainly don't mean to sink a ship they've boarded, so to speak. Hackers tend to take advantage of whomever they can, which is why they target your end users. They have the least to lose, and typically have a fair amount of

(Continued on page 3)

How to Thwart Targeted Phishing Attacks

Modern businesses rely on email as a central part of their communications infrastructure, but this comes with its own set of threats and issues that can derail operations. Spam in particular is troublesome for organizations to deal with, as it wastes time and exposes your users to danger. While spam can be blocked, more dangerous types of messages can make their way past your defenses. These types of threats are known as phishing scams, and they present a considerable threat to your organization.

Phishing attacks are targeted attempts by hackers and scammers to steal information from your users, whether they know it or not. These messages are personalized to look like legitimate requests for information in a way that makes them difficult to see as threats. Spam can be sent in large quantities to hit as many targets as possible, but phishing attacks are designed to penetrate defenses in a decisive way that spam can only hope to achieve. Keeping this in mind, it should come as no surprise that many cyberattacks start off as simple phishing scams. According to DarkReading, the results of a survey showcased that 91% of cyberattacks start off as a phishing email.

(Continued on page 2)

Managed IT Service Works for the Modern Business

Managing your business' technology can be challenging, especially if you're a small business with a limited budget. Either you have the money to pay a small in-house IT department to manage your organization's assets, or you don't. Depending on the way your organization is structured, you might even have your employees manage their own technology, which isn't the right way to go. As strange as it is to read, managed IT services are capable of providing an effective way to manage IT.

Managed IT services are outsourced services that your organization can take advantage of when it doesn't have the assets available on-hand to hire new staff. Managed IT can be something as simple as managing an email server or hosting a cloud solution, or it can be as advanced as the management and maintenance of an entire IT infrastructure in an off-site environment. Either way, managed IT is meant to help your business take advantage of services that your organization can't take advantage of normally.

Now, we know what you might be thinking. How can people who don't work for your organization know how to properly manage your IT?

What a lot of businesses need to know about managed IT services is that it's like having an extension of your own business dedicated to properly managing and maintaining your organization's IT assets. It's like having your own IT department, but without having to worry about fitting salaries into the budget, as well as any benefits that you might provide. You ultimately save money by working with a managed IT provider, making the service much more affordable in the long run.

Furthermore, the quality of IT management goes from "uncertain" to "guaranteed" when you work with an IT provider like Ashton Technology Solutions. Trained technicians do a much better job of managing technology solutions than those who are untrained, and this can save your business precious capital by minimizing the chances of a project implementation going wrong. Failing to implement a project right the first time can be expensive, as you're wasting both time and assets that could be better allocated elsewhere. It's much more efficient to let professionals who know what they're doing do the heavy lifting.

Simply put, managed IT services make managing IT easier for small businesses, even if they do have an IT department. There is always work to be done, whether it's helping employees with small issues or implementing a large-scale project. To learn more about how your business can take advantage of managed IT services, reach out to us at 216-397-4080.

Share this Article!
http://bit.ly/2wYY1n2

How to Thwart Targeted Phishing Attacks

(Continued from page 1)

These results come from PhishMe, which identified the reasons why phishing attacks work as well as they do:

- Curiosity: 13.7%
- Fear: 13.4%
- Urgency: 13.2%

These numbers make quite a lot of sense, considering how much stress the average employee is placed under just by going about their day-to-day duties. Some might think their performance isn't up to snuff, or they might feel pressured to click on attachments depending on who the message is from.

This puts your organization in a precarious position, as they might not think twice before downloading a suspicious attachment because it doesn't actually look suspicious to them at that particular moment. Therefore, you need to take measures to make sure your employees know how to identify phishing scams.

Ways to Mitigate Phishing Scams

If you can't convince your employees that identifying phishing scams is important, consider the following tips:

- **Undergo regular phishing scam training:** Training your employees to identify phishing scams might help them avoid these types of attacks in the future.
- **Double-check any suspicious messages:** You should always report suspicious messages to your IT department, even if you think it might not be worth looking into.
- **Never respond to urgent requests before following up:** If you receive a message that demands your immediate attention, or requests a wire transfer of funds, check in with whoever supposedly sent the message before doing so.
- **Review best practices and workflows:** If you think something about an email is out of place, follow best practices as dictated by your industry.

"Modern businesses rely on email as a central part of their communications infrastructure, but this comes with its own set of threats and issues that can derail operations. Spam in particular is troublesome for organizations to deal with, as it wastes time and exposes your users to danger."

To learn more about how your organization can stay safe from phishing scams, reach out to us at 216-397-4080.

Share this Article!
http://bit.ly/2x0J97I

Your Employees Are Your Biggest Cybersecurity Risk

(Continued from page 1)

work to do, so they are more distracted than someone who is diligent about going through their incoming messages. Here are three issues your IT administrator may run into.

User Error

Everyone makes mistakes, and your employees are no exception. Employees could click on a link that exposes them to threats or downloads malicious files, or they could download dangerous attachments from emails. All it takes is one weak link in the fence to break it down, and the same rhetoric can be applied to your network.

Phishing Attacks

While some low-level spam can be blocked by your email server, more advanced, targeted threats can make it past these defenses. This is because they are highly customized to attack specific individuals or organizations, making them more difficult to identify by spam blocking solutions. In these cases, it's best to train your employees to identify the warning signs and be suspicious about any out-of-place messages.

Mobile Device Usage

If you allow your employees to use their own personal devices for work, you open up an entire pathway for hackers to take advantage of to get to your business. Employees could be careless with how they use your business' data, and when they can walk out the door with it, this becomes a problem. Furthermore, employees will bring their mobile devices to the office, whether you like it or not, increasing the urgency to address these issues with your workforce.

If you want to keep your employees from creating problems for your business, we recommend taking the following actions. First, you implement a comprehensive employee security training strategy for your organization that's required by each and every worker you have. This helps to make them aware of the threats your organization faces every day. Once this has been handled, you can implement secondary security solutions to limit their exposure to threats in the first place, like spam blocking, content filtering, and so on. These measures make it so that your employees can both identify potential threats and dodge them altogether--a potent combination--that can surely keep your organization more secure than it's ever been.

To get started with preventative security measures and training ideas, reach out to Ashton Technology Solutions at 216-397-4080.

Share this Article!
http://bit.ly/2x0NZlj

Is Antivirus Software Important?

Modern organizations have a lot of threats that they need to secure themselves from. This is not something that you can ignore, as the slightest fault in your network security could usher in much more dangerous threats. If you haven't implemented some of the most basic security solutions out there, you're needlessly putting your business' future on the line. We're here to help make sure you don't do that.

If your organization is a bit on the smaller side, you might see enterprise-level security as something your business simply doesn't need. After all, you're a small business, and hackers aren't going to look twice in your direction… or will they? This rhetoric isn't the most solid way to approach network security, as the only thing keeping your organization secure from threats in this case is the whim of a hacker. If anything, hackers are more likely to target small businesses for this reason alone--they're more likely to actually get results from their attacks. Remember, there is always value to be gained from antivirus software and taking preventative measures.

It's difficult to argue against the strategy of taking preventative measures, as from a business standpoint the failure of your network security is, by an extension, the failure of your business. You have nothing to lose by implementing a network security system, including a firewall, spam protection, and content filter, but antivirus in particular can be troublesome to consider. Implementing antivirus accepts the reality that your organization could be infected, and it's something that no business wants to think about. Antivirus actually helps businesses meet their expected technology ROI, even if it's not immediately apparent.

An antivirus solution helps your business achieve a return on investment, but to truly understand what this means, you have to assess just how much your organization can lose in the event of a data breach. Imagine everything that could go wrong. If a threat makes it past your defenses and latches on to your network, it could spread and cause even more damage. It could spread itself across multiple devices and be incredibly difficult to get rid of. The time spent clearing your network of threats, as well as the downtime caused by your employees not being able to work as intended, can build up and cause considerable damage to both your budget and your reputation. After all… nobody wants to work with a business that doesn't take its network security seriously.

It's critical that your organization has a way to deal with threats after the fact--capturing and quarantining them before they have a chance to cause too much...

Read the Rest Online!
http://bit.ly/2x7A0dF

Could Your Business Benefit from E-Commerce?

Commerce has been fully embraced by the Internet, with online stores slowly phasing out many brick-and-mortar establishments. While you may not be in too much danger, depending on what you offer, you may also have the opportunity to leverage this trend in your favor. Below, we've outlined a few factors to help you decide if e-commerce is the right fit for you.

Can My Product/Service Be Sold Online?

Let's face it - if what you have to offer isn't something that someone would be likely to purchase online, you may have to get a little bit creative. After all, it makes sense to purchase goods online, but a service can sometimes seem a little out-of-place on an order form. However, if approached with the right mindset, a service-based business can easily offer things online while simultaneously benefitting their marketing efforts.

Instead of selling your services themselves, you can sell the kinds of things that support and encourage confidence in your services. Maybe you sell training sessions to help teach your clientele how to better use their solutions, or you offer premium content on your website for a nominal fee, like whitepapers and other useful materials. If you plan to follow this route, you need to make sure that your premium content adds additional value as compared to what the rest of your website's content offers.

Of course, you could include an order form for your services on your website… but if your services are priced based on scale, this could easily complicate things. In such cases, it is probably a better call to skip the order form and replace it with a call-to-action that recommends your inquisitive visitor to reach out directly and...

Read the Rest Online!
http://bit.ly/2wZAoL0

At Ashton Technology Solutions, we don't think of ourselves as computer guys, geeks or techies. Instead, we're problem solvers in the business of helping clients leverage technology for lasting business results. We just happen to have some serious technical skills as well. Of course we can talk geek with the best of them, but that's just the starting point for what we do, not the heart of it.

While we do take pride in delivering the most technically elegant solutions, at Ashton, we get the biggest satisfaction from integrating into our clients' processes, helping them look ahead, avoid trouble, and find better and more cost-effective methods of operating. In other words, we become partners in their growth. Ultimately, we earn our real enjoyment by watching our clients grow and prosper right along with us.

How to Speed Up a Computer

When a computer is new, it seems to blaze through tasks at unbelievable speeds… but this doesn't seem to last very long at all. In short order, a computer seems to slow to an excruciating crawl. What makes this happen, and how can it be fixed? We'll go over this below.

What Makes a Computer Slow Down

As many of us have learned the hard way, it can be remarkably difficult to find anything in a disorganized space. The same can be said of a computer. The less stuff that it has to deal with, the better it works. Stuff like clutter on desktops and in hard drives, caches that have built up, fragmented files, and a host of other factors only serve to slow down your system and stunt its capabilities.

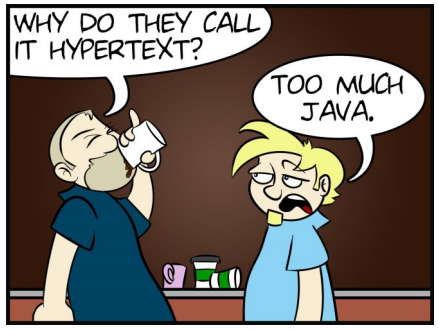
Fortunately, this can be fixed.

How to Fix It

Tidy Up

As we said, as your computer accumulates junk files and programs, it has a harder and harder time operating as intended. Take the desktop, for instance. Any icons that are displayed have to be loaded and refreshed, putting a drain on the computer's resources. In addition, there are often programs that run in the background that may be unneeded, pulling more resources away from what you are trying to do. Your IT resource should be able to help you reduce and consolidate the clutter on your...

Read the Rest Online!
http://bit.ly/2wYe2d0



Ashton Solutions

23625 Commerce Park
Suite 130
Beachwood, Ohio 44122
Voice: 216-397-4080

Visit us **online** at:
newsletter.ashtonsolutions.com

newsletter@ashtonsolutions.com
facebook.ashtonsolutions.com
linkedin.ashtonsolutions.com
twitter.ashtonsolutions.com
blog.ashtonsolutions.com