two river™
TECHNOLOGY TIMES

What's New

4 Ways Technology Can Improve Your Business

It boosts productivity. Technology like task management software can change how you work through a day. Everything is listed out, and you can check it off as you go. You can even make dependent tasks so tasks are automatically created for anyone who may be next in line to work on a project.

It's crucial to marketing. You need online and social media marketing. This is where people are. Understanding how social media marketing works can increase the number of people who know about your company, which increases your customer base.

It's essential for security. Technology and security go hand in hand. As your business relies more on technology, you need to rely more on security to protect your networked equipment, like all of your employees' PCs and your many servers.

You can't communicate without it. With things like e-mails, VoIP phone services, and direct messaging through social media sites, technology has made communication easier than ever. When you know how to use all these forms of communication, it puts you above the competition.

Pixel Productions Inc., 7/20/2019

December 2019

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Cybercriminals Are Taking Aim At Your Business … Is Your Network Protected?

Cybercriminals love to test your defenses. They love to see how far they can get into the networks of businesses all over the globe. Cybercriminals really love going after small businesses because they can all too often sneak onto a network, copy data and move on. Through the use of ransomware, they can hold your data hostage and refuse to cooperate until you pay them some amount of dollars – and if you don't pay up, they threaten to delete all your data.

But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take that target off your back.

The first thing you need to do is understand why cybercriminals target small businesses and what makes your particular business vulnerable. There are many things small businesses do and don't do that open them to attack and data theft. These may include not having enough (or any) security in place or not training employees on security protocols.

Realistically speaking, the biggest threat to your business does, in fact, come from your own employees. This doesn't mean they are intentionally harming your business or leaving your network exposed to outside threats. It means they don't have the proper training and knowledge to protect your business from a cyberthreat.

Continued on pg.2

Continued from pg.1

For instance, your team needs to be trained to use strong passwords, and those passwords *must* be changed periodically (every three months is a good rule of thumb). A lot of people push back on strong, complicated passwords or use the same password for everything, but this is just asking for trouble and should not be allowed at your company.

Once strong passwords are in place, enable two-factor authentication (2FA) on everything you possibly can, from network access to every account you and your employees use. This is an additional layer of security on top of standard password protection. This feature is generally tied to a mobile number or secondary e-mail, or it may be in the form of a PIN. For example, when 2FA is enabled, after you've put in your password, you will be prompted for your PIN for the associated account.

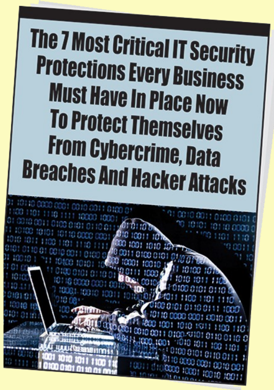
> **"You can take steps to significantly reduce that threat and take that target off your back."**

Another thing you must do to get that target off your back is to get anti-malware software installed. Every workstation or device should have some form of this protection. Not sure what to use? This is when working with a dedicated IT company can come in handy. They can help you get the right software that will meet your specific needs without slowing you down. They will install software that is compatible with your PCs and other networked equipment. Plus, they will make sure anti-malware software is working and is regularly updated.

On top of this, you want to have an active firewall in place. Every business should have its network protected by a firewall; like anti-malware software, firewall security comes with a number of different settings, and you can customize it to fit the needs of your network. Firewalls help keep attackers and malicious software off your network. When paired with a good anti-malware software, your layers of security are multiplied. The more layers, the better protected you are.

Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, malware protection policy and proper e-mail and web-surfing etiquette. The bad guys are never going to stop attacking, but you have the power to protect your business from those attacks.

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Get Your FREE Copy Today by emailing your request to kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

HD Mask Surveillance Camera USB Spy Cam

Sometimes, you don't want security cameras in plain sight or you don't even want to go to the trouble of installing cameras. Meet the HD Mask Surveillance Camera USB Spy Cam. This device makes video monitoring easier than ever.

The HD Mask is a tiny camera disguised as a USB charger. At a glance, you would have no idea it was a camera. Even better, it actually works as a USB phone charger, which really sells the disguise. It records as soon as it's activated with motion and has many practical purposes, from keeping an eye on pets to monitoring certain areas of your office for security purposes. You can access the footage right on your smartphone and watch in real time. Learn more at HDMask.com.

What A Football Coach Can Teach You About Getting Better

Woody Hayes spent 28 seasons as the head football coach at Ohio State University, and then he was fired after a now-infamous incident in the 1978 Gator Bowl.

With time running down in the fourth quarter and the Buckeyes already in a position to try a game-winning field goal, Hayes called a pass play. A Clemson player intercepted the pass and was knocked out of bounds along the Ohio State sideline, securing the victory for the Tigers.

Frustrated by the play and the opponent's celebration among his troops, Hayes lost his temper and hit the Clemson player.

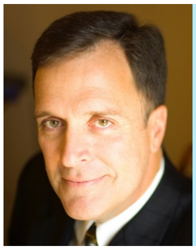
For most Ohio State fans, however, that's not the legacy of Woody Hayes. Some, naturally, see his legacy in his coaching record – 238 wins, 72 loses, 10 ties, 13 Big Ten titles, and three National Championships. That proved more than enough to land Hayes in college football's Hall of Fame. The OSU Woody Hayes Athletic Center is also named in his honor.

Others, however, see his legacy in a chair – the Wayne Woodrow Hayes Chair in National Security Studies. In keeping with his wishes, donations made in his honor following his death in 1987 were directed toward academics, which led to the creation of the chair. Hayes, who once grilled Richard Nixon about foreign policy, always took academics as seriously as he did football.

I remember Hayes for all of those things, but I remember him most for something he said during a pep rally when I was a student on the Columbus campus: "You're either getting better or you're getting worse," he told the crowd. "Status quo is a myth."

I used to think that was coach talk, but time and experience taught me the truth in what he meant. In a competitive world, if you stay the same, you get passed by. It highlights the incredible importance of the "innovation imperative": keep making your value better, because your competition keeps getting better.

Regardless of how good you've become, you can't afford to stay the same because status quo is a myth.



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

Stay Safe Online This Holiday Season

Online holiday season shopping: The facts

Shopping heats up in November and December, and a lot of those transactions occur on laptops, tablets, and mobile devices. Amid the increase in e-commerce, financial fraud climbs, too.

- 8% of consumers surveyed in 2018 said they were a victims of identity theft during the holiday season.
- 43% of online shoppers surveyed said their identity theft occurred holiday shopping online.
- 56% of holiday shoppers plan to make purchases online in 2019.
- $1,047.83: average amount that American consumers plan to spend on holiday shopping in 2019.
- Up to $149 billion: online holiday shopping sales for 2019 (projected), from November to January.
- 84% of holiday shoppers plan to use their smartphones to research products and look for coupons before buying in-store.
- 18%: The amount online sales are projected to grow in 2019 compared with 2018.

Ship to a secure location

The rise of online shopping has led to an increase of home deliveries — and with it, an increase in “porch pirates”, or thieves who steal packages from doorsteps. If no one’s home to accept a package, consider shipping to your office or another safe place. UPS, Amazon, and FedEx all now have shipping lockers available for secure deliveries.

Only use official retailer apps to shop

Mobile apps allow you shop for and purchase items while you’re on the go — making holiday shopping a breeze.

But the danger arises if you unknowingly install an app laced with malicious software, or malware. Criminals use these apps to infiltrate smartphones and do any number of things, like direct users to fraudulent premium subscription services or automatically subscribing users to expensive content providers without the user’s consent. .

Protect yourself against malicious mobile apps by only downloading apps from reputable stores, such as Galaxy Apps, the App Store, Amazon App Store and Google Play. Some providers, such as Google Play, scan apps for malware prior to publishing them on their store.

Don’t save your credit card information on your accounts

While it may be convenient to store personal and payment information in your online accounts, it does come with risk. Some retail websites may not be equipped to secure your info, which could leave your personal details and payment card data vulnerable to cyberthieves or data breaches.

If a hacker accesses your favorite shopping account, it could then be easy for them to make fraudulent purchases with the credit card information you’ve saved in that account. That’s why it’s best to either skip the autofill option or try using a password manager, which provides an extra layer of protection to your account info.

Consider using a Digital Wallet for a second layer of protection

Credit card fraud is a serious problem in the U.S., but using a digital wallet or app, such as Apple Pay, Google Pay, Venmo, or others can increase your transaction security.

The digital wallet obscures your payment card information so the merchant sees a unique, one-time code that’s only good for that purchase. So if a store employee or a hacker tries to get their hands on the store’s payment information, they wouldn’t be able to see your credit card or bank details.

Never make purchases on public Wi-Fi

You might be tempted to take your shopping spree to a coffee shop for a cup of joe. Keep in mind, Wi-Fi networks use public airwaves. With a little tech know-how and the freely available Wi-Fi password at your favorite cafe, someone can intercept the data you send and receive while on free public Wi-Fi.

Shopping online usually means giving out information that an identity thief would love to grab, including your name, address, and credit card information. Bottom line: It’s never a good idea to shop online or log in to any website while you’re connected to public Wi-Fi.