two river™
TECHNOLOGY TIMES

What's New

The Real Reason Your Team Isn't Ready To Work

The pandemic caused many employers to allow their employees to work remotely. As we enter the second winter during COVID-19, fewer people have returned to the workplace, and many wonder if they will ever return to the pre-pandemic work environment. The truth is that the virus has caused many uncertainties for people.

There's no telling if there will be more mandates in the future that will cause employees to stay working remotely. Many have changed how they handle childcare and would need time to make new arrangements if asked to return to work. Microsoft recently dealt with this, announcing a "return to work" date for its employees to eliminate any uncertainties. The company wants to find ways to ease people's minds before bringing them back into the workplace. The more comfortable your employees are, the better they will perform and the more likely they will be to stay with the company.

December 2021

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!"

Don't Let Hackers Ruin Your Holidays

Online shopping has become more popular than ever before. In 2020, more than 2 billion people bought products or services online. Whether they're shopping online because it's more convenient or they're avoiding going to brick-and-mortar retailers during the ongoing pandemic, more people are turning to online retailers every day.

It's not just the convenience or health safety that's drawing people to shop online; shopping this way has become more secure than ever before. That doesn't mean all retail websites are created equal when it comes to of safety and security. Hackers and scammers are still out there trying to get your information, but by taking the proper precautions, you have no reason to worry while shopping digitally.

If you plan on buying online this holiday season, here are five tips to ensure your information stays protected.

Use Well-Known And Secure Sites

When looking to purchase a product or service online, you have thousands of options to choose from. To avoid having your personal information stolen, it's best to use familiar sites such as Amazon, Walmart or any of the other major retailers. If you search for a product on a search engine, you may be presented with prices that are extremely low. There's a good chance these are not trustworthy sites. When it comes to online shopping, if it seems too good to be true, something is wrong.

Pay attention to the security of the site where you're trying to make a purchase. Look for a lock icon in the browser bar. If the website has one, then you should be safe on their site. Another way to tell is by looking at the beginning of the web address. If it begins with "https" instead of "http," you are in good shape, and you can continue using the site. Secure websites help protect your

Continued on pg.2

Continued from pg.1

financial information as well as passwords. Shopping at unsecured sites can put your personal information at risk.

Create Stronger Passwords

A strong password can make all the difference between your information remaining secure and someone stealing it. You need to make your passwords as difficult as possible so that hackers and thieves can't hack into your accounts. It's best to use a complex mix of uppercase and lowercase letters while including special characters and numbers. Avoid using common spellings of words and personal information in your passwords because these can be easier to crack.

> **"In 2020, more than 2 billion people bought products or services online."**

If you're worried about not remembering a complex password, use a password manager. This tool will remember the passwords for your accounts while also keeping them protected. Utilizing password managers is the best way to create complex passwords since you won't have to personally remember them, and they will still be protected.

Keep Track Of Your Statements

You should always be watching your finances, but it becomes even more important when shopping online. It's a good habit to form and will help you catch overcharges or purchases that you did not make. It's also a good idea to only shop with a credit card when shopping online. If someone hacks into your account and steals your debit card information, they will have direct access to your money. Most credit cards have protections in place for fraud, so you won't be at fault for any errant charges on your account.

Protect Your Information

When entering a new website, you should be wary if they ask for any personal information upfront. No online retailer should ever ask for your Social Security number unless you are applying for a credit card on their site. Be cautious if they ask for your birthday as well. Hackers can use this information in conjunction with your credit card number to wreak havoc on your life.

Don't Shop On Public WiFi

While it might seem like a good way to keep yourself entertained while enjoying a coffee at a local café, shopping on public WiFi can leave you at risk of being hacked. Public WiFi is often not very secure, and entering your personal information while using it can give hackers easy access. It's much safer to bookmark the item and wait until you're home or no longer using WiFi to make the purchase.

Shopping online can be as safe and reliable as shopping in a store – as long as you take the proper precautions. Take some time to ensure that you are following the right security measures before making purchasing or entering any information.

Free Report : The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

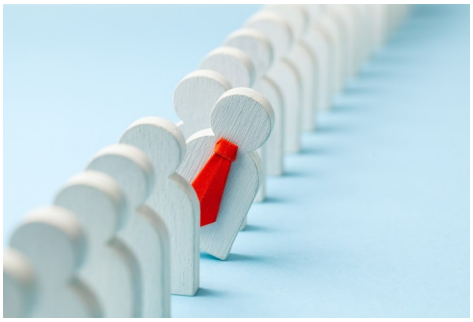
To receive a copy of this FREE report, email kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

Travelmate Robotics

Tired of the usual, old-fashioned luggage? Travelmate Robotics is trying to change the luggage game. With these suitcases, you never have to worry about the safety of your items. It comes standard with a secure Bluetooth-enabled lock and GPS tracking if your bag ever goes missing. The suitcase also comes with a scale so you'll never have to worry about overpacking. The best part? The suitcase is entirely autonomous and will follow you around through a Bluetooth connection. The "Follow Me" function as well as the obstacle avoidance system sets Travelmate Robotics ahead of the competition. It's the ideal suitcase for any businessperson or frequent flyer.

When To Cut People From Your Team



Not long ago, I had a subscriber reach out to me with a challenging question. This person's business had made many changes due to COVID-19 and the economy. They wondered when they should begin cutting people from their team. To explain my views on the matter, I like to turn to a story from the Bible.

A man named Gideon was selected by God to lead the Israelites and free the people of Israel from those who were worshipping idols. Gideon gathered 32,000 men from four tribes in an effort to defeat the Midianites. After Gideon had gathered the troops, God came to him and informed him that he had gathered too many soldiers.

When Gideon asked what he should do, God said he should give a rousing speech to the 32,000 troops, but he should end the speech by saying, "Now that we're off to fight … if there's anybody here who's afraid and you think we're about to lose this upcoming battle with the Midianites, you can be excused at this time. Go home, we can't use you this time." When Gideon gave this speech, 22,000 members of his army decided to call it quits.

This is an important story to consider when trying to decide if you need to make cuts to your team. When you are recruiting, it's hard to get an idea of how someone will actually turn out. You're bound to make some wrong hires who don't appreciate what you are trying to do. If someone does not believe in the cause, they do not deserve a spot on your team.

God came to Gideon after he relieved the 22,000 soldiers from service and told him he still had too many soldiers. Gideon was instructed to march his troops until they were hot, thirsty and tired before bringing them to the river. Gideon did just that, and when they arrived at the river, 9,700 of his troops dropped their shields and spears before jumping into the water. Gideon then excused those troops and was left with 300.

Gideon took his 300 troops and led them to attack the Midianite camp when night fell. By using a strong strategy and the might of his small – but dedicated – team, Gideon sent the Midianite army fleeing in terror.

I am a big believer in creating a small but dynamic team. By recruiting the right people, you have a better chance of success. The more difficult part of leadership is letting go of those people who are too afraid or negative and replacing them with suitable candidates. It might not be easy, but it is necessary.

While Darren Hardy was growing up, his father always told him to be the exception. He has taken this philosophy and applied it to his many pursuits in the world of business. Darren has remained at the forefront of success media for over 25 years and is not stopping anytime soon.

Services We Offer

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

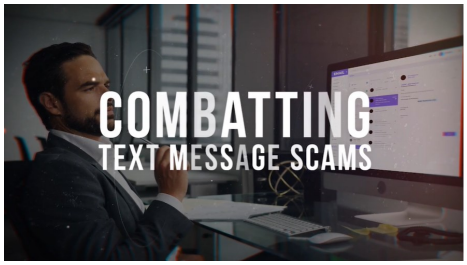
TRTG Happenings

#GIVEBACKATWORK

We have returned to our office, and we are ready to continue our holiday tradition of giving back this season! We have partnered back up with Bell Works to run our annual Holiday Food Drive to benefit our local food bank, Fulfill. Starting on December 1st tenants and visitors will have the opportunity to place their donated food items in the large cages located at the entrance of the building.

We will also be running a fun holiday themed box decorating contest amongst the tenants in the building. On December 21st, the last day of the food drive, all tenants participating in the box decorating contest will bring their decorated boxes down to the atrium and will get judged by the Creative Team at Bell Works along with a team member at Fulfill. First, second and third place winners will receive prizes. We can't wait to kick off the season of giving back!

Combatting Text Message Scams



Cybercriminals are always looking for new ways to sneak into your life and text messages are becoming one of their favorite avenues. Text message scams are already prevalent and dangerous in the digital world, so be on the lookout. Many text scams utilize similar tactics as email or voice phishing (also known as vishing), by using social engineering and available information on you to craft a text that you are likely to interact with.

Many of these scams offer something to their victim like a prize, a low interest credit card, or help with loans. But many of these prizes come with the cost of your personal information that the cybercriminal can then use against you. **They could act as a vendor or service you** use frequently claiming an issue with your payment information, suspicious account activity, or sending a fake invoice and asking you to contact them if you didn't authorize the payment. They might use popular shipping companies against you by sending a fake delivery notification with a link that could leave your device to being infected with malware.

Cleverly cybercriminals have a lot of options when it comes to how they want to scam people through text. But you also have a lot of option for limiting your interactions with these scams.

You can use the settings on our phone to filter spam and unknown messages. On iPhone, you navigate to Settings, Messages, then turn on filter Unknown Senders. On Android, go to your phone app, click the three vertical dots, find your way to Settings, Blocked Numbers, then turn on Unknown.

Your wireless provider may also be capable of filtering out unknown senders, so try giving their customer support line a call. For even more protection, you can download a call blocker app that also block texts.

Lastly, remember to follow the most important rule of dealing with text message phishing attempts, if you don't know the sender, do not interact with any links or attachments, and do not reply.

Since its invention texting has reigned as the number one method of communication over long distances. This means that text messages are used more often than email or phone calls, and that means cybercriminals are going to try and take advantage of them. Do not let them get the upper hand. Start protecting your text messages today!

Is It Time For Cybersecurity Planning?

The time to start planning for a security threat isn't during a virus outbreak or immediately after you discover funds transferred within your banking accounts. Decisions and judgments made during this time are typically driven by emotion and not facts. The time to make those cyberthreat plans is now.

Things to consider when you're planning:

- Physical access to your building(s)
- What to do with lost or stolen mobile devices
- PCI (payment card industry) compliance requirements
- Data-breach incident response
- Threat monitoring

That's where we are here to help! Give us a call and we'll be glad to help you evaluate your "cybersecure" plan.

There are great resources out there for businesses that just don't know where to start with cybersecurity. Take a look at http://www.fcc.gov/cyberplanner for a customizable guide to where to get started with operational and organizational planning.