two river™
TECHNOLOGY TIMES

What's New

Top Business Apps To Get You Organized

If you're struggling to stay on top of your work tasks, there are some great apps available to help out.

- **Asana** helps your business improve communication and collaboration. You can view all tasks and projects and follow progress on a communal board so you can communicate without having to rely on e-mail.
- **Proven** helps organize your hiring process by posting listings to multiple job boards with one click. You can also review and sort applicants with ease.
- **Boxmeup** organizes and tracks your packages, containers and bulk storage items to make storing and shipping a breeze.
- **Evernote** keeps all your notes organized in one place and allows you to easily share notes and lists with co-workers.
- **Trello** tracks your team's workflow. Whenever you make a change to a project or task, the app notifies each team member involved so you don't have to.
- **KanbanFlow** helps managers visualize overall workflow. It gives overviews of work status, tracks progress and assigns tasks to team members.

Nerdwallet, Apr. 21, 2020

December 2020

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 Confess:

The Top 3 Tricks And Sneaky Schemes They Use To Hack Your Computer Network That Can Put You Out Of Business

Cybercriminals and hackers are rarely shy about the methods they use to attack their victims. Many of them are more than happy to share how they broke into a business's network or how they walked away with thousands of dollars after successfully extorting a business owner whose company is now destroyed.

There are new stories out there to get your blood boiling as cybercriminals work to ruin people's lives and livelihoods. These criminals don't care what kind of damage they do. They only care about one thing: money. If they can get away with it – and many do – they'll keep on doing it.

It's up to the rest of us as business owners (and employees) to stay at least one step ahead of these cyberthugs. The single best way to do that is to **stay educated on the latest threats.** The second-best way is to **stay up-to-date with the latest technology designed to combat cyber-attacks.**

Here are three tricks of the trade cybercriminals are using right now in an attempt to get their hands on your money:

Ransomware. This is very common. It's a form of malware, and it can sneak onto your network and into your computers in a number of different ways:

- **Ad Networks.** These ads can appear on social media sites and on familiar websites. Someone clicks a compromised ad or pop-up, and it initiates a file download. It's quick and it can be confusing. This is where anti-malware and anti-ransomware come in very handy.
- **Malicious Links.** The cybercriminal sends you a legitimate-looking e-mail,

Continued on pg.2

Continued from pg.1

supposedly from your bank or a familiar online store. It may even be disguised as an e-mail from a colleague. The e-mail contains a link or file. If you click the link or file, it installs the ransomware.

- **Hidden Files On Thumb Drives.** This happens way too often where someone brings a thumb drive from home. While the user doesn't know it, the drive has a malicious file on it. When the thumb drive is inserted into a networked machine, the file is installed.

No matter how the ransomware gets onto your devices, the result is basically the same. The ransomware goes to work and begins encrypting your files. Or it may completely block you from accessing your computer altogether. You'll get a full-screen message: *Pay up or never access your files again.* Some ransomware programs threaten to delete all of your files. Others say they will never restore access.

DDoS Extortion. Short for distributed denial of service, DDoS attacks are a relatively easy way for hackers to take down your business's online presence and wreak havoc on your network. These attacks mimic online users and essentially "flood" your network with access requests. Basically, it's as if millions of people were trying to access your website at once.

Your network simply can't handle that kind of traffic and, as a result, it goes down. The hackers can continue the attacks until you take action. That is to say, until you pay up. If you don't pay up, the hackers will do everything they can to keep you offline in an attempt to destroy your business. If you rely on Internet traffic, this can be devastating, which is why many businesses end up paying.

Direct Attacks. Some hackers like to do the dirty work themselves. While many cybercriminals rely on bots or malware to do the work for them, some hackers will see if they can break through your network security in a more direct way. If successful at breaking in, they can target specific files on your network, such as critical business or customer data.

Once they have the valuable data, they may let you know they have it. Sometimes they'll ask for money in return for the sensitive data. Sometimes they won't say anything and instead simply sell the data on the black market. Either way, you're in a bad position. A criminal has walked away with sensitive information, and there is nothing you can do about it.

> **"You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm."**

Except, that last sentence isn't true at all! There *are* things you can do about it! The answer is preventative measures. It all comes around to these two all-important points:

- Stay educated on the latest threats
- Stay up-to-date with the latest technology designed to combat cyber-attacks

If you do these two things and work with an experienced IT services company, you can change the outcome. You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm.

Help Us Out, And We'll Give You A Brand-New Kindle Fire For Your Trouble

We love having you as a client and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of December.

Simply refer any company with 10 or more computers to our office to receive a FREE computer network assessment (a $397 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Kindle Fire of your choice as a thank-you (or donate $100 to your favorite charity ... your choice!).

Send your referral to kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

SelfieSpin360 For GoPro

A GoPro camera is great for a crystal-clear, wide-angle video of yourself or your subject, and you can attach it to the end of a selfie stick for some nice static shots, too. But if you're ready to take things up a notch and capture even more truly awesome moments, then you need the SelfieSpin360.

It's all there in the name: the SelfieSpin360 gives you a way to get incredible 360 degree footage of yourself in any setting. You attach your GoPro or smartphone to the end of a sleek and secure base, which is attached to a long cord with a handle for camera controls on the end. Hit Record, then start swinging the device up and around your head lasso-style to capture a unique version of yourself in a special moment. The SelfieSpin360 kicks boring old selfies to the curb. Visit SelfieSpin360.com to purchase yours.

Successfully Convince A CEO In 3 Steps

Here is your chance. You don't want to blow it.

You have a meeting scheduled with a CEO. Your goal is to convince them...

- To spend $1 million on your product or service or to make a large donation to your cause
- To hire you, promote you or give you your dream job
- To invest in your idea

Ineffective Ways To Convince A CEO

Many people "show up and throw up" and push a lot of information at the CEO — either verbally or by PowerPoint. I'm not sure why so many unpersuasive people follow this approach. Maybe it's to "show you know what you are talking about." But it does not make a CEO say "yes."

Another bad approach is to phrase your request as a "we ought to." CEOs don't decide to do things just because other people say they ought to do something. Or worse yet is when people only talk about why *they* want something to happen, fully ignoring the wishes, concerns and perspective of the CEO.

Successfully Convince A CEO In 3 Steps

1. Seek first to understand the CEO's perspective — that is Stephen Covey's advice. It needs no further explanation. Your first step in discussing a topic with a CEO is to put all your energy into asking probing questions, listening and learning what the CEO thinks about a topic and why. Forget about your agenda or your needs for a moment.

2. Reflect the CEO's perspective to their satisfaction. This step is hard. Most people cannot objectively reflect or restate another person's perspective about a topic without putting their own personal slant on it. I first learned this step during my psychology PhD training in a class on conflict resolution. At this step, you must restate the CEO's perspective on the topic simply and without putting words in their mouth or trying to spin it in your favor. You know you have succeeded at this step once the CEO says the magic word. The magic word is "exactly." This means that the CEO believes that you understand their perspective. Then, and only then, have you earned permission to move to the final step.

3. Propose your idea as a way to help the CEO achieve their goals. The mindset for this step is not that you are about to trick or fool a CEO into doing something that's not good for them. Your mindset is that you are about to convince a CEO to do something that *is* good for them. (And by the way, if what you are about to propose is not in the CEO's best interest, then don't propose it!) A simple way to propose your idea is to say, "Your goals are X. Your concerns are Y. So, I propose you do Z."

And, contrary to popular belief, great ideas don't sell themselves. It takes a skillful leader to successfully convince a CEO.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book *Who: A Method For Hiring* and the author of the #1 Wall Street Journal best seller *Leadocracy: Hiring More Great Leaders (Like You) Into Government*. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a Bachelor of Arts in Economics with honors from Northwestern University and a Master's and Doctorate in Psychology from Claremont Graduate University.

Services We Offer

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

TRTG Happenings

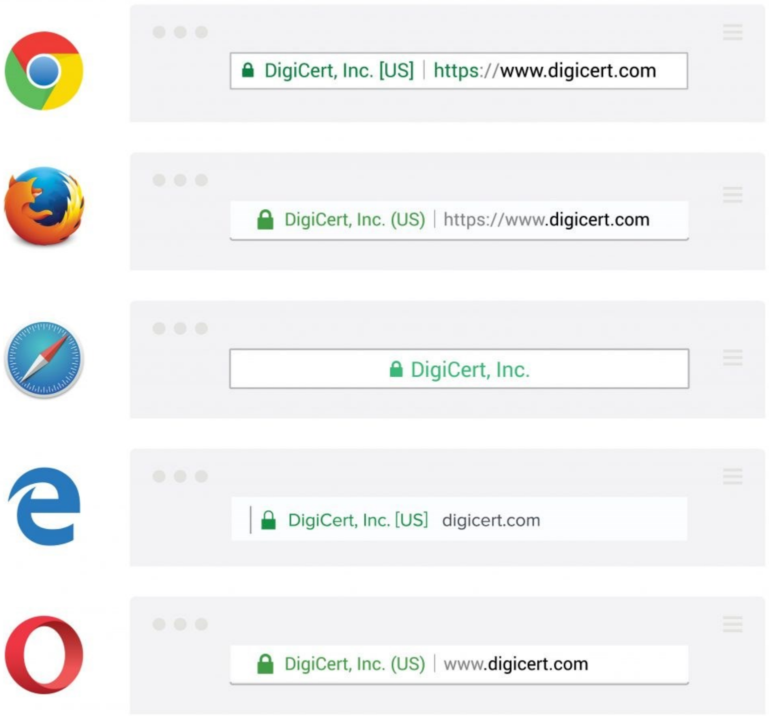
Online Shopping? Read These Tips To Stay Safe

As the holiday season quickly approaches, the coronavirus pandemic has already altered this year's shopping experience. With fewer visitors joining the in-person shopping crowds, Covid-19 has accelerated the shift away from physical stores to digital shopping. While retailers compete for online business with massive blowout sales, enticing customers in an attempt to create the easiest shopping experience possible, threat actors have also taken notice.

As we wait in anticipation of the upcoming holiday sales, it is not only the stores and buyers who are getting ready; threat actors are organizing their infrastructures to exploit this year's holiday spending. To stay protected this holiday season, remain vigilant, and follow these online shopping recommendations:

1. Confirm you are using an authentic website.

In the past, people rushed to their local store that promoted gate-crasher deals to the first 100 customers on Black Friday. Consumers planned their shopping extravaganza and knew which shops, which shelves and which products they wanted to buy. In person, there's no mistaking the physical shop. Over the decades, trust with those brands has been established.



DigiCert, Inc. [US] | https://www.digicert.com

DigiCert, Inc. (US) | https://www.digicert.com

DigiCert, Inc.

DigiCert, Inc. [US] digicert.com

DigiCert, Inc. (US) | www.digicert.com

However, one of the vulnerabilities with online shopping is that when rushing to grab that super deal, consumers may not check for the little padlock on the web address. Do they even check the web address? Google and Amazon are now the most imitated brands in terms of phishing reports. In other words, threat actors create similar-looking websites in order to trick consumers into using their site for purchases and thereby capture personal data for malicious purposes.

Before providing your personal information and payment details, confirm that the website is authentic. It is always best to be cautious and ensure that the source is authentic by going to the retailer's official website.

2. Learn how to spot holiday phishing emails.

Another popular phishing technique involves cybercriminals sending emails that prompt shoppers to click on links that will then take them to specially constructed websites that impersonate legitimate shopping sites where they can steal credit card details entered unwittingly by users. Last year, the number of people who had accessed e-commerce-related phishing websites during the online shopping season had more than doubled since 2018.

To avoid falling victim to a phishing scam, take your time to confirm that your holiday shopping emails are accurate. Beware of lookalike domains and spelling errors in emails or websites. Be cautious with files received via email from unknown

TRTG Happenings

senders, especially if they prompt for a certain action you would not usually do. And, again, if you're redirected to a website, ensure you are ordering goods from an authentic source. One way to do this is to Google your desired retailer and click the link from the Google results page. If a promotion sent via email is legitimate, it should also show up on the retailer's website.

3. Avoid breaches due to password compromise.

More than 80% of hacking-related breaches involved the use of lost or stolen credentials, and approximately 35% of all breaches were initiated due to weak or compromised credentials. So how can you avoid falling victim to password compromise while using your online shopping accounts?

Complexity is the enemy of security. People often get tired of trying to remember multiple passwords and resort to one password everywhere or they think they're outwitting hackers with small changes like changing just one letter. Here's an easy solution you can implement right now: Use a passphrase.

Passphrases are more secure — the more digits, the harder it is for threat actors to write algorithms to break them — and easier to remember. Once you've built a system in your mind, it's simple. For example, many sites require that a password contain letters, numbers and special symbols, so my advice would be to build your own shorthand language. Let's say every vowel is capitalized, except the letters "i," which would correspond to the number 1 and "a," which would correspond to the @ symbol. So a simple passphrase like "I'mfromCalifornia" becomes "1mfrOmC@l1fOrn1@." The key is remembering your simple set of rules.

4. Avoid questionable deals.

Finally, if a deal seems too good to be true, it most likely is. Threat actors will distribute malicious phishing links to their victims via email, hoping their email will slip through undetected amid the multitude of legitimate discount offers. Has Apple ever discounted its latest gadget by 90%? Never.

So when you see a deal too good to be true, trust your gut.

Protech Your Accounts—Change Your Password!

When it comes to updating passwords, we are creatures of habit -- and change is hard.

But it's 2020 and it may be time to beef up your security game because, according to new research, people are still using easy-to-hack passwords like "123456789," the word "password," and "iloveyou."

Of the 200 worst passwords, "123456" is the most commonly used of 2020, with 2,543,285 people choosing it. It takes less than a second to crack.

Despite several reminders from cybersecurity experts, after comparing the list of the most common passwords of 2020 to that of 2019, there is little to no difference -- aka we haven't learned much.

The top 10 most common passwords were:

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. qwerty

If your password is on the list, it's probably time to make a change.

Try to avoid using dictionary words, predictable number combinations, or strings of adjacent keyboard combinations. And this should go without saying -- but under no circumstances should you use a password based on any personal details like your phone number, birth date, or name.

We suggest changing your passwords every 90 days with a mix of upper and lowercase letters, and creating a different password for each of your accounts.

If you find yourself having difficulty figuring out a unique password or remembering passwords, use a password locker like LastPass.