The Tech chronicle

Courtesy of BRANDON BUSINESS MACHINES

What's New

BBM'S NEW CUSTOMER PORTAL!!!

- Now available for your use
- Easily managed from any device
- Accessible 24/7

YOU CAN NOW …

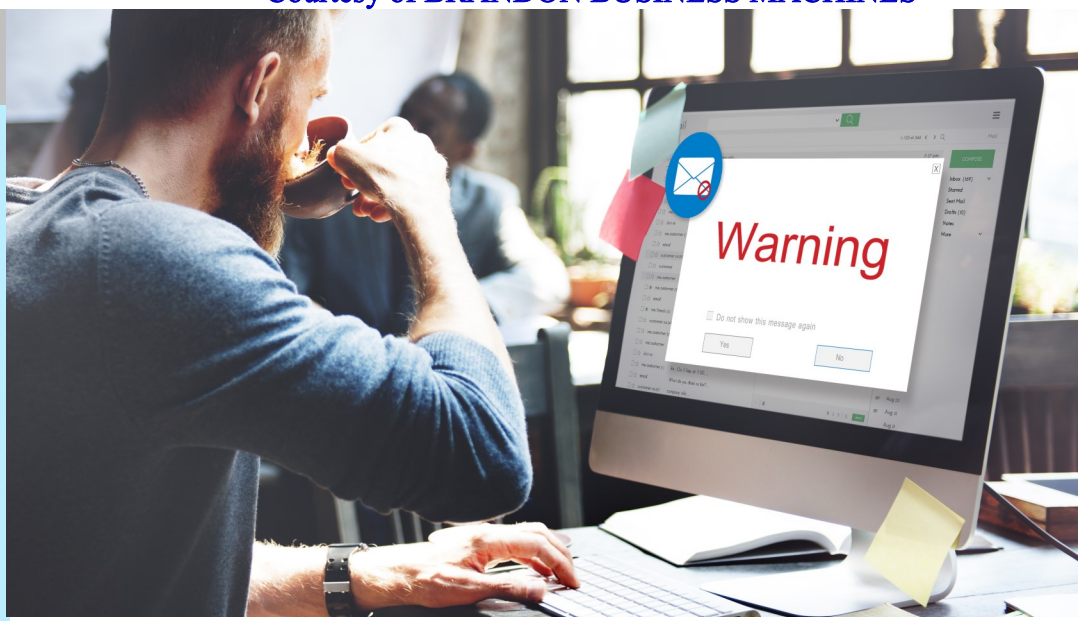
SET UP YOUR OWN ACCOUNT
Go to https://myportal.bbmusa.com/ and click on New User? Sign up now. Need help? Call 813-689-1950 and we will walk you through setting up your account.

REQUEST FOR SERVICE
Create a work order ticket for service, repair or supplies.

MAKE SECURE PAYMENTS
View and print invoices. Schedule and make payments online.

TRACK ALL YOUR EQUIPMENT
Find a list of all your equipment.

October 2020



The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

We all make mistakes. It's a fact of life. But as we all know, some mistakes can have serious and lasting consequences – especially when it comes to business, cyber security and the constant cyberthreats that are out there.

While some businesses have invested heavily in cyber security, many have not. When it comes to network and data security, one of the most vulnerable areas of the economy is small businesses.

More often than not, small businesses simply don't go all-in when it comes to IT security. Some fear they don't have the budget and worry that IT security is too expensive. Others don't take it seriously – they have an "it will never happen to me" attitude. Then there are those who invest in *some* security, but it's limited and still leaves them vulnerable in the long run.

But there is one area of IT security where *every* business is vulnerable. You can have the greatest malware protection in the world and still fall victim due to this one big mistake.

Your employees lack IT security training.

It's as simple as that. When your team isn't trained on IT or network security *and* they aren't aware of today's best practices, you open yourself to major risk. Here's why: We make mistakes.

Scammers and cybercriminals have the most success when they are able to trick people or play on the emotions of their victims. One common emotion they use is fear.

No one likes to get a message telling them that their bank account has been compromised. This is how phishing e-

Continued on pg.2

Continued from pg.1

mails work. The scammer sends an e-mail disguised as a message from a bank or financial institution. They may tell your employee that their account has been hacked or their password needs to be changed immediately. They use fear to trick them into clicking the link in the e-mail.

So, concerned about their bank account, your employee clicks the link. It takes them to a web page where they can enter their username, password and other credentials. Sometimes it even asks for their full Social Security number. (Scammers are bold, but people fall for it!)

As you guessed, the web page is fake. The link in the e-mail directs your employee to a page that allows the scammer to collect their data. Some thieves use it to access their bank account, but others sell the information for a quick buck. No matter the situation, the information has fallen into the hands of crooks.

The challenge is that phishing e-mails have gotten harder to spot. Scammers can spoof legitimate web addresses. They can make fake e-mails look like the real deal. But there are still plenty of minor details that indicate the e-mail is a fake.

This is one of the MANY reasons why comprehensive employee IT training is so important. Training helps employees identify red flags. But more than that, it helps them identify *changing* red flags. For instance, a phishing e-mail from 2010 looks nothing like a phishing e-mail from 2020.

"Your employees are your first defense against outside cyber-attackers."

Scammers stay ahead of the curve. They know the trends, and they know how to adapt. Your employees also need to know the trends and need to be ready to adapt.

Good IT training covers much more than phishing e-mails. It helps your employees identify security red flags across the board.

These include:

- Phishing e-mails and phone calls
- Poor or outdated passwords
- Malicious software hidden in links, attachments or online ads
- Poorly configured security on employee devices (a big deal for remote employees!)
- Lack of guidelines related to Internet or social media usage on employee devices
- Outdated software or hardware

Good training is also continuous. Cyber security training isn't a one-and-done deal. It's something you do every quarter or twice a year. Just as you keep your business's equipment maintained, you have to keep your employees' cyber security knowledge maintained. After all, your employees are your first defense against outside cyber-attackers. When they know what they're dealing with, they're better equipped to stop it in its tracks and protect your business.

The bottom line is that a lack of training is the biggest threat against your computer network and the health of your business. You need to have a strong training program in place to make sure your employees stay up-to-date. But you don't have to do it yourself. We can help. Along with your team, let's protect your business together.

SECTION 179 at a Glance

What is the Section 179 Deduction

Most people think the Section 179 deduction is some mysterious or complicated tax code. It really isn't, as you will see below.

Essentially, Section 179 of the IRS tax code allows businesses to deduct the full purchase price of qualifying equipment and/or software purchased or financed during the tax year. That means that if you buy (or lease) a piece of qualifying equipment, you can deduct the FULL PURCHASE PRICE from your gross income. It's an incentive created by the U.S. government to encourage businesses to buy equipment and invest in themselves.

Several years ago, Section 179 was often referred to as the "SUV Tax Loophole" or the "Hummer Deduction" because many businesses have used this tax code to write-off the purchase of qualifying vehicles at the time (like SUV's and Hummers). But that particular benefit of Section 179 has been severely reduced in recent years (visit www.section179.org, see 'Vehicles & Section 179' for current limits on business vehicles.)

However, despite the SUV deduction lessened, Section 179 is more beneficial to small businesses than ever. Today, Section 179 is one of the few government incentives available to small businesses, and has been included in many of the recent Stimulus Acts and Congressional Tax Bills. Although large businesses also benefit from Section 179 or Bonus Depreciation, the original target of this legislation was much needed tax relief for small businesses – and millions of small businesses are actually taking action and getting real benefits.

Here's How Section 179 works:

In years past, when your business bought qualifying equipment, it typically wrote it off a little at a time through depreciation. In other words, if your company spends $50,000 on a machine, it gets to write off (say) $10,000 a year for five years (these numbers are only meant to give you an example).

Now, while it's true that this is better than no write-off at all, most business owners would really prefer to write off the entire equipment purchase price for the year they buy it.

And that's exactly what Section 179 does – it allows your business to write off the entire purchase price of qualifying equipment for the current tax year.

This has made a big difference for many companies (and the economy in general.) Businesses have used Section 179 to purchase needed equipment right now, instead of waiting. For most small businesses, the entire cost of qualifying equipment can be written-off on the 2020 tax return (up to $1,040,000).

Limits of Section 179:

Section 179 does come with limits – there are caps to the total amount written off ($1,040,000 for 2020), and limits to the total amount of the equipment purchased ($2,590,000 in 2020). The deduction begins to phase out on a dollar-for-dollar basis after $2,590,000 is spent by a given business (thus, the entire deduction goes away once $3,630,000 in purchases is reached), so this makes it a true small and medium-sized business deduction.

Who Qualifies for Section 179?

All businesses that purchase, finance, and/or lease new or used business equipment during tax year 2020 should qualify for the Section 179 Deduction (assuming they spend less than $3,630,000).

Most tangible goods used by American businesses, including "off-the-shelf" software and business-use vehicles (restrictions apply) qualify for the Section 179 Deduction.

For basic guidelines on what property is covered under the Section 179 tax code, please refer to this list of qualifying equipment. Also, to qualify for the Section 179 Deduction, the equipment and/or software purchased or financed must be placed into service between January 1, 2020 and December 31, 2020.

For 2020, $1,040,000 of assets can be expensed; that amount phases out dollar for dollar when $2,590,000 of qualified assets are placed in service.

What's the difference between Section 179 and Bonus Depreciation?

Bonus depreciation is offered some years, and some years it isn't. Right now in 2020, it's being offered at 100%.

The most important difference is both new and used equipment qualify for the Section 179 Deduction (as long as the used equipment is "new to you"), while Bonus Depreciation has only covered new equipment only until the most recent tax law passed. In a switch from recent years, the bonus depreciation now includes used equipment.

Bonus Depreciation is useful to very large businesses spending more than the Section 179 Spending Cap (currently $2,590,000) on new capital equipment. Also, businesses with a net loss are still qualified to deduct some of the cost of new equipment and carry-forward the loss.

When applying these provisions, Section 179 is generally taken first, followed by Bonus Depreciation – unless the business had no taxable profit, because the unprofitable business is allowed to carry the loss forward to future years.

Section 179's "More Than 50 Percent Business-Use" Requirement:

The equipment, vehicle(s), and/or software must be used for business purposes more than 50% of the time to qualify for the Section 179 Deduction. Simply multiply the cost of the equipment, vehicle(s), and/or software by the percentage of business-use to arrive at the monetary amount eligible for Section 179.

If you lease, you pay only the monthly lease payments out of pocket and still get to deduct the full purchase price on your taxes.

Source = www.section179.org

The above is for informational purposes only and is not intended as tax or legal advice. Always check with your accountant or tax advisor to verify your eligibility for any tax deduction.

Improve Your Cash Flow With These Tips

Have Better Billing Processes – Make it as easy as possible for customers to pay their bills. Provide your customers with emailed invoices for quicker receipt. Be diligent about sending invoices ASAP after customers buy from you.

Get Cooperative – If it's possible or practical, work with other businesses to form a buyers' co-op. This gives you more buying power when buying in bulk.

Credit Check Customers – When dealing with higher-priced goods or services and a customer can't pay in cash, don't be afraid to run a credit check. Customers with poor credit can be a liability and cost you big.

Audit Your Inventory – Identify what costs you money by sitting around. If you're stuck with inventory that isn't moving, you may need to discount it to get rid of it.

Pay Online – Pay all of your bills online. This way you can select the exact date when those bills are paid each month, giving you more control over your cash flow.
SmallBiz Technology, Jan. 27, 2020

Top Ways To Prevent Your Remote Workers From Letting Cybercriminals Steal Your Data

1. Set expectations, rules and boundaries for employees, ensuring everyone is on the same page and held accountable.

2. Put together standard operating procedures for employees so they know what to do and who to call should anything go wrong.

3. Have a disaster recovery plan ready to back up and restore any system or data, should it become compromised.

4. Establish guidelines for employees, defining which approved devices and software they should be using.

5. Make sure those devices and software are routinely updated with the latest security patches.
Cyber Defense Magazine, June 3, 2020

3 Things You Can Do To Use Stress To Your Advantage

Embrace Deadlines – Research suggests we are the most productive with deadlines looming. Give yourself deadlines for everything. If you struggle with procrastination, move deadlines up in order to get things done.

Stress Yourself Out (On Purpose) – You can actually build a tolerance to stress. All you have to do is step out of your comfort zone and intentionally put yourself into stressful situations. You become more resilient to stressful situations and test your own boundaries at the same time.

Identify Stress "Weaknesses" – When stressed, identify what it is about a situation or task that is causing you stress. Then, focus on that cause and determine what you can do to mitigate it. It might mean reorganizing your day, such as reading and responding to e-mails at a different time. Or maybe you need more information on the issue you're dealing with, so do some research and see what you can find to help.
Inc., July 8, 2020

What Our Clients are Saying

Highly recommend! Very responsive, always resolves my issue, great customer service. I use their services for IT service and copier service.
Angel Wilkinson-Petry - Guardian Angel Financial Services, Inc.

BRANDON BUSINESS machines