RELIABLE IT BANKING

THE VAULT

Reliable IT Referral Program

We appreciate the opportunity to serve you and your referrals are one of the highest compliments we could receive. When you refer someone to Reliable IT, you trust us to deliver superior levels of quality and service to a company you respect as well.

We value your trust, and as a way to thank you for your referrals, we offer this incentive to our clients:

Introduce us to a new prospective client and if that client signs an agreement for Managed Services, you will receive the amount of their first monthly fee (minus 3rd party costs) credited to your company's statement for Reliable IT services, up to one month of *FREE* services, on your next bill.

For More Information, please contact:

Aaron Biehl at 866.634.3230 or Abiehl@RITBanking.com

February 2020

This monthly publication provided courtesy of Aaron Biehl, Chief Operating Officer, Reliable IT Banking.

We are a 24-year-old SOC 2 Managed IT, Security and Compliance Provider for Community Banks Nationwide. We provide monthly support to 40+ Community Banks representing 4500+ devices under management. Our standard of excellence includes personalized attention with a dedicated team, 24/7 live answer/monitoring, & on-going innovative engagements with your key stakeholders to ensure IT is effective, secure, and accelerates growth.

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.

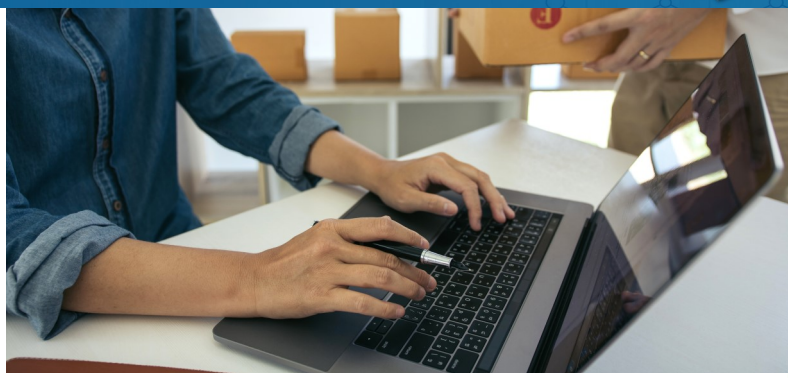
Continued on pg.2

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.

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



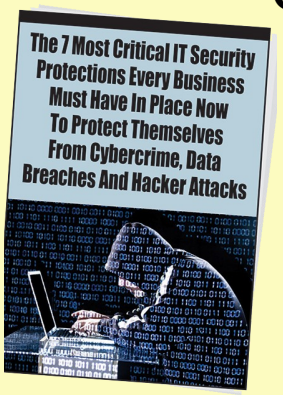
other networked equipment. Plus, they will make sure anti-malware software is working and is regularly updated.

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.

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

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



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.

Claim your FREE copy today at
www.RITBanking.com/cybercrime/

Client Testimony:

"Reliable IT understands the pressures of a community bank and they keep Security a Top Priority, which gives us reassurance that our partner values our bank's security, especially when emergencies strike."

Reliable IT has been a trusted advisor and partner for Golden State Bank for almost 10 years. I can always depend on the team at Reliable IT to offer informed recommendations on improvements and solutions to our existing IT issues. **They understand our process and can seamlessly integrate with bank core platforms, as they continuously stay on top of financial services technology trends, evolve with the changing technology landscape, and understand the regulatory and compliance requirements for the banking industry. They are a true value-add to our organization and growth.** Reliable IT always puts their clients first, as the helpdesk team goes above and beyond to ensure our staff's needs are met. Their senior engineers are top notch in their expertise and take a proactive approach to work, and we have never had an issue with response time to ensure our issues are resolved quickly.

Nikki Almazan, Vice President & Information Technology Director
Golden State Bank

6 Time Management Tips For The Busy Entrepreneur

Face it, there will never be enough hours in the day to accomplish everything you need to do. But if you methodically review how you spend your days and instill focus and discipline while completing daily priorities, you will soon find more time to work on the long-term success of your business. Here are six ways to do it.

1. CONDUCT A TIME AUDIT.
Sit down and review three months of activity. The data from the analysis will show where you spent your time (which projects, tasks and priorities demanded your attention) and with whom you collaborated to get the work done. The audit will also shed light on areas where you were distracted, where you were the most productive and which tasks/projects took more (or less) time than anticipated.

2. **ELIMINATE TIME DRAINS.**
These are the kinds of things that sneak up on you and steal time and can be better put to use growing your business. Look for these time drains: not delegating tasks, not managing meetings efficiently (Tip: always have an agenda!) and spending too much time writing/responding to e-mails. If you've done your job as a leader, members of your team can handle a majority of meetings and e-mails. You hired great people. Now let them do their jobs.

3. **TAKE CONTROL OF YOUR CALENDAR.**
Remember: you drive your schedule; don't let others drive it. Block time throughout your day and guard against changing your schedule to work on tasks that are not important or urgent. The way you allocate your time has a direct correlation to your effectiveness as a leader and, ultimately, the performance of your business. Prudent calendar management will also send a strong signal to your team that you take this seriously.

4. **PLAN YOUR DAY.**
When you know your priorities for the day, you will be better prepared to reset your work schedule if the unexpected comes your way. Once your schedule is set, block off chunks of time to work on your priorities. I recommend 90-minute blocks so you can concentrate on big-picture items or work on a group of related tasks. Stay disciplined and don't allow yourself to go over that allotted time.

5. **LIMIT INTERRUPTIONS.**
Now comes the hard part. Once you start working on each priority, you need to remain focused. Close the door and don't answer the phone unless it's a critical issue. Avoid checking e-mail. Don't let distractions slow you down.

6. **HOLD YOURSELF ACCOUNTABLE.**
Share your tasks, priorities and deadlines with a colleague. Meet with that person at least monthly to review how well you managed your time. The probability of success increases when you have someone watching your progress and coaching you across the finish line.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

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*

RELIABLE IT
BANKING

1540 Main St.
Suite 218, #107
Windsor, CO 80550

Inside This Issue:

To view previous newsletters, visit: **www.RITBanking.com/about/newsletter/**