The Tech chronicle

What's New?

Are you still using an old phone system with outdated features? Are you tired of missing calls when you are out of the office? Do you hesitate making a call from your cell phone due to caller id on the other end? Do you want to provide your employees with a true mobile office? Do you cringe when inclement weather hits because you can't into the office to change your voicemail message?

If you answered yes to any of those questions we need to talk. Our voice solution has a full feature set that will enable you to accomplish more than you could ever imagine.

September 2019

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business

Five Ways Smart People Blow The Close

The weirdest thing happens when it's time to close a deal. Smart people turn to mush! I've seen it a hundred times. Here are some of the common ways smart people blow the close.

1: HITTING MUTE

I was with a colleague in the boardroom of a billionaire CEO of the #1 company in his industry. Right after the CEO talked about the ways he wanted our help, my colleague had the chance to close the deal and help this great entrepreneur achieve his vision. Rather than bring it to a close, my colleague's mind hit mute. Silence. Twenty seconds of silence while the client expected to wrap up the conversation and close this deal! My colleague recovered, and we ended up with a happy outcome. Clients want help wrapping up a conversation and turning to an action plan. Don't just sit there! Close the deal!

2: IMPOSING

I was in another boardroom with a different colleague late in the day. My colleague did an amazing job of using reflective listening techniques to help the CEO identify his biggest leadership challenges. And then my colleague let the meeting end with no next steps. Afterward, I asked, "Why didn't you close him on the next step you want to take to solve the problems you just identified?" My colleague said, "I didn't want to impose! I didn't want to turn it into a sales call." "Impose?" I asked, "How is helping a

Continued on pg.2

Continued from pg.1

CEO solve his #1 problem imposing!" That one didn't turn out so well for us.

3: DAZZLING WITH COMPLEXITY

One of my colleagues is a ninja at turning a trusted advising conversation into an actual project. But she was not always this good! In the early days she talked at 90 mph, offering complex, nuanced analyses sprinkled with long, multipart questions. Her intent was to show how smart she was and dazzle clients into hiring us, but clients felt they couldn't get a word in edgewise. This is a common pitfall for smart people who come out of consulting backgrounds.

4. WINNING THE ARGUMENT

During a meeting, one of my colleagues put his hand up like a "stop" gesture in the face of our client. The consultant said, "Let me stop you there. I think your logic doesn't hold. Here is why …" The client was not impressed with the posture. Serving clients is not about winning arguments; it's about understanding the client and figuring out how to get them what they want. You are on the same team. If you forget this, you may win the argument but lose the deal.

5. STAYING SAFELY VAGUE

When I was hiring a law firm many years ago, I had a specific goal of designing an employee stock purchase program. I wanted to know the steps in drafting the plan, how long it would likely take and how much it would likely cost. The bad lawyers stayed "safely vague" or "Well, that all depends." I felt like saying, "Well, no kidding, but I'm trying to get a rough estimate of the time and cost of designing this plan." The good lawyers said things like, "I'm going to ask a few questions, and I'm happy to give you an estimate for how long this project might take, how much it's likely to cost, and I'll tell you the things that will affect the time and cost." Be specific. Clients like it when you offer specifics that will help them achieve their goals.

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 No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *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 BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*

Two Steps to Help Prevent Bank Account Fraud

Are you aware that your company's bank account is not afforded the same protections as a personal bank account when it comes to fraud? If a hacker takes money from your business account the bank is NOT responsible for replacing funds. Many people erroneously believe that the FDIC protects you from fraud but it does not; it only protects your business account from bank insolvency.

Before you can take additional steps to protect your cash assets you need to understand what, if any, coverage your bank offers. Ask your banking representative for the policy information regarding refunding money stolen from your business account to determine what applies to you specifically. After you determine your current coverage levels you can increase your protection to levels where you feel comfortable.

Here are two easy steps you can take to protect your business account from fraud:

Step 1: Insurance

Invest in insurance to protect you from fraud. This is one of the only ways to truly recoup money that is fraudulently taken from your business account.

Step 2: Monitoring

Set up e-mail alerts to receive notifications any time money is withdrawn from your account. The faster you catch fraudulent activity, the better your chances are of keeping your money. If you contact the bank immediately after any money is taken out, you have a very high probability of stopping hackers from robbing you. It may seem like a lot of extra emails but it's worth taking the time to review them if it can save your business from losing cash.

Cybercriminals Are Plotting To Hack Your Network—Here's What You Can Do To Prevent It

Did you know that small businesses are more likely to be targeted by cybercriminals than any other business or organization? Hackers love to go after small businesses for one very big reason: they are less likely to invest in top-notch (or even worthwhile) cyber security.

According to the Verizon 2019 Data Breach Investigations Report, 43% of cyber-attacks hit small businesses. Hackers go after targets they can profit from, by holding a business's data hostage and demanding a ransom (and get that ransom – hackers got $460,000 from Lake City, Florida officials after a ransomware attack on government computers), or by stealing customer data and either selling it on the dark web or using it for themselves.

But why are small businesses targeted so much? It's simply a numbers game. Hackers know most small businesses lack good cyber security and this makes these businesses easier targets. Target enough of them, and you're going to make money (from selling stolen data or paid ransoms).

So how can you protect your network? First and foremost, you have to realize YOU are a target. If you haven't been hacked before it just means the hackers haven't gotten to you yet. Once you realize this you can go to work and get your business ready for an attack.

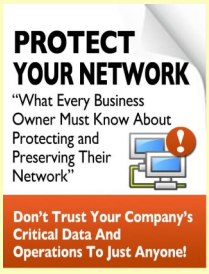
This is where a risk assessment can be beneficial. You may already have some security measures in place, but do you know how effective those measures are? You need to know where your holes are so you can plug them and then reinforce them. You don't want just a wall around your business, you want an entire ocean.

And it doesn't end there! One of the most powerful tools against hackers and cybercriminals is knowledge. Next to securing your business, the best thing you can do is train your employees on understanding cyber security and the threats that exist to harm the business they work for. Your team needs to be able to identify phishing schemes, fraudulent websites and virus scams and stay regularly updated on the threats out there. In addition, everyone in your organization should be using complex passwords that are locked away in a password vault or manager to add another layer of security.

"First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before."

Finally, make sure you are working with an IT team who knows what they are doing. It's one thing to tackle this all by yourself, as many businesses do, but it's another to work with an experienced IT security firm. If you go it alone you might miss something or you might not fully understand the security you have in place. Having an outsourced team of pros means you're one step ahead of the hackers.

Free Report: What Every Small-Business Owner Should Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



This report outlines in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.ccmgtech.com/protect or call our office at (267) 381-2025.