WCI Technology Insider

Insider Tech Tips – Written for Humans, Not Geeks

Building a StoryBrand
by Donald Miller

Communication is essential in the world of business. you will never see growth or success in your business if you can't communicate with your customers or other businesses. Whether you're writing copy for your website or promotions for your products, the language you use needs to be easy to understand while also making the reader feel like they're gaining something beneficial from it. Donald Miller's *Building a StoryBrand* can help any business leader communication better through their writing. This author aptly teaches his readers how to simplify a brand message for understandability as well as how to create effective wording for websites, brochures and social media.

August 2022

**Bill Wright
Founder &
CEO**

Our Mission:
Technology systems that anchor your business and protect what you have built, from a company inspired to make the world better.

Internet Safety Tips
for Parents

In today's climate, is there anything more prevalent than the internet? In fact, we've grown so accustomed to using it that the internet now seems to help us meet any need or want. Unfortunately, we don't often think about the effect that has on our kids, who have never known a world without this level of technology.

For the most part, the internet is an incredible boon to our children. They can look up anything they're curious about, and will be met with information than previously fathomed. Many of us remember visiting the library to research topics, and, even then, resources were limited compared to what can easily be found online today.

While the internet offers many benefits to our kids, there are also many risks. That's why it's important to keep them protected. Before your kids get a social media account, or dive headfirst into the web, take the following security measures.

Parental Restrictions
Nearly every device that can connect to the internet has some level of parental control available. With computers and laptops, you can restrict what websites and apps your children visit. You can also specify which websites you want totally blocked. This is an option on many tablets and smartphones, as well. With those, you can actually set time constraints and limits that make it so your child can only use the device for a certain amount of time, and you can even completely restrict usage at night.

... Continued from Cover

Potential Risks

When your children first start using the internet, you must ensure that they understand any potential risks. We all know people aren't always who they say they are on the internet. Similarly, not all information found online is true. When your kids visit websites or use apps, remind them not to share any personal information about themselves. They should never give out their address, school information, phone number, or even their email address to anyone online. Even if the person requesting this information claims to be someone they know, they might not be. If your child is using social media, inform them not to accept friend requests from people they don't know. It's important that kids understand all of the risks to ensure they stay safe in the digital and physical world.

Get Familiar

If your children are using the internet, you should become familiar with the websites and applications they use. Make sure all websites have the little padlock icon by the URL, which indicates that they are on safe websites. Look through the apps and websites your children frequent to ensure that these are safe for your children to use, and that they do not contain any inappropriate content.
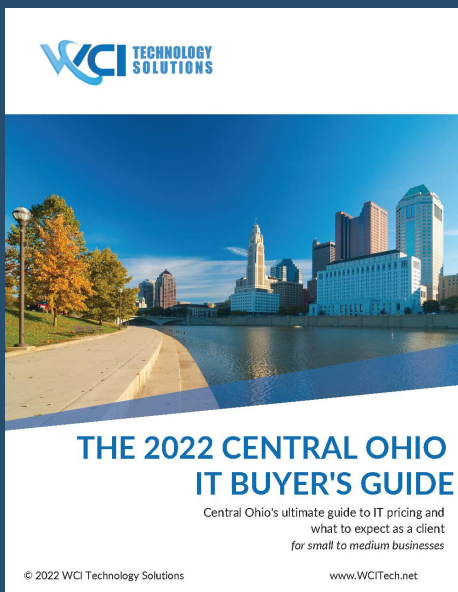
Lead by Example

Your children's first interactions with the internet will most likely stem from you, so do your best to set a great example for them.

This is your opportunity to model positive online habits for your children. Your social media posts should also be appropriate and not break any of the online rules you set for your own children. In their eyes, it won't be fair if you or someone else in the family can do things they cannot.

Our children are some of the most important people in our lives, so it makes sense that we would do everything in our power to keep them protected. Just make sure your protective efforts extend from the physical world into the digital world, as well.

"Your children's first interactions with the internet will most likely stem from you, so do your best to set a great example for them."

Tech Fact #1

As people become more suspicious of technology, new phobias develop. Technophobia is the fear of technology and cyberphobia is the fear of computers.

Tech Fact#3

In the 1950's, computers were called 'Electronic Brains'. Shall we stick with 'computer'?

Tech Fact #2

Want to know how old you were when the internet was born? Visit www.howoldistheinter.net

Bill's Favorite Business Gadget of the Month

If you want to upgrade your webcam without spending a lot, you can use your phone's camera. But, you'll also need a good tripod to hold it.

The Joby GripTight ONE is a great option. It's under $50, has bendy, flexible legs, magnetic feet, and is small enough to carry from home to the office.

WCI TECHNOLOGY SOLUTIONS

Inspirational Quote of the Month:

"Technology will never replace great teachers, but technology in the hands of great teachers is transformational."

- George Couras, Innovative Teaching, Learning, and Leadership Consultant

August's Featured Everyday Gadget:

Oura Ring Generation 3

For the past few years, fitness trackers have become all the rage. Between Fitbits and the Apple Watch, nearly everyone has, or is at least familiar with, fitness trackers. One of the most common complaints about many fitness trackers is comfort. Oura decided to take the wristband out of the equation with the Oura Ring. The Oura Ring is a fitness tracker that you wear on your finger. It tracks sleep, activity and readiness measurements. This device is even more accurate than other fitness trackers since the finger is a better spot to record heart-rate data. Through temperature sensors, a library of informational resources and much more, the Oura Ring is the perfect fitness tracker for just about anyone who is looking to improve or maintain their physical health.

3 Ways to Run Meetings Like a CEO

In my opinion, most meetings are a complete waste of time. Although the relayed information might be important, it isn't always delivered in an effective way, since most managers do not know how to run meetings. Successfully leading huddles or meeting is an important part of building great relationships and leading talented teams. If you want to start getting more from your employees and your meetings, try utilizing the following three methods to run your meetings like a CEO.

Always Request an Agenda

Early in my career, an acquaintance invited me to a business lunch. I can remember wondering, "What does he want to talk to me about?" After a little bit of small talk, he unveiled his agenda. He wanted to sell me a new insurance policy. It ended being a huge waste of time for both of us. After that meeting, I made sure to only accept invitations that had an agenda - this comes with three distinct benefits.

The first is the fact that you can see what will be discussed in the meeting, and you can decline the invite if it doesn't pertain to you or your work. The second is that you can actually prepare for the meeting. The final benefit is that it makes you appear competent. Since you can come prepared, it will look like you have everything under control.

Ask Questions and Avoid Talking Too Much

One of the biggest mistakes managers make when leading a meeting is trying to dominate the conversation. You may be thinking, "Aren't CEOs supposed to tell their attendees what to do in meeting?" The answer is no; the great CEOs don't. In fact, the best CEOs will spend their time asking questions that are strategic, reflective and related to accountability. This help them brainstorm new ideas with their team, ensure everyone is on the same page and put the responsibility on others so they can follow up in the future.

Discuss, Debate and Decide

The beginning of your meetings should focus on your strategy and what needs to be discussed. After a topic is introduced, CEOs will say things like, "Let's debate what we should do about this. Who has some ideas?" That brainstorming will help develop the best solution, and the CEO will then make a decision about what to do, or who should handle each responsibility. Your meetings need to be focused on production. If you give people the freedom to speak openly, you will accomplish much more.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple *New York Times* best sellers. He stays active in his community and has advised many government officials.

Who else is sick of spam?

For business owners, spam is bad news.

Not only is it annoying, but it's also eating up hours of your team's time each year. In fact, it's estimated that people who get more than a hundred emails every day could be losing around 80 hours of their time each year, sorting out spam.

As well as the impact on productivity, have you considered how else it might be harming your business?

For example, how many of the emails that you send out - especially your marketing messages - are being marketed as spam?

Spam filters give each email a score based on the sender reputation, domain name and many other factors. They also read the emails to spot common words and phrases used by spammers.

Using one "spammy" word in an email isn't a disaster in itself. But using too many can give you a higher spam score, and your message could be filtered into the spam folder.

Try not to use things like '$$$' or 'free money'. Other flagged words and phrases are more surprising - 'being a member', 'free trial', 'unlimited', and even 'amazing'.

Next time you're creating a marketing email, take a moment to consider how spammy your email could be perceived before you hit send. Staying out of the spam folder improves deliverability and open rates.

Did You Know

paying ransomware makes you a bigger target?

Ransomware is evil. It's where your data is encrypted until you pay a ransom fee to get it back.

Many business owners say they'd pay the fee to resolve the problem quickly. But doing that can make your business an even bigger target for attacks.

80% of ransomware victims who paid up were then hit a second time by the same attackers.

Whoa.

The greatest defense against ransomware is being 100% prepared. You need a working and verified backup, a ransomware resilience plan, and all the right security measures in place BEFORE you are attacked.

Are you blacklisting or whitelisting?

New to Windows 365

Hit send too soon in Outlook?

We've all accidentally sent an email before it was ready. Or sent it to the wrong person.

And while Outlook's recall is a popular feature, historically it hasn't always worked. It was only reliable if the recipient used Outlook, too.

Great news. An update due for release next month will make email recall work regardless of where the recipient gets their email.

You know what it means to be blacklisted, right? (we don't mean through personal experience, of course).

Blacklisting is where you block something you don't trust. It's used to keep networks and devices safe from bad software and cyber criminals.

But, there's another, safer way of doing that - and that's called whitelisting.

Rather than trying to spot and block threats, you assume everyone and everything is a threat, unless they've been whitelisted.

But, which is the right approach when it comes to keeping your business safe? This debate rages on, with many IT professionals holding different views.

Here are the main differences...

- Blacklisting blocks access to suspicious or malicious entities
- Whitelisting allows access only to approved entities

- Blacklisting's default is to allow access
- Whitelisting's default is to block access

- Blacklisting is threat-centric
- Whitelisting is trust-centric

There are pros and cons to each approach. Whilst blacklisting is a simple, low maintenance approach, it will never be comprehensive as new threats emerge daily. It's also easy to miss a threat, as cyber criminals deisgn software to evade blacklist tools.

Whitelisting takes a stricter approach and therefore comes with a lower risk of access. But, it's more complex to implement and needs more input. It's also more restrictive for people using the network and devices.

Confused? You're not alone! If you'd like to discuss which approach is best for your business, get in touch.

Technology Update

Not just content to fill our roads with his electric vehicles, now Tesla's Elon Musk is about to demonstrate a household robot.

The humanoid Optimus robot (aka the Tesla Bot) will be able to take on the repetitive and dangerous tasks that people hate. It'll be 5'8" tall, will carry up to 45 lbs, and walk at 5 mph.

Sounds like a perfect shopping companion....

Elon's shifted his planned AI day from later this month to the end of September. He hopes to have a working prototype ready to show us.

Which hated household tasks would you handover to a Tesla Bot? Could you see a use for it in your workplace?

Who will be this month's quiz winner?

Place your bets now, please

1. **How many programming languages are currently in use?**
2. **What's the name of a website designed just to be used for sharing information inside a company?**
3. **Which mobile operating system does Google control?**
4. **What does PDF stand for?**
5. **What is a computer trojan a form of?**

Question

How can I avoid being phished?

ANSWER
The best thing is treating every email with caution. If you're unsure, check the address its been sent from, look for grammatical errors, and see if the layout looks like a normal email from that person or company. If you're unsure, don't click any link.

Question

What's an insider threat?

ANSWER
It's the name for when someone within your business gives cyber criminals access to your devices or network. Usually, it's not malicious. But it's why regularly training your team in cyber security is a must.

Question

How do I choose the right backup for my data?

ANSWER
Security and reliability should be your main considerations. Get in touch and we'll tell you what we recommend.

Quiz Answers

1. IT'S REALLY HARD TO SAY. WIKIPEDIA HAS A LIST OF ABOUT 700, BUT SOME PROGRAMMERS CLAIM THERE ARE UP TO 9,000 LANGUAGES IN ACTIVE USE
2. AN INTRANET
3. ANDROID
4. PORTABLE DOCUMENT FORMAT
5. MALWARE

WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech

Tech Trends to Improve Customer Loyalty

If you want your business to succeed, you must build a solid customer base. Over the past few years, advancements in technology have made it easier for their companies to improve their relationships with their customers. One such way is through the use of AI chatbots. If someone has a question about your service or product, you don't want to leave them waiting for an answer. Chatbots can be programmed to answer common questions until a live representative is available, if they're even needed.

Additionally, you should make an effort to monitor content created by people outside your company. If someone is spreading false information about your business, you need to combat it. If disinformation is allowed to fester, it can quickly sink a small business. Simply replying to misinformed reviews or reporting inappropriate content about your business can go a long way toward becoming a more trustworthy source in your industry.

4 Ways to Better Protect Your Personal Information

Most people keep their personal information as secure as possible. They don't post their passwords on social media, or share Social Security numbers with untrustworthy sources. These practices seem obvious, but there are smaller things we can do to provide better protection. You'll find four or those tactics here:

Dangers of Unsecured WiFi - Hackers can use this connection to download malware on your devices.

Password Manager - You shouldn't use the same password between multiple accounts. Utilizing a password manager will help you keep track of different passwords.

Breached Companies - When a company's security is compromised, all of its customers' personal information can be exposed. Avoid working with these companies until they've offered improved security.

Think Before Posting - Be careful about what you share on social media. Revealing too much personal information can leave you vulnerable to a cyber-attack.