

The Tech chronicle

Vishing

No, not a typo, Vishing is short for voicemail phishing.

It's not an actual voicemail, but an email that points to a saved voicemail online.

"Voicemail-themed phishing campaigns continue to be a successful social engineering technique for attackers since they are able to lure the victims to open the email attachments..." - Zscaler

It is important to know what type of threats are out there so we can all be better informed to take appropriate action.

August 2022



This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.



Creating A Safe Online Presence For Your Children *In 4 Easy Steps*

Children in this day and age are growing up in a technological climate that many of us never could have imagined 20 years ago. Kids who were born during the last decade will never know a world where everyone doesn't have a cellphone on them at all times. They'll never truly understand what the world was like before the Internet.

This rapid development of technology has made it so our kids' online and offline lives are merged into one. The conversations they have on social media or over texting are the exact same as the conversations they would have in person. They have direct access to just about anyone at a moment's notice and can see

directly into other people's lives through social media. Additionally, many kids are stumbling upon graphic content and some pop-ups are even encouraging them to click on inappropriate material.

To put it simply, it's becoming much more difficult to keep our children safe online. They're able to share information, pictures and videos at a moment's notice, and oftentimes, the parents are unaware their children are participating in these behaviors. Considering that 40% of American children receive cellphones before they turn 11, it's important that parents do everything in their power to ensure their children stay safe online.

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website
www.ctmaryland.com or call 240-399-9600

Continued from pg.1

If you're unsure of what steps you need to take to ensure your children's safety online, don't worry - we've got you covered.

Slowly Introduce Digital Media.

Fostering a safe online environment for your children starts at an early age. They should be introduced to the online world when they're young and taught the safest way to use it. Once they've been introduced to the Internet, set time constraints and do everything you can to ensure their technological devices aren't interfering with their sleep.

Think Before You Post.

Many children will get their first experience with social media thanks to their parents, so lead by example by making appropriate, safe posts that do not reveal personal information. There should be no graphic or mature content on your feed as well, especially if it's public.

"40% of American children receive cellphones before they turn 11."



Encourage The Use Of Strong Passwords.

Make sure your children know how to create strong passwords as well as the dangers of having a weak password. Teach them to use different passwords for each account and to never share their passwords with anyone outside of the family.

Set Up Parental Controls.

Parental controls are great when it comes to streaming services and computers, but did you know that most smartphones also come with parental controls? On your child's smartphone, you can set parental controls for time limits as well as content restrictions. You can even choose which specific websites they're allowed to visit while blocking everything else. This is a great way to prevent them from stumbling upon inappropriate or harmful content.

The Internet can be an informative and enjoyable place for your children if you take the proper precautions. Teach them the basics of the Internet and preach safety above all else.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This ...

INTRO TO CLOUD COMPUTING

"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud"



Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get your **FREE** copy today:
go.ctmaryland.com/cloudreport

General Motors

Do you own a Chevrolet, Buick, GMC, or Cadillac?

Be aware that GM recently acknowledged that they fell victim to a credential stuffing attack a little over a month ago.

The company said that they detected suspicious network activity between April 11th and April 29th of 2022.

Some items that were affected were first and last name, email address, physical address, username and phone number of registered users, OnStar package subscriptions, profile pictures, search and destination information and more.

Other less useful information was car milage history, service history, Wi-Fi Hotspot settings, emergency contact information and the like.

As breaches go, this one wasn't as bad as many of the others we've heard about thus far this year.

However, armed with the information above, a hacker certainly have enough details to steal someone's identity.

Be warned and stay vigilant. I know it gets old, but change your passwords, don't recycle or repeat your passwords, make them complicated, don't share your passwords. Stay Alert!

4 Ways Smart People Blow The Close



Picture this scenario: You've been working closely with a potential client for the past few weeks. During that time, you've been proactive and communicative. Anything that client needed, you took care of, but when it comes time to officially close the deal, something happens that makes the client unsure of whether they want to proceed with your business or not.

This is a situation I see all the time. I work with incredibly smart people who get asked to help some of the most successful CEOs and boards in the world solve their top leadership problems. When my colleagues are actively doing the work, they appear to be confident, caring and, at times, daring. But when it comes time for them to sell the work, many struggle.

Over the years, I've witnessed four common ways smart people fail to close deals.

Hit Mute

I recently had a meeting with a billionaire CEO who was at the peak of his industry. He told me and my colleague about his concerns about hiring and leading talented teams across his portfolio of businesses. This was an easy sell for us. After the CEO talked for about an hour, he asked my colleague a

question to wrap up the conversation. Instead of answering promptly, my colleague's mind went blank and he didn't recover for 20 seconds. Though we recovered in this situation, clients want help wrapping up a conversation and turning it into an action plan.

Don't Impose

I sat in on another meeting with a different colleague and CEO that went really well. My colleague was providing valuable and insightful advice in this meeting but let the meeting end without making an action plan or closing the deal. I asked him why he didn't close, and he said he didn't want to impose. We ended up giving this CEO hours of free help before he officially hired us.

Too Complex

An issue that many smart people face is being overly complex and dominating the conversation. They have this desire to prove how smart they are and try to prove it in these meetings. When you try to overpower the conversation while discussing complex topics, you end up overwhelming or even insulting the client. Slow down and be conversational.

Win The Argument

When you're trying to close a deal, the conversation should not be argumentative. I once sat in on a meeting where my colleague put his hand up and told our client, "Stop right there. I don't think your logic holds." It did not go over well. To serve your clients, you need to understand and respect them.



Dr. Geoff Smart is chairman & 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.

■ Using Tech To Improve Your Customer Service Experience

Customer service expectations have grown over the last few years, and businesses have had to adapt to meet the needs of their customers. Here are a few ways that tech can be implemented to improve the customer service experience.

For Communication: You can program a chatbot to respond to customers' immediate needs or questions on your website or app.

For Interaction: With the use of augmented or virtual reality, you can demonstrate how a product will look or work for your customers.

For Personalization: Through certain automation programs, you can ensure that your e-mails appear as if they were tailored for each customer.

■ The Growing Threat Of Ransomware

As the COVID-19 pandemic continues to slow down, technology experts fear that the next major issue to affect our country will come from the digital world. Throughout the pandemic, ransomware attacks have increased 500% and don't seem to be stopping anytime soon.

Ransomware attacks occur when a hacker installs software on a network that prevents the owner from accessing any of their devices or data. They essentially hold

the business hostage as they demand a ransom payment. To combat this, your business needs to put some cyber security practices in place to prevent ransomware attacks. This includes implementing offline backups and keeping your software up-to-date.

■ The Best Tech Helps Attract And Retain Talent

The technology your company uses has always been important in attracting experienced and talented employees, but it has become even more important with remote and hybrid work. Very few employees will want to work remotely for a company that doesn't provide any of the basic tech needed to perform their role. A recent study by Barco, Inc. found that 1 in 3 hybrid employees say that one of the top factors in searching for a new job is their frustration while dealing with tech issues. If you want to retain your top talent, you need to provide your team with the tech needed to perform their daily duties, check on them to make sure they have everything they need and even the playing field between your remote and in-office employees.



I didn't see any compliance issues.

CartoonStock.c