PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions August 2022

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 communicate 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. Miller's book is a helpful resource for anyone who is trying to effectively communicate with their potential customers.

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

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 more 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 for kids, there are risks. That's why it's important to keep your children 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. 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

continued on page 2

completely restrict usage at night.

Potential Risks

When your children first start using the Internet, you must ensure 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 e-mail 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 them, which indicates they are safe websites. Look through the apps and websites your children frequent to ensure they're safe for them to use and 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 child. 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."**

Cartoon of the Month

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 of 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.

URGENT MESSAGE FROM OUR CEO

This is an urgent message to Business Managers and Firm Administrators to pay close attention when completing your cyber insurance questionnaires and surveys.

Recently, industry behemoth Travelers Insurance, asked a judge to rescind a policy due to misrepresentations by their client on their Cyber Insurance Questionnaire. In particular, they checked a box that they thought was correct ("Are all Admin accounts using multifactor authentication?"). As it turned out, their internal IT team was not compliant thereby allowing hackers to infiltrate the company. The CEO signed the form but it's unclear whether he received advice from his IT team to validate the form before it was sent to the carrier.

Obviously, this will be a multi-million dollar claim that this particular business may not be able to financially survive. I bring this up because these questionnaires are becoming more complex and nuanced. Quite often, we are not consulted before they are returned to the insurance company. We offer this advice as a free service and are happy to help anyone complete them properly.

In the article on page 4 of this newsletter entitled **"3 Times Businesses Were Denied Cyber Insurance Payouts,"** we've included three incidents in the news that I feel all business owners need to be aware of.

Please contact us if you would like to review any past questionnaires you have already signed (it's not too late to solve if you have not had a claim) or any you may receive in the future.

Yours for a more secure world,

Chuck Poole, CISSP
CEO
PalmTech Computer Solutions

3 Times Businesses Were Denied Cyber Insurance Payouts

Cyber insurance is a type of insurance that protects businesses from financial losses that can result from a cyberattack. While it's an essential tool for businesses of all sizes, there are some facts you should be aware of before purchasing a policy.

Just because you have cyber insurance, it doesn't mean you are guaranteed a payout in the event of an incident. This is because you may not have the correct coverage for certain types of cyberattacks or you might have fallen out of compliance with your policy's security requirements. As a result, it is critical to carefully review your policy and ensure that your business is adequately protected.

Learn From The Past

Here are three real-life examples of denied cyber insurance claims:

Cottage Health vs. Columbia Casualty

The issue stemmed from a data breach at Cottage Health System. They notified their cyber insurer, Columbia Casualty Company, and filed a claim for coverage.

However, Columbia Casualty sought a declaratory judgment against Cottage Health, claiming that they were not obligated to defend or compensate Cottage Health because the insured didn't comply with the terms of their policy. According to Columbia Casualty, Cottage Health agreed to maintain specific minimum risk controls as a condition of their coverage, which they then failed to do.

This case reminds organizations of the importance of reading their cyber policy, understanding what it contains and adhering to its terms.

BitPay vs. Massachusetts Bay Insurance Company

BitPay, a leading global cryptocurrency payment service provider, filed a $1.8 million insurance claim, but Massachusetts Bay Insurance Company denied it. The loss was caused by a phishing scam in which a hacker broke into the network of BitPay's business partner, stole the credentials of the CFO of BitPay, pretended to be the CFO of BitPay and requested the transfer of more than 5,000 bitcoins to a fake account.

Massachusetts Bay Insurance stated in its denial that BitPay's loss was not direct and thus was not covered by the policy. Massachusetts Bay Insurance asserted that having a business partner phished does not count as per the policy.

Although BitPay is appealing the denial, this case emphasizes the importance of carefully reviewing insurance policies to ensure you understand what scenarios are covered. This incident also highlights the importance of employee security awareness training and the need to reach out to an IT service provider if you don't have a regular training policy.

International Control Services vs. Travelers Property Casualty Company

Travelers Property Casualty Company requested a district court to reject International Control Services' ransomware attack claim. The company argues that International Control Services failed to properly use multifactor authentication (MFA), which was required to obtain cyber insurance. MFA is a type of authentication that uses multiple factors to confirm a user's identity.

Travelers Property Casualty Company claims that International Control Services falsely stated on its policy application materials that MFA is required for employees and third parties to access email, log into the network remotely and access endpoints, servers, etc. They stated that International Control Services was only using the MFA protocol on its firewall and that access to its other systems, including its servers, which were the target of the ransomware attack in question, were not protected by MFA.

This case serves as a reminder that when it comes to underwriting policies, insurers are increasingly scrutinizing companies' cybersecurity practices and that companies must be honest about their cybersecurity posture.

Travelers Property Casualty Company said it wants the court to declare the insurance contract null and void, annul the policy and declare it has no duty to reimburse or defend International Control Services for any claim.

Do Not Be Late To Act

As we have seen, there are several reasons why businesses can be denied payouts from their cyber insurance policies. Sometimes, it could be due to a naive error, such as misinterpreting difficult-to-understand insurance jargon. In other cases, businesses may be maintaining poor cybersecurity hygiene.

An IT service provider can help you avoid these problems by working with you to assess your risks and develop a comprehensive cybersecurity plan. Feel free to reach out for a no-obligation consultation at info@palmtech.net or 561-969-1616.