6 Examples of Phishing Attacks Area Businesses Need to Prepare For
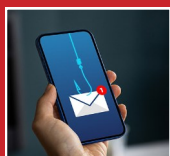
Phishing is one of the most prevalent forms of cyberattacks out there today, taking many forms and affecting everyone from individuals to entire organizations. Any business operating today needs to be aware of the numerous shapes that phishing can take.

Here are six common examples...

Read the Rest Online!
https://dti.io/6exphishing

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

Four Strategies to Help Build Robust Cybersecurity

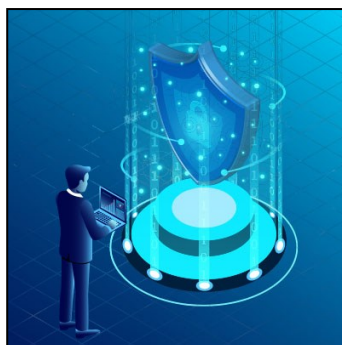Your business' IT security effectiveness relies heavily on how well your technology works. With this in mind, educating your staff on their responsibility to safeguard your business' digital assets is important. Let's explore the key priorities businesses need to consider to establish a robust security training platform that works to protect those assets.

Your Security Posture

You might have encountered the term "security posture," indicating how proactive an individual is in protecting themselves online. With the prevalence of cloud-based applications and the increasing adoption of remote work, employees play a vital role in organizational cybersecurity.

Here are four considerations to guide your cybersecurity strategy:

Get Employees Engaged

Making network security engaging for individuals outside the security domain requires creativity. Relatability is crucial; use real-world examples in educational materials to connect with employees who may have experienced identity theft or data leaks. Demonstrate that the measures to protect the company align with actions taken to

Cyber Censorship is a Complicated Issue
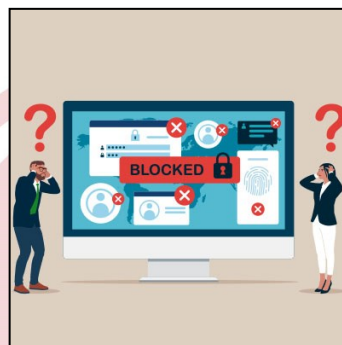
The web is filled with all types of content, and depending on where you live, it can be regulated by a myriad of organizations from all sections of society. From internationally recognized trade organizations to governments to industry regulators, there are a lot of moving parts in data regulation as it now stands. That leads to people wanting more control over data and censorship. Let's take a look at cyber censorship and how it's a bigger issue than you might think.

Where Do You Find Cyber Censorship?

Cyber censorship can be found in various forms and locations, often manifesting within authoritarian regimes where governments seek to control and suppress information to maintain power. It is prevalent in countries like China, where the Great Firewall restricts access to certain websites and monitors online activities. Some democracies also engage in selective censorship for national security reasons, raising concerns about the balance between freedom of expression and security. Corporations and social media platforms may also implement censorship policies to comply with community guidelines, significantly impacting the flow of information.

Why It Isn't Always Bad?

It can be argued that certain instances of censorship are necessary to maintain societal order and security. Cyber censorship can play a crucial role in preventing the spread of harmful and malicious content, such as hate speech, extremist ideologies,

"Don't be pushed around by the fears in your mind. Be led by the dreams in your heart." — Roy T. Bennett

How to Choose the Right Security Cameras for Your Business

So, you're thinking about adding to your business' security with a camera system. This is an excellent course of action for any business to take—provided that it is approached thoughtfully and with discretion. There are many, many options out there, after all, which only makes it more challenging to make the right choice.

That's (part of) why Directive is here: to help area businesses make the right choices when it comes to their business technology, including their security camera systems.

Selecting the Right Security for Your Business Isn't Always Easy

Like I said, there are a lot of options and variables that you need to consider. First off, you may be tempted to turn to a system designed for residential protection. I urge you not to succumb to this temptation. Much like you shouldn't trust a consumer hard drive for your business' backup needs, turning to a consumer-focused device for your security is a gamble that ultimately isn't worth the...

Read the Rest Online!
https://dti.io/bizcam

How Scammers Try and Steal Your Business' Data
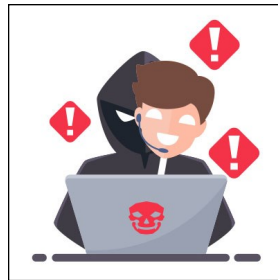
Picture this scenario: while going about your daily routine, an email lands in your inbox, purportedly from a cybersecurity company. The alarming claim is that you've become the target of a hacking attack. Despite lacking IT expertise and being unfamiliar with your security agency's protocols, you trust the message and promptly respond. Little do you know, the email is a cleverly disguised cyberthreat, and you find yourself ensnared in their trap.

Beware of Cyberthreats Posing as Cybersecurity Companies

It may sound unbelievable, but hackers have the audacity to impersonate cybersecurity firms and other trusted entities, attempting to deceive even the most vigilant. There have been many phishing campaigns where cyberthreats masquerade as security software. In this scheme, unsuspecting users called a fake helpline seeking support, unwittingly allowing the hacker to remotely access their computer.

The unsettling part is that it could appear legitimate to someone who didn't scrutinize the message closely. The deceptive email discusses outsourced security providers, a common practice today, abnormal activities, and potential compromise—elements that could be misconstrued as valid. The fraudulent email includes a case number and contact details to address the supposed concern. When the victim contacts the provided number, the hacker installs a remote access tool on their device, granting them unhindered access at their discretion.

Uncovering the Motive

The motive behind such attacks varies from case to case. It could be an attempt to infect systems for future remote access or to profit by selling access to compromised devices to the highest bidder. Regardless, it's a perilous situation that demands caution.

What to Do?

In nearly all instances, your security...

Read the Rest Online!
https://dti.io/datascam

Four Strategies to Help Build Robust Cybersecurity

safeguard personal data.

Keep Promoting Security

People are impressionable, and a security-rooted company culture can significantly impact employee behavior. Consistently emphasizing the importance of comprehensive security will resonate with your staff and get them to subconsciously consider doing the things to keep from running afoul of IT administrators' attempts at securing a network.

Train and Test

Pushing the security agenda is essential,

but it must be coupled with training tailored to address specific issues. Employees need to grasp concepts such as avoiding phishing, understanding network resources, recognizing their role in data protection, practicing solid password management, and knowing how to respond to security mistakes. Regular testing goes a long way toward growing security awareness and understanding...

Read the Rest Online!
https://dti.io/buildsecurity

Cyber Censorship is a Complicated Issue

(Continued from page 1)

and misinformation. Restricting access to content like this makes it possible to protect individuals and communities from potential harm. It can also contribute to safeguarding national interests, preventing cyberattacks, and maintaining a stable online environment.

What are Your Rights?

Preserving the freedom of expression is crucial to life online, and advocating for the right to bypass cyber censorship ensures an open exchange of ideas. Individuals can access diverse perspectives and information

by promoting tools and technologies enabling users to circumvent censorship. By empowering people to make informed decisions and engage in open discourse, individuals can strengthen democratic principles and build a more substantial and inclusive online life.

Censorship is one of those issues that is extremely divisive. In fact, nearly three-of-four people surveyed in a current poll think that many of the massive tech companies that people

Share this Article!
https://dti.io/cybercensor

Remember World Backup Day is March 31st

World Backup Day, observed on March 31st annually, serves as a designated occasion to underscore the critical importance of regular data backups for ensuring data continuity. Although this day effectively highlights a fundamental best practice, we firmly advocate for a continuous commitment to maintaining and safeguarding backups rather than confining such awareness to a single day.

To fortify your understanding of optimal backup procedures for your business data, let's go into some key best practices derived from the lessons of World Backup Day.

The central concept behind World Backup Day is straightforward: To instill a culture of routinely backing up data while underscoring its significance. At the core of a robust backup strategy lies adherence to the widely acknowledged 3-2-1 Backup Rule.

The 3-2-1 Backup Rule can be succinctly summarized as follows:

- Ensure you possess at least three copies of all your data. One of these copies functions as your operational copy, the primary dataset you work from, while the other two serve as backups.
- Store your backup copies separately from your operational data, utilizing at least two distinct storage mediums to enhance redundancy.
- Maintain at least one copy of your data in an offsite location, preferably in the cloud, to guard against site-specific emergencies.

Implementing these principles aligns with the essence of World Backup Day and establishes a robust framework for safeguarding data in emergency scenarios.

Share this Article!
https://dti.io/backupday2024

Marketing Ideas & Tips for Your SMB

6 Essential Tools to Bring Marketing Back to Your Website

Your website is the roadway for all digital information about your company's services, products and vision. Leveraging your website to generate and convert leads is pivotal in today's digital landscape. In this article we will discuss six marketing tools that, when utilized adeptly, can guide potential customers directly to your digital doorstep.

1. Social Media Platforms
Utilizing social media - including Facebook, Twitter, LinkedIn and Instagram - can expose your business to new audiences. It's crucial to see social media not just as a standalone platform but as a component of your marketing funnel. Use these platforms to share engaging content from your website, like your blog articles, incorporating links to drive traffic back to your site.

2. Email Marketing
Email remains a potent tool to attract visitors to your website. Now, to be clear...

**Read the Rest Online!**
https://dti.io/bringmktbac

Employee Spotlight: Devin Chase

This month, we wanted to show our appreciation to someone who's been here from the beginning: Devin Chase, our Vice President of Sales and Cybersecurity Officer. Raised right here in the City of the Hills, Devin learned everything he knows through real-world experience. Born to the CEO and COO of our company, he was raised around technology and fostered an interest in it as a result. He started as a tech, working on networks in high school, but moved to sales after realizing he was more drawn to that aspect of the work.

Now, Devin draws on his tech history to approach his sales work with a greater appreciation and understanding of the process. He also gets to see clients satisfied with the services they've received, something that IT techs don't usually get to see. Devin's time with Directive has been punctuated with happy memories of time spent working with his parents and helping his community. According to him, the benefit that local charities see from his efforts makes all the hard work worth it. Outside of work, Devin enjoys outdoor activities... hiking, spending time on his motorcycle, and spending as much time with his family as possible.

Devin wants to remind everyone to avoid oversharing on social media (and to always have their cybersecurity cap on, in general). He also encourages everyone to invest in a 529 education plan for their kids. Thank you for everything you do for us, Devin!
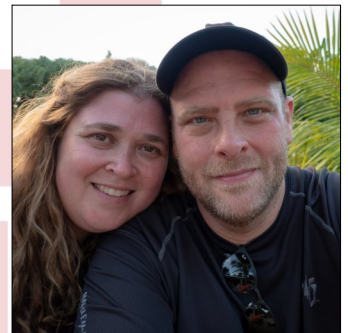
Chris (CEO) and Charlotte (COO) Chase

Tech Trivia
49% of people think that wearable technology boosts productivity.

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com

facebook.directive.com

linkedin.directive.com

x.directive.com

blog.directive.com

instagram.directive.com

I'M BEGINNING TO THINK YOU AREN'T WORKING ON A SPREADSHEET.