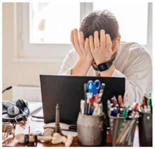
directive

TECHMinutes
June 2020
Your Small Business Technology Information Source!

This Issue:

The Employee's Guide to Working

The Employee's Guide to Working Remotely



It's not uncommon where a situation arises and you will find yourself working from home. To make this work, it is important that you keep a few additional issues in mind so that you can make the most of it. We have put together a few simple best practices that you should keep in mind as you operate remotely.

Security Considerations
Even though you aren't in the office, you still need to follow the same security protocols and the processes you would need to follow if you were working in the office…

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

25+ YEARS IN BUSINESS
est. 1993

2-Factor, 2-Furious - How 2FA is Our Last Hope

Two-factor Authentication, also referred to as Multi-Factor Authentication, or 2FA, is typically where you log in to something and have to type in a small code from your mobile device in order to finish the sign-in process. It's really the only thing protecting your accounts anymore, so it's critical to use it.

If you haven't seen or used 2FA by now, it will probably feel like something that Maxwell Smart (from 1965's Get Smart) would use to get into his fancy car (in the series, Max Smart is a super techy government agent who is big on goofy security gadgets - self destructing messages, shoe phones, and hidden cameras. I digress, but, 2FA makes you feel like you are stepping into the Pentagon with security clearance when you are simply logging in to your Facebook. That is, it feels that way the first time you have to do it. After that, it's more of a chore.

An important chore, mind you.

How Does 2FA Work?

When you log into a network or an account (like your bank account, your Amazon account, your email, Facebook, etc.) you need to use a password. Most people don't use different passwords across all of their accounts (although they desperately need to) and because of this, if one organization gets breached, hackers can figure out how to get into your other accounts because they have your one overused password.

(Continued on page 2)

Small Businesses Face Hard Work Getting Back to Normal

It isn't exactly business as usual, but things are beginning to resemble the reality we all knew before COVID-19, thanks to the use of cloud services as a means to continue processes while social distancing is still in play. However, some businesses may still be reluctant to embrace them.

Let's go over what cloud services are, their varieties, and how they can directly benefit your business.

What are Cloud Services?

Cloud services are a specific way of obtaining computer resources, making use of the Internet to do so. While "the cloud" invokes the image of the fluffy white things in the sky, in this context, "the cloud" actually refers to hardware, usually a server, that someone else is hosting for you. A user can connect to this server over the Internet and access the contents of this server.

This setup has proven to be quite beneficial for businesses to use in a variety of ways, serving to provide improved flexibility throughout its different uses and deployments.

The Different Varieties of Cloud

When adopting the use of the cloud, there are a few options that a business has to select from.

(Continued on page 3)

"Our technology forces us to live mythically."
- Marshall McLuhan

Let's Go Through Some Security Best Practices

While there is no question that security is important to any business, there is often a disconnect between this principle and any actual implementations that it reflects. Unfortunately, this can often leave a business vulnerable. To prevent this outcome, it is important that you follow a few best practices when it comes to fortifying your business against attack.

Security Steps

Good security practices will require a process for your team to follow. Take the time to go through every aspect of your business' infrastructure and develop the policies to ensure that your security is solid. As you do so, make sure you are addressing all scenarios and situations, including things like…

- What qualifies as confidential data, when and how this data is to be shared, best practices and requirements for storage and access credentials
- How devices used for work are to be maintained and handled, which devices may be approved for use, how to get a device approved
- How employees are required to go about transferring data, remote work policies, threat reporting processes

… as well as the other considerations that pertain to your business and its data. Directive can help you through this as well, to make sure nothing is missed.

Training

While many organizations tend to underestimate the importance of sufficient employee training, overlooking it could potentially bring down the whole of your operations. Time and again, a business' employees have been shown to be that business' largest vulnerability. Most often, this is simply due to ignorance, rather than the negligence or active malice that many managers and owners would presume.

After all, your employees are mathematically the most fallible of your many business resources. Not only are errors a very real possibility, cybercriminals have learned that technology is considerably harder to fool than a human being. As a result, there are considerably more threats out there that target your employees directly.

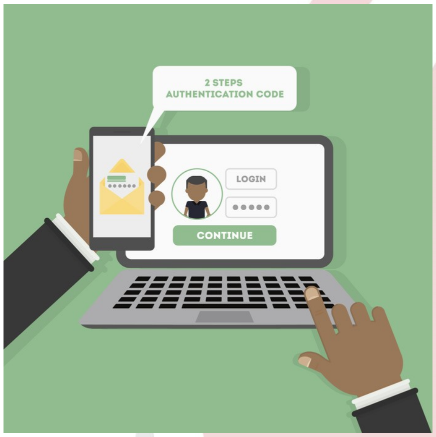
Phishing, or the attempt to gain critical information or access by posing as someone or something else to fool a user, is regularly deployed against professional and private users alike. While the most familiar example of phishing may be the classic Nigerian Prince scam, assuming that all attempts are so easy to spot is a shortsighted mistake that could leave your team more vulnerable to the much more sophisticated phishing attacks that are common enough today.

This is just one example of the many best practices that your employees need to know but are commonly overlooked, especially as time passes. Ongoing training and evaluation will help to maintain awareness of these threats…

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

2-Factor, 2-Furious - How 2FA is Our Last Hope

(Continued from page 1)



Want a good example? If you log into Netflix with your email address and a complex, random password that you use for your Amazon account, and Netflix gets breached, then nothing is stopping hackers from scraping the data stolen from Netflix and trying all the logins on other sites. This is often how individual accounts get compromised.

This happens a lot, and as individuals, we're all using more and more online accounts these days.

2FA levels the playing field. When you log into an account, you not only need your password, but you need to have your phone on you. Most 2FA works by sending you a text message, or maybe an email with a short code to type in while logging into the site. This is usually enough to prevent letting someone else in, who may have your password.

More secure 2FA methods use an authenticator app, like Google Authenticator, LastPass Authenticator, Duo Authenticator, or one of the others. These are even better because it's possible a hacker could have control over your email or they might be able to intercept your SMS messages, but if they aren't physically holding your smartphone they can't get in.

2FA is becoming a requirement for many industries, and it really should be considered by most businesses today. Enforcing 2FA for your users will ensure that their weak personal password habits don't put your business or its data at risk.

Want help setting up 2FA across your network? Give Directive a call at 607.433.2200.

Share this Article!
https://dti.io/2fahope

Small Businesses Face Hard Work Getting Back to Normal

(Continued from page 1)

Public Cloud

Public clouds are those that are provided and maintained by another company, such as Microsoft, Google, or Amazon. Typically available under the as-a-Service model, these solutions are very versatile and allow for a business to scale up or down as needed. This convenience, as well as the lack of maintenance that a subscriber is responsible for, makes these clouds a very popular option for businesses that need a cost-effective means of getting a given service.

Private Cloud

The private cloud is very similar to the public cloud, with exception to the fact that the resources are not shared, and that access to these clouds is specified to the company that owns it. This means that the security of these clouds is more assured, as the control of the setup and maintenance of the solution falls to the company.

Hybrid Cloud

As you might imagine, hybrid clouds work as a kind of combination between the public and private options. Some resources are hosted in the public cloud and some in the private cloud, with the freedom to interact with one another. This provides the benefit of the public cloud's scalability paired with the private cloud's inherent privacy.

Services Hosted in the Cloud

As we inferred above, the cloud can be used to support various needs… especially when referring to the public or hybrid varieties. In addition to storing data (which all are capable of) these two types can also deliver additional benefits delivered through the as-a-Service model.

Infrastructure-as-a-Service

This kind of cloud service gives the user a complete computing environment...

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

Data Security is Essential

Today, the threats businesses encounter from the Internet are more frequent and dangerous than any previous threats. To avoid being the victim of a cyberattack, you will need strategies and procedures aimed at mitigating them. Let's look at some strategies you need to consider if you are to keep the threats off your network.

Securing Your Endpoints

Really, cybersecurity is just the central management of several tools designed specifically to keep unauthorized users, and malicious software, off of your business' network. Since your network's endpoints are the closest to the actual Internet, fortifying them is important, but where you really have to focus your attention is the people on your network. You see, 94 percent of cyberattacks against businesses are actually driven by someone who works on the network. This makes most data breaches, malware attacks, and the like, completely avoidable. Let's go through four strategies that can keep you from being a victim of a cyberattack.

#1: Deploy and Maintain Security Solutions

The first suggestion is one that network administrators have made for decades: secure your network with software. Firewall, anti-malware, antivirus, spam and content filtering, and even a dedicated monitoring platform will pay big dividends for a company looking to keep nefarious entities off their network.

#2: You Need to Train Your Staff

The statistic referenced above should be the only piece of information you should need to put in a comprehensive cybersecurity training platform for your business. How do you go about implementing such a thing? Initially you begin with email training, since this is where the lion's share of problems begin. Here are three easy steps…

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

Cybersecurity Tips

Combating the Spread of Cybercrime

While it has taken some time to adjust, certain new self-care skills have been harnessed to keep ourselves and our loved ones safe. Good hygiene, social distancing and protective equipment can keep us safe, so why not apply these practices in a similar sense to our cybersecurity efforts?

Learn how you can use current safety precautions to combat the spread of cybercrime. https://dti.io/cst26

Get our Cybersecurity Tips to your inbox weekly!

Each week we send an email with **FREE** cybersecurity tips to help you to avoid a data breach. These tips can be used to educate yourself and your employees on security best practices.

Sign up today!
https://dti.io/gettips

Marketing Ideas & Tips for Your SMB

6 Steps in Building a Solid Web Presence

So, you have a brand new website that offers some pretty outstanding products/ services, and now you have the expectation that it is going to sell, sell, sell. Great products, after all, are the best marketing you can have. Let me tell you first so you don't have to hear it from someone else...**that is *not* enough**.

You have to do **more**! You can't just expect to have a website and think that your prospects will just stumble across your website over the MILLIONS that are currently out there. You need to create a strong online presence. This online presence that you cultivate affects your credibility, reputation, professional relevance, and referral power - so, do not succumb to the several problems with the "*build it and they will come*" approach. Your audience may need time, education, and repetition to convince them to make a purchase.

Your product/service solves a problem, so - intrinsically - it is a solution. The more you instruct, the more you escalate the urgency to solve their predicament, the faster you will sell. However that is not done though your product/service alone - that is through quality website content creation and marketing.

1. Plan And Strategize: *What Are Your Goals?*

First and foremost, it is paramount that you have established business and marketing goals - both short and long-term - as well as the resources and budget that they will require to make them materialize. It helps to create S.M.A.R.T goals that are **S**pecific, **M**easurable, **A**chievable, **R**elevant, and **T**ime-bound.

Having a strategic plan like this will ensure that the activities you are doing online are on the path that will help you reach these overall goals. This is a prime opportunity to reevaluate any current marketing activities that are not meeting your standards.

2. Build and Publish: *Construct a Solid Platform*

Capture their attention with content! Post new content on your website that is useful, relevant and consistent in quality, style, and frequency. It's relatively easy to produce content, whether that content is blogs, videos, or online deliverables. The more ways you can entice your audience to come back to your site, the higher the chances for an increased ROI.

However, it's not enough to just produce the content and put it up on your website. Make sure you direct all traffic back to that content on your site through your marketing efforts. Otherwise, it's likely just going to end up sitting there.

3. Share and be Social: *Information vs. Knowledge*

Everyone can obtain information; what they need is knowledge. The knowledge that they desire should reside in the content that you produce and share. The trick of the trade to having a lucrative online presence is distributing the right content with the right people... meaning, the right target audience.

This is where social media can come into play; it's a great...

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

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Chris Chase
Solutions Integrator

Charlotte Chase
Solutions Integrator

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
twitter.directive.com
blog.directive.com
instagram.directive.com