

**DTS**

DanTech Services

Computers under control!™

Technology Times October 2021 Issue

“With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you’ll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes.”



Dan Foote
Owner/President

What's Inside:

Page 2

5th Circuit Court Finds Cyber Insurer Must Pay for \$1 Million Social Engineering Attack

Credit Card Epiphany

Page 3

Performing security scans before issuing policies

Shiny New Gadget Of The Month:

FlexiSpot Memory Controller
Electric Standing Desk 48"x30"
Black Frame+ Black Top

Page 4

Official Statement from Facebook regarding October outage

“10 Questions to Ask Yourself Before You Adopt Any New Technology” - *Continued from Page 1*

Got IT Problem? - Click Here!



10 Questions to Ask Yourself Before You Adopt Any New Technology

By Jessica Stillman

Every new technology seems to give rise to hand-wringing about its potential impacts. Are screens making kids anxious and depressed? Is social media increasing political polarization? Do remote work tools boost productivity or kill productivity (or both)? Will improvements in A.I. replace drudgery with abundance or kick off an accidental apocalypse? Each innovation gives rise to a new corresponding flavor of anxiety.

Given that people have been fretting about technology at least since the advent of the written word (Plato worried that writing would destroy young people's memories), these kinds of discussions are probably inevitable. According to tech writer L.M. Sacasas, they're also often conducted in a less than ideal way.

New technology isn't simply 'good' or 'bad.'

- Continued on page 4



Get More Free Tips, Tools, and Services at [https:// www.dantechservices.com](https://www.dantechservices.com)

5th Circuit Court Finds Cyber Insurer Must Pay for \$1 Million Social Engineering Attack

A simple social engineered Business Email Compromise attack resulted in fraud that the cyber insurer contended was not covered under the policy.

We've written a number of times about court cases where the attacked organization sued their insurer because the insurer wouldn't cover the claim... and the insurer won due to a technicality. In a turn of events, the court case between financial services provider HMI and their insurer Twin City has recently resulted in the favor of the client.

HMI was the victim of a BEC scam pretending to be a client, the Geibs, requesting that \$1M be transferred to what was a threat actor-controlled account. HMI fell for the scam, losing \$1M of the Geibs' money. A settlement was made and HMI filed a claim with their insurer Twin City. **The denied claim resulted in a lawsuit that reached the 5th Circuit Court on appeal.**

Twin City maintained that the claim was invalid due to the following clause:

"Loss...in connection with any Claim based upon, arising from, or in any way related to any actual or alleged...rendering of, or failure to render, any services for or on behalf of others for a fee..."

HMI maintained no fee was incurred by the Geibs **and the courts agreed, finding for HMI and mandating Twin City pay the claim.**

While this case worked out for the attacked organization, it's important to realize that in every case, it seems that cyber insurers are going to scrutinize every word in the policy, looking for ways to get out of paying the claim.

A better approach – in addition to having cyber insurance – is to put Security Awareness Training in place (as part of a layered defense strategy) to educate those employees.

Credit Card Epiphany

This knowledge is certainly not just mine, yet unless you've had to replace multiple credit cards it may benefit you. It's bad enough to lose a credit card—whether you've left it someplace or through it being compromised, it's pretty much the same. One word: painful. The cost of replacement can be measured by a number of factors, one of them being notifying businesses that use that card for recurring payments.

Multiply this by losing your wallet, billfold, or purse. Multiply this by having to rebuild yourself through the necessities & fodder that fills your life—necessary fodder, like driver's license, membership cards, credit & debit cards, and other items. All of this becomes a learning process, too. Like, "don't want to do that again!" and "oh yeah, I need to do this too..."

Another learning moment came when I reached out to my various card carriers. **One rose to the top: American Express.** Here is why.

During the process of dealing with card termination, I was able to speak to a live person. And ask questions. Paramount question was: because this card is used for a number of recurring payments, will I have to notify them to change card numbers? Their

answer was that *as long as the vendor is in our system having used that card, we know what to expect and we will accept the charges without interruption.*

Compare this response to the one, inability to talk to a live agent for my Visa card, and two, having to take the time to make those account changes for all vendors concerned, it showed to me that AmEx is far more business friendly than any of my other cards. Included into this is that I had a replacement AmEx card in 3 days—FedEx'd. (Both AmEx & Visa did provide instant replacement numbers, so that's a draw.)

It's suggested that the cost of an American Express card is more than the competitors. I'd say that's marginally true. I'd also say that the benefits as a business owner outweigh those costs. This column isn't to do anything other than point out my experience. My hope is that you'll never undergo an experience like this.

I will note one other thing: on the security aspect of losing your collective wallet-sized self, it should be treated in a manner similar to identity theft. That, my friends, is another story.

Dan Foote



**NEED ADDITIONAL BACKUP STORAGE,
RUN OUT OF SPACE?**

CALL OR TEXT DANTECH SERVICES AT 907-885-0500

Shiny New Gadget Of The Month:



FlexiSpot Memory Controller Electric Standing Desk 48"x30" Black Frame+ Black Top

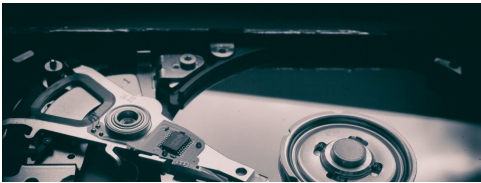
With FLEXISPOT's top-of-the-line height-adjustable desks, you can effortlessly achieve the perfect sit/stand balance throughout your entire workday.

Using a sit/stand desk helps to counteract the negative health effects of a sedentary job. This premium height-adjustable desk includes all the features necessary to deliver the benefits you expect from a standing desk, such as enhanced focus and increased calorie burning.

These desks are FCC and UL certified, ensuring the safety and quality of the design.

Start enjoying the health benefits of standing more and sitting less.

Are You're Worried About Safety Of Your Business Data?



data backup

Call 907-885-0500

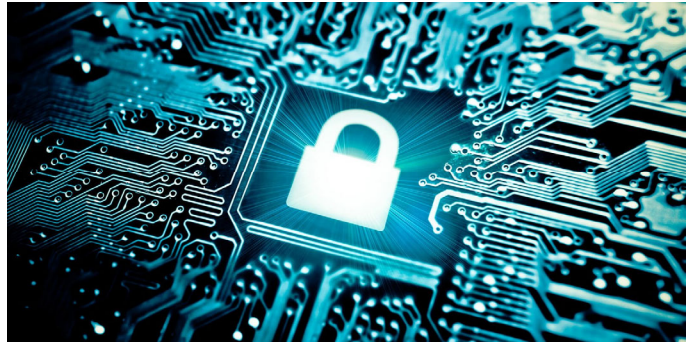
Performing security scans before issuing policies

A cyber insurer's security scans during the underwriting phase and post-issuance have led to a 65% reduction in ransomware claims. At this year's RSA security conference, [FBI Special Agent Joel DeCapua stated](#) that 70-80% of all network breaches are caused by attackers hacking into remote desktop servers exposed on the Internet.

Since no company wants to deal with a ransomware attack, businesses commonly have cyber insurance to cover the costs to restore devices or the potential payment of ransoms. To battle the rising tide of ransomware insurance claims caused by exposed RDP servers and vulnerable devices, cyber insurance company [Corvus](#) utilizes security scans as part of their underwriting process. Corvus Scan is a non-invasive security scan that examines a customer's network for exposed RDP servers, vulnerabilities in gateway devices and servers, and public-facing concerns.

The insurance company then provides a report to the customer about what equipment needs to be secured, including exposed RDP servers.

"Every customer receives the findings of the Corvus Scan with their insurance quote, and a detailed report with detailed security recommendations once purchased," Corvus told BleepingComputer.



Since introducing Corvus Scan 2.0 in April, Corvus states that the amount of ransomware-related claims has dropped by 65% with zero claims in new customers caused by breaches through RDP.

"Since the launch of the Corvus Scan 2.0 in April 2020, Corvus has written or renewed several thousand Cyber Insurance policies. The company's overall rate of ransomware claims has dropped 65%, from 26% of all claims to a rate among the new policies of 9%. In fact, new policies have had zero RDP-caused ransomware claims during that time. Several Corvus policyholders did experience ransomware caused by other vectors of attack," Corvus announced today.

These scans will continue to be conducted every quarter to warn of newly introduced threats for existing clients. With the use of security scans to illustrate the security deficiency's in a customer's network, it not only dramatically reduces the risk to the insurance carrier but also forces businesses to shore up their defenses proactively.

*** DanTech Services has cyber-security scan solutions!
Call 907-885-0500 x 1**

Official Statement from Facebook

(so you know what they claimed)

"To all the people and businesses around the world who depend on us, we are sorry for the inconvenience caused by today's outage across our platforms. We've been working as hard as we can to restore access, and our systems are now back up and running. The underlying cause of this outage also impacted many of the internal tools and systems we use in our day-to-day operations, complicating our attempts to quickly diagnose and resolve the problem.

Our engineering teams have learned that configuration changes on the backbone routers that coordinate network traffic between our data centers caused issues that interrupted this communication. This disruption to network traffic had a cascading effect on the way our data centers communicate, bringing our services to a halt.

Our services are now back online and we're actively working to fully return them to regular operations. We want to make clear that there was no malicious activity behind this outage — its root cause was a faulty configuration change on our end. We also have no evidence that user data was compromised as a result of this downtime. *(Updated on Oct. 5, 2021, to reflect the latest information)*"

The former Facebook product manager said the company puts profit over people and its products "harm children, stoke division and weaken our democracy." She called on Congress to take action against the company, as the platform, she says, has "repeatedly misled" the public and continues to hide research about its shortcomings.

If you use Facebook—remember that!



"10 Questions to Ask Yourself Before You Adopt Any New Technology"
- Continued from Page 1

In a fascinating recent appearance on the podcast of *New York Times* columnist Ezra Klein, Sacasas explains that too often when we discuss new technology, we look for blanket answers. Is this thing good or bad? Should I adopt it fully or reject it entirely? Sacasas pushes back against this tendency, telling Klein "part of the point that I often try to make is that something can be morally significant without necessarily being good or bad by itself."

All tools make it easier or harder to do particular things. They push us to think or behave in particular ways. They spotlight particular perspectives and hide others. Having a cell phone with a camera constantly in your pocket makes it much more likely you'll take pictures of your vacation or your kids. Delivery apps save you time but might disrupt family dinner. Whether shifts like that are for the better or no depends on your goals, values, and circumstances.

So how should you start to think through these more subtle tradeoffs and decide what technologies you personally want to adopt and when? In his newsletter *The Convivial Society*, Sacasas recently outlined 41 questions we should ask of the technologies we use. If that sounds like too much for you, fear not. Klein helpfully whittled them down to just 10 of the most important to get you started:



1. What sort of person will the use of this technology make of me?
2. What habits will the use of this technology instill?
3. How will the use of this technology affect my experience of time?
4. How will the use of this technology affect my experience of place?
5. How will the use of this technology affect how I relate to other people?
6. How will the use of this technology affect how I relate to the world around me?
7. What practices will the use of this technology cultivate?
8. What practices will the use of this technology displace?
9. What will the use of this technology encourage me to notice?
10. What will the use of this technology encourage me to ignore?

As Klein's fascinating podcast makes clear, these aren't yes/no, right/wrong type questions. In the episode the two men talk through how each question might be applied to a particular technology, illustrating how these questions nudge you to think more deeply about what you gain and lose when you choose to let a given tool into your life.

Ask these questions yourself and you should come away armed with the information you need to make more informed decisions about which new innovations to use and how.