



# Tech chronicle

Creative Consultants Group, Inc.

September 2018

## 4 Security Risks of the BYOD Strategy

Taking work home, or practically anywhere, has never been easier. The bring your own device (BYOD) strategy has become a popular approach for many businesses to conduct work more efficiently and flexibly.

But this strategy is not without risks.

[www.getccg.com/4-risks/](http://www.getccg.com/4-risks/)



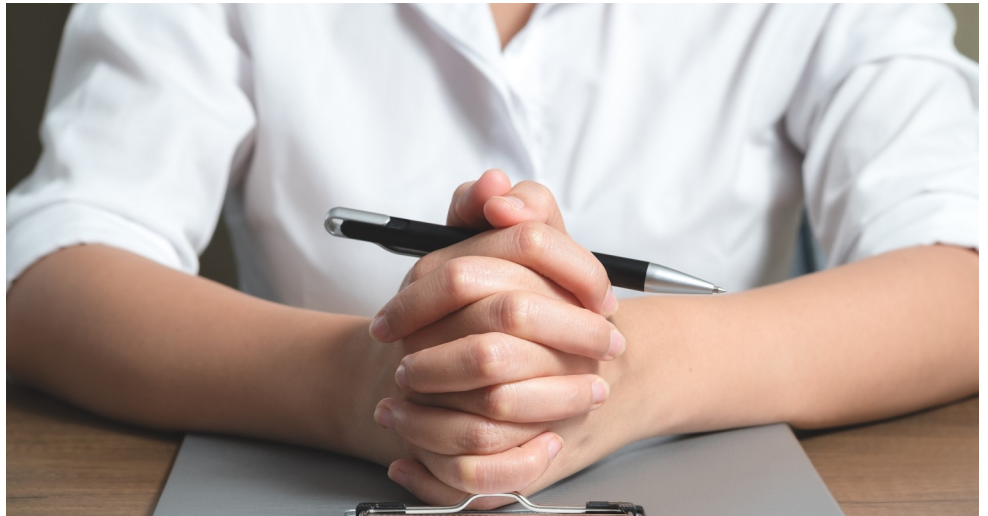
**September 2018**



This monthly publication provided courtesy of Bill Hinson, CEO of Creative Consultants Group, Inc.

### 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.



## 4 Questions You Should Ask Any IT “Expert” Before Letting Them Touch Your Network

As businesses have become ever more dependent on technology, IT services providers have been popping up left and right. They’ve all got different strengths, capabilities and price points to consider. Some charge you by the hour and, while available to address any concerns you may have, they are pretty hands-off. Others are working on your network around the clock but charge more in turn. Many may boast an impressive record when working with a broad range of companies, but lack the experience necessary to understand the ins and outs of your specific industry. Some cost way too much month-to-month, while others try the “bargain bin” approach, but as a result, can’t afford to field the staff needed to respond to issues in a timely fashion.

There’s certainly a lot to consider when looking for an IT services provider for

your business. And if you’re not particularly knowledgeable about information technology yourself, it can sometimes feel like you’re going into the process blind.

To suss out whether an IT company will mesh with your business’s workflow and industry-specific requirements, it’s important to vet them thoroughly. The key is to ask the right questions. Here are four that will allow you to zero in on any IT company’s priorities and strengths, and help you determine whether they’re a good fit for your organization.

### **1. Do you take a proactive or ‘break-fix’ approach to IT?**

When your car breaks down, you take it to the shop and you get it fixed. The mechanic charges you for the work done and for the parts, and then sends you on your way. Many business

*continued on page 2*

Get More Free Tips, Tools and Services At Our Web Site: [www.getccg.com](http://www.getccg.com)

(843) 234-9980

owners consider their computer network to be the same kind of deal. Why not just wait until an outage happens and then call up somebody who charges by the hour to fix it? That way, they imagine, they won't be paying for "extra" services they think they don't need.

But unfortunately, unlike your car, when your network is out, you're losing dollars every single minute. The cost of a network outage is difficult to overstate – not only will it bring your business to its knees while it's out, but it'll frustrate customers and employees and result in a cascading set of problems.

Instead of a "break-fix" technician on hand, you need a managed IT services provider. These experts work directly with your company to optimize your network and its security at every turn, and are available nearly any time to address your concerns. And they're genuinely invested in providing the best service possible, since it's in their best interest as well.

**"a network outage [will] bring your business to its knees while it's out ... it'll frustrate customers and employees and result in a cascading set of problems."**

**2. What is your guaranteed response time?**

We've all needed something fixed before and had to wait for hours, days or even weeks before anyone bothered to come by and solve the problem. Don't let that happen to your business. If a company can't guarantee a response time, it's probably not a company you want to be working with.

**3. What will cost me extra?**

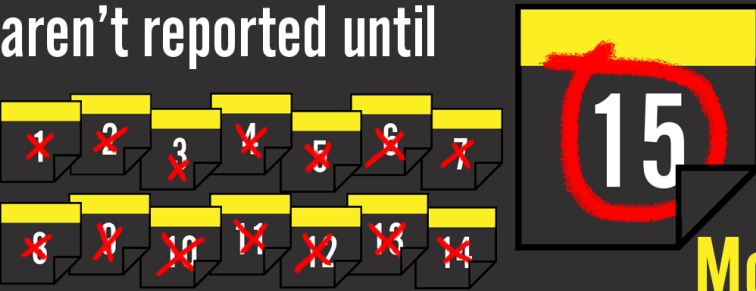
This question is particularly important if you're looking at a managed services provider (which you should be). The last thing you need is for a crisis to strike, only to discover you need to shell out a bunch of surcharges to get your network back up and running. Make sure the costs and services included are crystal clear before you sign anything.

**4. How much experience do you have?**

As scrappy as the "new kid on the block" may be, you don't want them in charge of one of the most important aspects of your business. Make sure any IT professionals you do business with have extensive experience not only in IT, but in your particular industry as well. That way they'll know exactly what to do to optimize processes and keep your data under lock and key.

For more information on CCG's services and to see what our clients are saying, visit our website at [www.getccg.com](http://www.getccg.com) or call us at 843.234.9980.

**On average, compromised credentials aren't reported until**



**15 Months**

**after the breach occurs.**

Based on Shape Security 2017 data.

**Are Your Credentials For Sale on the Dark Web?**  
**Contact us before October 31st, 2018 and we will provide a FREE Dark Web Analysis. For more information and to sign up, visit:**  
[www.getccg.com/darkweb/](http://www.getccg.com/darkweb/)

## SHINY NEW GADGET OF THE MONTH

### Is This The Best Bag For Frequent Flyers?

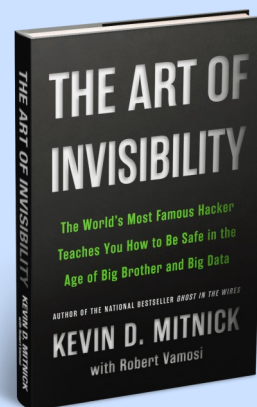
If you're constantly travelling around the country for business, you need a piece of luggage that's essentially indestructible, and hopefully one that you can carry on any flight you need, saving on costs and precious minutes wasted at the luggage turnstile. Luckily, with the Victorinox Lexicon Hardside Frequent Flyer 8-Wheel bag, you may have a contender that checks all your boxes. With a sleek, ergonomic, compact design, it offers plenty of volume without being bulky, along with a slick eight-wheel design that makes scooting around the ticket lines easier than ever. And for those of us living in the 21st century, there's a dedicated pocket for a battery pack, enabling you to attach a USB charging cord directly to your bag for when you need a little extra juice.



## The Art Of Invisibility

By Kevin D. Mitnick

Today, everybody is talking about privacy in the digital space. But in reality, the vast majority of people harping on the privacy of their data unknowingly have little to no privacy at all. Nearly everything on the Internet is indexed, tracked, analyzed, and recorded, whether you're sitting at your laptop checking your e-mail or even paying your bill at a local restaurant.



In famous hacker Kevin D. Mitnick's *The Art of Invisibility*, he breaks down all the data that the world is collecting about you day by day, and how you can protect yourself from prying eyes. With a few simple techniques, you can get the privacy you deserve, even in the modern age.

## Why It's So Dangerous To Use The Same Password For All Online Accounts

A complex password is a necessity in the age of cyberthreats, data breaches, and other security incidents. When you've landed on what you think is the perfect, complicated, yet easy-to-remember password, it's tempting to use it for every site you log in to. This is a shockingly common — and very dangerous — mistake.

When an online retailer or website gets hacked, oftentimes all you hear about in the news is how many credit card numbers were lost or the scope of the financial damage. You rarely hear about the thousands of user accounts that were compromised. But they're there!



If yours is among those compromised accounts, it's possible that your username and password are published and available to anybody who wants to look at it on the Internet. A clever crook knows that you probably use the same

password on the compromised website as you do on your eBay, Amazon or other online accounts tied to your bank account. So, they try it out and, lo and behold, now they have access to your bank account.

### Secret Techniques For Dealing With Late-Paying Clients

If you have a client who's habitually paying you late, it can be incredibly frustrating. But there are a few ways to mitigate the problem and get them back on track.

First, try billing twice per month or upfront instead of monthly. The former option will get them on a firm schedule and prevent getting backed up, while the latter will eliminate the problem altogether.

Also, try getting in touch with a contact in accounts payable. That way you can cut out the middleman and streamline the process.

Finally, make sure to send follow-up e-mails along with any invoice you send out. Pester them enough and they'll get the picture.

*SmallBizTrends.com, 6/20/2018*

## Watch Out For This Persuasive Phishing Email

Anglers catch fish by dangling bait in front of their victims, and hackers use the same strategy to trick your employees. There's a new phishing scam making the rounds and the digital bait is almost impossible to distinguish from the real thing. Here are the three things to watch out for in Office 365 scams.

### Step 1 - Invitation to collaborate email

The first thing victims receive from hackers is a message that looks identical to an email from Microsoft's file sharing platform SharePoint. It says, "John Doe has sent you a file, to view it click the link below..."

In most cases, the sender will be an unfamiliar name. However, some hackers research your organization to make the email more convincing.

### Step 2 - Fake file sharing portal

Clicking the link opens a SharePoint file that looks like another trusted invitation from a Microsoft app, usually OneDrive. This is a big red flag since there's no reason to send an email containing a link to a page with nothing but another link.

Step 2 allows hackers to evade Outlook's security scans, which monitor links inside emails for possible phishing scams. But Outlook's current features cannot scan the text within a file linked in the email. Once you've opened the file, SharePoint has almost no way to flag suspicious links.

### Step 3 - Fake Office 365 login page

The malicious link in Step 2 leads to an almost perfect replica of an Office 365 login page, managed by whoever sent the email in Step 1. If you enter your username and password on this page, all your Office 365 documents will be compromised.

Microsoft has designed hundreds of cybersecurity features to prevent phishing scams and a solution to this problem is likely on the way. Until then, you can stay safe with these simple rules:

Check the sender's address every time you receive an email. You might not notice the number one in this email at first glance: johndoe@gma11.com.

Confirm with the sender that the links inside the shared document are safe.

Open cloud files by typing in the correct address and checking your sharing notifications to avoid fake collaboration invitations.

Double check a site's URL before entering your password. A zero can look very similar to the letter 'o' (e.g. Office.com/signin).

Third-party IT solutions exist to prevent these types of scams, but setting them up and keeping them running requires a lot of time and attention. Give us a call today at 843.234.9980 for information about our unlimited support plans for Microsoft products.

TechAdvisory.org

## CCG Monthly Trivia -Win \$250 Gift Card!

The Grand Prize Winner of last month's Trivia Challenge Quiz is Beth Mayhew of Piedmont Plumbers of Myrtle Beach! Beth's name was randomly chosen among those that correctly answered my quiz question from last month: Which 2 Atlantic hurricanes hold the record for the longest time spent as a Category 5 (wind speed of 157 mph or greater)? The answer was b) Ivan and Irma.

Now, for September's trivia question. Email your answer to: [swoollums@creativeconsultants.net](mailto:swoollums@creativeconsultants.net).

**Which NFL coach has the most wins in NFL history?** a) George Halas b) Tom Landry c) Bill Belichick d) Don Shula.



© MARK ANDERSON

WWW.ANDERSTOONS.COM

