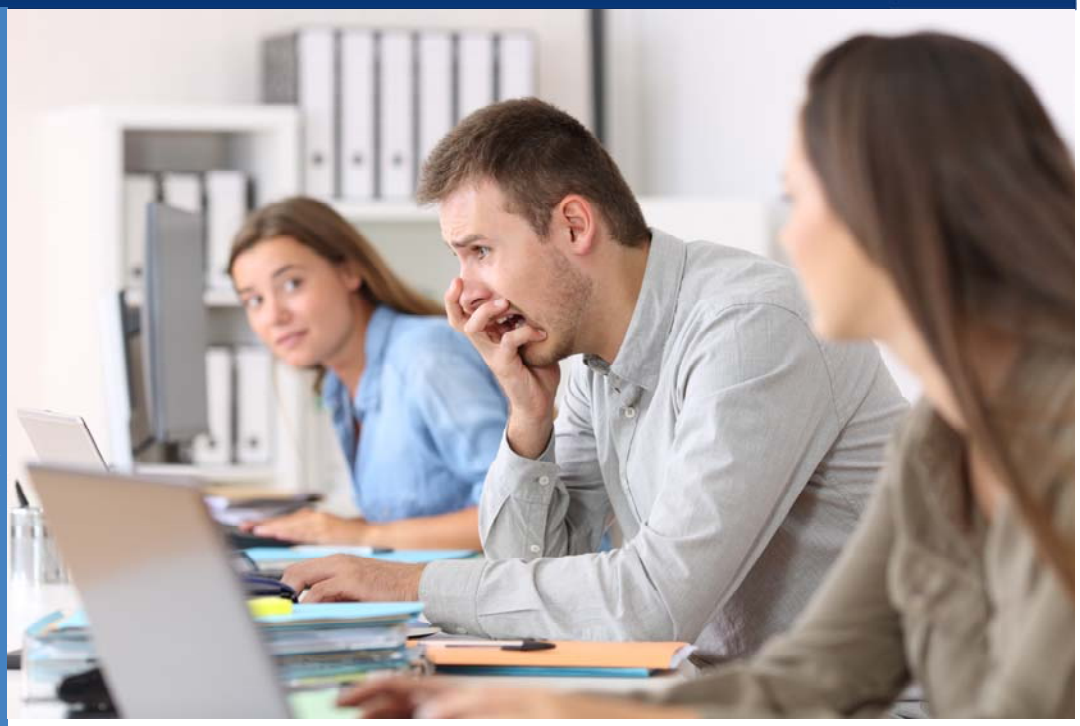
DTS DanTech Services
Computers under control!™

Technology Times March 2018 Issue


"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

## What's Inside:





# 5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the Harvard Business Review – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

*- Continued on page 4*

## Business Briefings:

### The "Not Me!" Problem…And Why This Is Almost Guaranteed TO Happen To You

Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea.

But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

### 7 Things Mentally Strong Leaders Never Do

Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1. They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.

2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.

3. They accept criticism with open arms. Instead of protecting a fragile ego, mentally strong leaders take unfavorable feedback and use it to improve their processes.

4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.

5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.

6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.

7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.

## Cash In On Your Million-Dollar Idea

*By MIKE MICHALOWICZ*

So, you came up with a brilliant idea. A million-dollar idea, even! But right now, that's all it is. The question is, how do you turn that big concept into cold, hard cash?

1. Write it down. How many light-bulb moments do you have at 2:00 a.m. and then forget come 9? Or, worried that your idea will be stolen, you keep it to yourself, promising to chase it down when you finally get the time. If you actually write down every moneymaking scheme you think up, one of them is bound to be the real deal eventually.

2. Once you settle on the idea you want to pursue, write a pros-and cons list. What could make your idea truly successful? What could make it a total bust? Once you identify the cons – a too-high initial production cost or a newcomer in a competitive industry – you can start your search for solutions.

3. Determine your audience. Who do you think will buy your product or service? Run business surveys to determine whether there's a market for what you want to sell.

4. Figure out what problem you're solving. Uber eliminated the inconvenience of hailing a taxi and the difficulty of preordering a ride, all for an affordable rate. Apple lowered the cost of technology and made it user-friendly at a time when computers were designed for engineers and tech professionals. If you solve a real problem that exists in the market, consumers won't be able to live without your product.

5. Find a business partner. Although you may want to keep your idea to yourself, remember that it takes two flints to make a fire. How many successful start-ups do you know that were founded by a single person?

6. Start to think about money. If you don't already have some rainy-day funds to dive into, consider crowdfunding, borrowing from friends, credit cards or loans. Know the risks you're taking before moving forward.

7. Create a financial model. If you want to attract investors, a financial model that forecasts the fiscal performance of your business will show them your expected profitability and their return on investment. This makes you a more reliable bet.

8. Develop your prototype or beta test. This will allow you to see if your idea will actually work in the real world.

9. Prepare to be flexible and roll with the punches. Odds are, your initial idea won't be the same as your final product, and that's okay.

10. Keep on the sunny side. There are going to be truckloads of people who try to tear you and your idea down on your road to success. Stick to your guns – it's your baby and your investment of time and money, so make sure you believe in it.

---

*MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small-business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.*

## Has your business had a need for short term funding for a purchase?

behalf

### Welcome to Behalf!

**Finance Any Purchase**

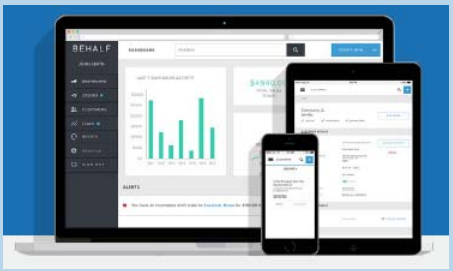
Use Behalf in place of cash or checks to fund equipment, inventory or anything else your business needs with interest rates up to 3%

**Get Flexible Terms**

Select your own short-term payment schedule and enjoy up to 6 months of extra time on each purchase

**Save 10% On Finance Fees**

* Get 10% off finance fees for choosing a weekly plan
* And the application process takes only minutes.
* DanTech Services works with Behalf to make this happen for your business! Technology upgrades do not need to break your bank or limit your cash flow.



**FOR YOU:**

* - Affordable, On Demand Financing
* - Net 30 Free of Charge
* - 1-3% Monthly Advance Fee
* - No Hidden Fees

**Give us a call at 907-885-0500 to find out more about this affordable and easy to use service!**

# Now — HERE Is a Devious Combo Pretexting / Vishing / SMS Social Engineering Attack!

*Someone on Reddit described how he was the victim of a very sophisticated social engineering attack. Wow, this is crafty. This is the story! - Published by KnowBe4*

"I have different passwords for every website I log into, 2-factor authentication when possible; I thought I knew all the scams and could spot them a mile away. This one still got me.

I was meeting a friend at a bar. Two drinks in I got a call from someone identified by my phone as Wells Fargo. I'm fully aware this could be spoofed, but it did not raise alarm bells yet. I was at a bar I did not frequent and have gotten calls from my bank before on suspicious charges that were legit, so I answered expecting this to be the case.

The person I spoke with said they were with Wells Fargo and they've identified fraudulent charges on my account but they need to verify my identity before they can discuss details. They said they sent me a text message (via the cell number they just called, which is my first clue this is phishing). They asked me to read back to them the 6-digit number just texted to me to verify my ID.

Being two drinks in, slightly expecting what this was about, I had zero alarm bells going off. My bad, this was stupid of me. I read the number to them. They suggested it timed out and I needed to read another number they texted to me. Minimal time had passed, a mild spidy sense was tingling, but I still was not concerned enough to ask questions and read them a second 6-digit code.

This person then read off 5 recent charges on my account, 4 of which I recognized as legit and a 5th that was a $1000 charge to a credit card I did not own. I immediately identified this as a fraudulent charge and they said "no prob dude, we'll freeze your card and send you a new one". They even gave me the last 4 on the card it was coming from. I was appeased enough to continue (sadly).

Finally, they said they sent me one final 6-digit code to confirm that they were crediting my account back with the $1000 fraudulent charge. I just needed to read off the final code they texted to me. At this point things seem weird to me but they got me at a good time. I was 2 drinks in, was interrupted from hanging with a close friend I hadn't seen in months and was outside trying desperately to avoid the loud noise inside the bar but still dealing with traffic noise outside. I just wanted to be done with this. I read them the final code and they thanked me and hung up.

At this point, I see why my phone had been vibrating constantly through this call. I had 4 emails from Wells Fargo. 1) Your user name has been reset, 2) your password has been reset, 3) Welcome to Zelle! an awesome $$$ forwarding service, 4) You've just forwarded $1000!!!!!

I called Wells Fargo via the number on the back of my card. After being on hold for 45 min trying to get the fraud department, I start to tell my story only to have the call drop (I'm pretty sure they hung up on me). I called back and was on hold for 1 hour 20 min (my account has been compromised >2 hours by this time) to get a second person. He told me this was a scam they've been dealing with for 3 months and I needed to go into a branch with 2 forms of ID to deal with it. There was nothing he could do tonight.

Dude spoofed Wells Fargo when calling me on my cell, requested a reset of my user name, password and approval for $1000 transfer. I stupidly read off the confirmation numbers I received via text to him, he entered them into Wells Fargo website to approve all these requests. Wells Fargo has known their customers have been getting scammed for 3 months and didn't bother to warn anyone. I now have to go into a branch, hang my head and tell my shameful story to a person and beg for access to my account because someone else has control of it all night tonight."

*Good lesson to be learned: Never, ever give any kind of confidential data to someone WHO CALLS YOU. Always call back to the number on the back of your card.* ***Let's stay safe out there.***

## Shiny New Gadget Of The Month:


### FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

SONICWALL™
• SecureFirst •

*DanTech Services provides knowledgeable management, support & sales of*

**SonicWALL UTM's.**

Call 907-885-0500 to keep your network secure and your ***Computers Under Control!™***

*- "5 Ways Your Employees Will Invite Hackers Into Your Network"*
*- Continued from page 1*

**1. They'll slip up because they don't know any better.**

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For this reason, most cyber-attacks come down to a lack of cyber security education.

**2. They'll let you get hacked on purpose.**

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

**3. They'll trust the wrong person.**

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

**4. They'll miss red flags while surfing the web.**

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

**5. They're terrible at passwords.**

According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

## SEO OPTIMIZATION

DanTech Services is offering you Search Engine Optimization for your web-site.
In 45 days we will put your web-site to the Top Searches on Google.
**Call today at 907-885-0500 to start your optimization.**