RIGHT HAND TECHNOLOGY GROUP
TECH TIMES

December 2018

What's New?

Why Phishing Works

A successful phishing attack accomplishes two basic goals: **it gains the trust of victims and exploits their emotions**. Take, for example, those classic advance-fee scams that promise a large sum of money for a small up front payment. You would never fall for one of those, right? Of course not. They're incredibly easy to spot, thanks to their too-good-to-be-true nature. But other phishing scams are more advanced. Imagine a friend of yours is looking for a job. She posts her resume on various sites and sends out applications. Then, she finally receives an email, that appears to come from Linkedin, with a great job offer. **All your friend has to do is click the link and upload her personal details. But is it a scam?** More importantly, would your friend, who has been on the job hunt for several months, even question its authenticity? Now let's flip roles. Let's say you handle the hiring of new employees and you get lots of emails from applicants with attachments. **How difficult would it be for a social engineer to push a malicious attachment, disguised as a resumé, to your inbox?** What about emails that appear to come from someone you know? Let's say a friend sends you a message that he's traveling abroad, has been robbed, and urgently needs you to wire him money in order to buy a ticket home. How would you respond? It is easy for social engineers to leverage emotions like compassion or concern against their targets. It gets even easier when their targets are at a point of desperation, often related to financial need. Simply put, people fall for advance-fee scams. People fall for fake job offerings. People fall for threats that claim to come from tax collection agencies. **Trust, desperation, and fear: the most effective weapons of scammers.**

2 Places You Should Never Cut Corners With IT

Today's technology empowers business owners in ways that would have seemed incredible even 10 years ago. With a humming network connecting your team to the rest of the world, and with just a few simple keystrokes, your organization can complete tasks that used to take days.

However, the endless possibility that accompanies technological advancement comes with a catch: to be truly effective, IT requires investment – not just of capital, but of time and attention, resources all too dear to the harried entrepreneurs of the modern age. Perhaps this is why, everywhere you look, small to midsize business owners are not only failing to realize the full potential of their technology, but are unknowingly leaving massive gaps in their systems and processes for malicious entities to exploit. And so, budding companies that would otherwise dominate the market are prematurely stamped out by competitors with more tech savvy or are hamstrung by costly data breaches.

Even in the midst of this trend, we understand how easy it is to ignore your company's glaring technological gaps. You imagine that you don't have the time or money to address the issue, or that you'll do it down the road once

continued on pg2

your business is better established. But no matter how big or small your business may be, there are two foundational tech concerns that you should never cut corners on.

1. Security

Pretty much every successful company today is intimately intertwined with the technology on which it depends. So it makes sense that your primary worry should be protecting what's yours from those who want to snatch it. Think of it this way: would you hire a $5 locksmith to secure your office? Of course not. Then why do so many business owners put their livelihood behind a flimsy, $5 firewall – or, even worse, a free antivirus? In 2018, it is more likely that your business will fall victim to a cyber-attack than it is that thieves will arrive at your office in the dead of night, according to a 2017 report from Kroll.

> **"... you're inviting a crisis into the equation that could easily have been avoided with a keen, proactive eye."**

In 2015, SEC Commissioner Luis A. Aguilar wrote, "Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses. The reason is simple: small and midsize businesses are not just targets of cybercrime; they are the principal targets." With this in mind, cyber security should always be one of your top priorities.

2. Tech Support That Goes Beyond The "Break-Fix" Approach

It's difficult to overestimate the money, time and stress it can cost you when your technology breaks down. Between server downtime, haywire software, connectivity issues and myriad other potential problems, when your stuff breaks, it can cause more than a massive headache – it can put you out of business.

Most business owners realize this, but many still opt for the classic "break-fix" strategy. Unfortunately, "If it ain't broke…" is a dangerous maxim by which to steer a ship. If you wait to address a problem until after it becomes an issue, you're inviting a crisis into the equation that could easily have been avoided with a keen, proactive eye. And when your server fails, or your network experiences hiccups, or some other unforeseen issue rears its ugly head, an unfamiliar break-fix technician will take longer to fix the issue than an expert who's been working with your specific network from start to finish and already knows it inside out. It's just not worth it.

In addition, proactively managed service providers will consistently make recommendations to keep your company competitive. Whether it be a small upgrade to software here, a patch there or an overhaul of your server system, these moves can be invaluable in the breakneck marketplace. And, of course, since they're keeping tabs on your tech at all times, any potential problems get addressed long before they hit your bottom line.

By leveraging technology, you and your business can do amazing things. Partner with a team of IT professionals who are actively invested in your success and confidently push your company into 2019.

Shiny New Gadget Of The Month:

The Casio Pro Trek Smart A Watch Built For Adventure

Today, a lover of the outdoors needs to demand more from their devices if they're going to get the most out of their adventures. The best tech boasts robust, easy-to-use features for when you need them but gets out of the way, leaving you to focus on the grandeur surrounding you.

Luckily, the Casio Pro Trek Smart WSD-F20ABU watch does exactly that in one attractive, intelligent package. Every capability you'd expect from an outdoors-focused device is overhauled here – from the altimeter to the barometer and even the feature-rich compass. Perhaps the best tool is the full-color map you can display on its face, which detects and displays changes in the atmosphere and weather up to the minute. If you're looking for a sturdy, powerful tool to bring along on your next excursion, it'd be tough to do better than this.

The Importance Of Pride

The Key To Better Serving Your Customers

The famous business guru Peter Drucker wrote more than 10,000 pages on the subject of management. Across 39 books translated into 36 languages, you can bet he learned a bit along the way. It's the reason he's widely considered the "founder of modern management." In his book The Practice Of Management, Drucker states, "There is only one valid definition of business purpose: to create a customer. The customer is the foundation of a business and keeps it in existence. He [the customer] alone gives employment."

Recently, I had the opportunity to work with Farm Credit Services of America, a customer-owned financial cooperative that finances and protects farmers and ranchers in Iowa, Nebraska, South Dakota and Wyoming. Everywhere I turned and with every person I interviewed, it was obvious Mr. Drucker would be thrilled with their business philosophy. Their customer is truly their No. 1 priority. All policies, procedures, products and services are in place for the sole purpose of helping their customers.

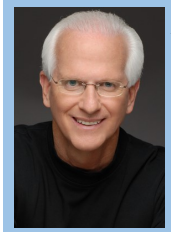
Maybe we should all consider ourselves "customer-owned cooperatives." After all, every part of our existence is based upon our customers. They may not directly own our companies, as they do at Farm Credit Services, but, as Mr. Drucker wrote, they alone give us employment.

Farm Credit Services was having an Executive Summit with 70 senior directors to discuss what more they could do to better serve their customers. They allowed me the opportunity to interview 15 people, from senior management to sales and field personnel, so I could dig down to find what really makes them tick. They didn't inquire as to what I would be asking their employees, nor did they give me any directions, concerns or restrictions as to what I could discuss. It doesn't get any more transparent than that.

Did I uncover any complaints, concerns or frustrations? Sure I did – every company has them. But more importantly, I discovered how proud they were to be serving their customers. Their heartfelt dedication to doing everything they could to ensure their customers succeed in a competitive and volatile market was a pleasure to witness. If someone were to ask me how I would sum up Farm Credit Services, I would choose one word: proud.

You can't mandate proud. You can't force people to be proud. Pride is a culture, a foundation deeply rooted in the fabric of an organization. You can feel it whenever you're around a proud organization, see it in the actions of their entire team and hear it in their words. We could all learn from Farm Credit Services's example. If you want to succeed, both personally and as a business, then you need to:

Robert Stevenson is one of the most widely recognized professional speakers in the world.



Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H. W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.

4 Ways Your Employees Will Invite Hackers Into Your Network

Cyber security is a complicated issue, no matter how you slice it, but one of the surest ways to reduce your risk and strengthen your defenses against hackers is to educate your team. Forewarned is forearmed, so make sure they fully understand the risks associated with the most common social engineering strategies. Phishing, the most prevalent, uses e-mails, chats or web ads impersonating trusted entities to trick employees into clicking malicious links. Baiting is similar, but purports to offer something enticing, such as a music or movie download, to deliver malware onto your system. Quid pro quo hackers offer a "service" in exchange for access to private data, such as an employee's login credentials. Tailgating is when an unauthorized person physically follows one of your employees into a restricted area or asks to "borrow" their device for a bit and steals all the info they need directly.

Make sure your team is on the lookout for these malicious techniques, and you'll be that much more secure. SmallBizTrends.com, 9/20/2018

Who Else Wants To Win A $25 Gift Card?

The answer to last month's Trivia Challenge Quiz was D) F7

December's Trivia Question is Below:

Which of the following types of attacks do hackers use to gain information from you without the use of specialized computer programs?

A) ARP Poisoning

B) Cross Site Scripting

C) SQL

D) Social Engineering

First Person To Email The Correct Answer to trivia@rhtg.net WINS!

Use These 3 Strategies To Break Your Bad Tech Habits

If you're trying to kick an addiction to your smartphone and other addictive tech, and you're tempted to turn to them whenever you feel uncomfortable or anxious, don't give up. Instead of seeking a distraction whenever you feel bored – for example, checking your e-mail for the 10th time or logging in to Facebook – learn to embrace silence, and yes, even boredom. If you find yourself checking your phone too much at work, set physical boundaries to restrict yourself. Put it in your desk or another place that adds an extra step to accessing it. The next time you have downtime, instead of whipping out your device right away, mull over a specific problem or idea on your own – you might be surprised what you discover. Inc.com, 7/20/2018