ISSUE
03
March 2020

MANAGEDTEK
MONTHLY
JOURNAL OF
INFORMATION

TekTimes

This issue

What's New!

If you've been following the latest news in cybersecurity, you know that attacks have only continued to grow in both size and sophistication.

Beware At The Gas Station…

If you use a credit card at the gas pump, you increase your risk of having your credit card information stolen. At the end of 2019, Visa warned a number of its customers that hackers are actively stealing credit card information by hacking into gas stations' point of sales networks. These networks, it turns out, are not as secure as they should be.

Hackers also use phishing scams. All the gas station employee has to do is click a malicious link and hackers can install software that steals credit card information from the station and sends it back to the hacker.

What can you do to protect yourself? Make sure your credit cards are up to date with the latest chip technology. Never use your card's magnetic strip, if possible. If you're still using your magstripe, ask your issuer for an updated card or find a new credit card provider. Cash is also a great option.

Are You Working SMART?

Rubbermaid thought they needed more products to be the leader in their industry. So, they set out to invent a new product every day for several years, while also entering a new product category every 12-18 months. *Fortune* magazine wrote that Rubbermaid was more innovative than 3M, Intel and Apple; now, that is impressive.

Then Rubbermaid started choking on over 1,000 new products in less than 36 months. Innovation became more important than controlling costs, filling orders on time or customer service. They ended up closing nine plants and laid off over 1,100 employees before Newell Corporation came in to buy (rescue) the company.

I had a mentor who once told me, "Rob, I don't care how hard you work. I care how smart you work." Rubbermaid was working hard, putting in time, money and effort while at the same time destroying their own company. How did that work out for them?

Eli Lilly thought they needed to hire 2,000 PhD researchers to create more products to keep Wall Street happy with their growth. The only problem was they didn't have the funds to hire them. So, they had to come up with another way to solve this problem – in other words, they had to work smarter.

They decided to take all their molecular problems, post them on the Internet and tell all molecular PhD researchers that they would PAY for solutions. Instead of having to pay the salaries and benefits for 2,000 new researchers with money they didn't have, they had thousands upon thousands of researchers all over the world sending in their suggestions for solutions to their molecular problems, and they only had to pay for the ones they used. Now, that is SMART!

Do you see **SMART** opportunities in these statistics?

· out 66% of employees would take a lower paying job for more work flexibility.

· About 62% of employees believe they could fulfill their duties remotely.

· About 60% of employees believe they don't need to be in the office to be productive and efficient.

Could you lower overhead and expenses by having some people operate from home? Some managers will immediately say, "That won't work; you won't have control of your employees. They won't get things done." If that is your argument, my statement to you is this: you have hired the wrong people.

JetBlue has hundreds of reservation agents operating from their own homes. Their home-based agents save, on average, up to $4,000 on their commuting expenses, not counting the savings of lunch, day care and wardrobe. JetBlue found they had a 25% increase in productivity once employees were allowed to work from home; they figured out a different, more productive, less expensive, more profitable … *SMARTER* way to operate.

To survive in this competitive marketplace, you must change, adapt, modify, challenge, innovate, transform, revise and improve, but what's paramount to your success is to be working SMART!

Sharing Your Email

Whenever possible, avoid using your work or personal e-mail. If you need to sign up for something and you don't completely trust the source (or just want to avoid spam), create a "burner" e-mail address you can use. It should be something different from your work or personal e-mail and not associated with business or banking.

Not Using HTTPS

Why is visiting an unsecured HTTP website dangerous? Any data you share with an unsecured website, such as date of birth, passwords or any financial information, may not be securely stored. You have no way of knowing that your private data won't end up in the hands of a third party, whether that's an advertiser or a hacker. It isn't worth the risk.

When visiting any website, look in the address bar. There should be a little padlock. If the padlock is closed or green, you are on a secure website. If it's open or red, the website is not secure. You can also click the padlock to verify the website's security credentials. It's best practice to *immediately* leave any website that is not secured. And never share your personal information on a webpage that is not secure.

Contact us today and let us help you develop security-driven policies and procedures for your business.

Clear Signs You're About To Get Hacked … And What To Do NOW

Do you use the same password for everything? If you do, you're not alone. We all have bad cyber habits, whether it's reusing passwords or connecting to unsecured WiFi. These habits can make it easy for hackers to steal our personal information and use it for their own purposes – or they can sell it on the dark web for an easy profit.

These are habits you have to stop right now – and habits your employees need to stop too. After all, good cyber security practices are a group effort! But using the same password for everything or using simple passwords aren't the only things that are going to get you into trouble. Here are three more clear signs you're setting yourself up for a breach.

Sharing Your E-mail

Countless websites want your e-mail address. Sometimes it's not a big deal if you're sharing it with a vendor or e-commerce site. You want to ensure you receive invoices and shipping confirmation. But other websites just want you to sign up for special offers, notifications, e-mail newsletters and other inbox clutter. It sounds mostly harmless, but what they fail to tell you is the fact that they're going to sell your e-mail address to advertisers and other third parties.

To make matters worse, you have no idea where your e-mail address will end up – or if it will fall into the wrong hands. Hackers are constantly on the lookout for e-mail addresses they can take advantage of. They use e-mail for several different kinds of cyberscams – most notably phishing scams. Hackers can even make it look like an e-mail is coming from a legitimate source to get you to open it.

Not Using HTTPS

Most of us are familiar with HTTP. It's short for Hypertext Transfer Protocol and is a part of every web address. These days, however, many websites are using HTTPS – the S standing for "secure." Some web browsers, like Google Chrome, even open HTTPS websites automatically, giving you a more secure connection. Of course, this only works if the website was made with an HTTPS option.

Saving Your Passwords In Your Web Browser

Web browsers make life so easy. You can save your favorite websites at the click of a button. You can customize them to your needs using extensions and add-ons.

And you can save all your usernames and passwords in one place! But as convenient as it is, saving passwords in your browser comes with a price: low security.

If a hacker gets into your saved passwords, it's like opening a treasure chest full of gold. They have everything they could ever want. Sure, web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this hurdle if given the chance.

"many password managers are designed to suggest new passwords to you when it's time to update your old passwords."

Use a password manager instead. These apps keep all of your passwords in one place, but they come with serious security. Even better, many password managers are designed to suggest new passwords to you when it's time to update your old passwords. LastPass, 1Password and Keeper Security Password Manager are all good options. Find one that suits your needs and the needs of your business.

Eye On It: What's Going On In Tech

Automation, automation, and more automation! Already heading out of this year's 1st quarter and automation improvements are still holding steady when talking about improving your business.

Small Business Trends listed

4 Ways To Improve Business In 2020

Automation – Boost efficiency with automation tools. Think accounting and financial management tools like FreshBooks and QuickBooks or project management tools like Trello. You can also use e-mail marketing apps like Mailchimp.

Accessibility – Make it easier than ever for customers to book your services. Online-scheduling software streamlines the process, allowing customers to schedule times that work for them and you. You can have customers book times on your website or Facebook page.

Employee Engagement – Delegate more, encourage more communication through apps like Slack and celebrate more achievements.

Customer Service – Chatbots and other types of similar customer service-based artificial intelligence are bigger than ever. Use them on your website or direct customers to Facebook Messenger. HubSpot's Chatbot Builder is a good tool to try when getting started.

Trending and we like it!

Personalized Customer Service – People don't want to be treated as numbers.

User Reviews Are More Important Than Ever – This is the first thing people look at before making a buying decision. This is why good, personalized service is so important – it earns you good reviews.

Businesses Recognize Employee Happiness – It's as simple as this: the happier the employees, the more productive they are.

More Remote Workers – Thanks to Internet access virtually everywhere, it's easier for people to work from wherever – and this plays a huge role in employee happiness, too!

This Month's Q&A TeK Tip

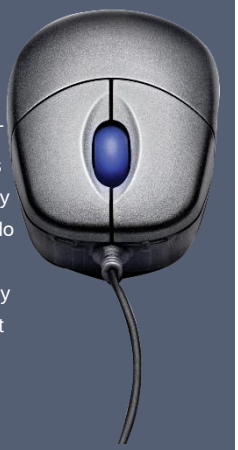
Q: Why are small businesses targeted?

A: How do they work their way into your network and find exactly what they're looking for? Well, it's much easier than you might think. They count on you to have no security. They count on you to have no security. This is why cybercriminals go after small businesses. They know most small-business owners don't invest in security or invest very little. Even if the business does have security, it's generally easy for a hacker to break through.

To make matters worse, if you get hit with a cyber-attack or data breach, it can be incredibly difficult to recover, and many small businesses don't ever recover. They struggle for a few months before finally closing their doors.

This is why you want to pair up with an experienced IT company, like ManagedTek. That's our speciality. It is very hard to run a business and try to be a data security expert at the same time. Thankfully, you don't have to do that. You can get the most out of your equipment, you can be prepared for future growth and you can be ready for the threats to your data! You just have to make that first investment. **Contact us today for a free consultation on developing your personalized security-driven policy for your business.**

info@managedtek.com | 707.205.3727



Cyber Awareness Plan:

The success and survival of your business will be determined by your ability to overcome security threats or breaches. You need a cyber readiness plan that includes elements of prevention, continuity and recovery strategies.

Policies and procedures regulate business operations and are essential for defining the standards and expectations of employee behavior and actions in the workplace. While establishing strict, security focused protocols is essential, a system of validation and enforcement is equally important. After all, rules without consequences are merely suggestions.

Contact us today and let us help you develop security-driven policies and procedures for your business.

Upcoming Events:

Patriot Boot Camp – Mar. 5-7, 2020 (Cancelled and new date TBD)

Channel Partners. Conference & Expo – **March 9-12, 2020** The Venetian & Sands Expo

ConnectIT Global – May 4-7, 2020.

Wingman2020 - June 3-5, 2020

GlueX 2020 – Sep. 27-29, 2020

ManagedTek
1090 Adams St.
Suite G
Benicia, CA 94510
info@managedtek.com | 707.205.3727
www.managedtek.com |