The Tech chronicle

What's New

Announcing Email Multifactor Authentication

With cybercrime on the rise, we have been actively researching additional ways to keep our clients' safe. One new method we are introducing is Email Multifactor Authentication (otherwise known as MFA or 2FA). This service will be available to all of our service agreement customers who utilize our online hosted email solution—and we'll be providing this additional service at no charge as part of our ongoing efforts to increase your security. We will be reaching out shortly to all customers to review this and other newly developed online security measures. If you're not a client of ours, give us a call today to learn more about how we can help protect you and your business.

March 2020

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business.

Clear Signs You're About To Get Hacked — And What To Do Now To Prevent It!

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 sell it on the dark web for an easy profit.

These are habits that you and your employees need to stop right now. 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. It's certainly understandable to share it with a vendor or e-commerce site, (you want to receive invoices and shipping confirmations after all) but other websites just want you to sign up for special offers, notifications, newsletters and other 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.

(Continued on page 2)

Continued from pg.1

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

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.

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

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.

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.

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. Dashlane, LastPass, 1Password and Keeper Security Password Manager are all good options. Find one that suits your needs and the needs of your business.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call 267-381-2025.

4 Ways to Improve Business in 2020

1. 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.

2. 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.

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

4. 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.

Small Business Trends, Dec. 1, 2019

Are You Working SMART?

Rubbermaid thought they needed more products to be an industry leader 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. 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 laying off over 1,100 employees before Newell Corporation came in to buy (rescue) the company.

I had a mentor who once told me, "I don't care how hard you work. I care how smart you work." Rubbermaid was putting in time and money to succeed but at the same time they were destroying their company.

Eli Lilly thought they needed to hire 2,000 PhD researchers to create more products to keep investors happy but they didn't have the funds to hire them. So they had to work smarter.

They decided to take 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 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!

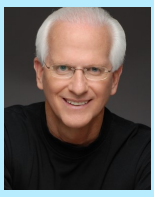
Do you see SMART opportunities in these statistics?

- About 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 work from home? Some managers will say, "That won't work; you won't have control of your employees." 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 homes. Home-based agents save, on average, $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!



Robert Stevenson is a professional speaker and author of the book 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, and Stephen Covey. He travels the world, sharing powerful ideas for achieving personal and professional excellence.*