The Tech chronicle

What's New

Effective immediately, we are offering our Remote Access ScreenConnect solution at no cost. This offer extends through the end of April for managed agreement clients.

If you or any of your staff members would benefit from the ability to work from home please create a ticket in our system with their name and the name of the computer system they work on in the office or give us a call directly.

As your trusted technology partner, we are hopeful that this small gesture will enable your organization to remain productive through these difficult circumstances.

Please reach out if you have any questions or would like information on additional ways you can work productively from remote locations.

April 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.

Employees Are Letting Hackers Into Your Network By Doing These 5 Things

If you run a small business, you are a target for cybercriminals—at this point it's just a fact of life. Hackers and cybercriminals of all kinds target small businesses because they are plentiful, and more often than not, they lack good cyber security. These criminals don't need to use malicious code or advanced hacking skills to get what they want. In reality, many of them target your biggest vulnerability: your own employees.

It's a sad truth, but every day, employees let hackers right in because they don't know better. They see an e-mail from the boss, open it and click the link inside. By the time they realize they've made a mistake, they're too embarrassed to say anything. From there, the problem gets worse. Actions like this can end in disaster for your business.

The problem is that most employees don't have the training to identify and report IT security issues. They aren't familiar with today's threats or they don't know to not click that e-mail link. There are many things employees are doing – or not doing – that cause serious problems for small-business owners. Here are five things people do that allow hackers in through the front door.

1. They don't know better. Many people have never been trained in cyber security best practices. While some of us may know how to protect our network, safely browse the web and access e-mail, many people *don't*. Believe it or not, people do click on ads on the

Continued on pg.2

Continued from pg.1

Internet or links in their e-mail without verifying the source.

This can be fixed with regular cyber security training. Call in an experienced IT security firm and set up training for everyone in your organization, including yourself. Learn about best practices, current threats and how to safely navigate today's networked world.

2. They use bad passwords. Many people still use bad passwords like "12345". Simple passwords are golden tickets for hackers. If they have a username and can guess the password, they can let themselves into your network.

Security experts suggest putting a policy in place that requires employees to use strong passwords. Passwords should be a mix of letters, numbers and symbols. The more characters, the better. Passwords also need to be for every account they have. Employees may groan, but your network security is on the line.

3. They don't practice good security at home. These days many businesses rely on "bring your own device" (BYOD) policies. Employees use the same devices at home and at work, and if they have poor security at home, they could be opening up the business to outside threats.

Combat this by defining a security policy that covers personal devices used in the workplace. Have a list of approved devices and approved anti-malware software. This is where working with an IT security firm can be hugely beneficial. They can help you put together a solid BYOD security policy.

4. They don't communicate problems. If an employee opens a strange file in an e-mail, they might not say anything because of embarrassment or a fear of getting in trouble. But by not saying anything, they put the business at risk. If the file was malware, it could infect your entire network.

> **"The problem is that most employees don't have the training to identify and report IT security issues."**

Employees must be trained to communicate potential security threats immediately. If they see something odd in their inbox, they should report it to a supervisor immediately. The lines of communication should be open and safe. When your team is willing to ask questions and verify, they protect the business.

5. They fall for phishing scams. One of the most common scams is the phishing scam. Cybercriminals can spoof e-mail addresses to trick people into thinking the message is legitimate. Scammers often use fake CEO or manager e-mails to get other employees to open the message.

Phishing e-mails are often caught in the details. For example, the CEO's e-mail might be CEO@yourcompany.com, but the scam e-mail is from CEO@yourcompany1.com. It's a small but significant difference.

Overcoming these threats comes back to training, education and open communication. If someone isn't sure if an e-mail is legit, they should always ask.

Help Us Out And We'll Donte $100 To Your Favorite Charity

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of April.

Simply refer any company with 10 or more computers to our office for our FREE computer network assessment (a $397 value). Once we've completed our initial appointment with your referral, we'll donate $100 to your favorite charity.

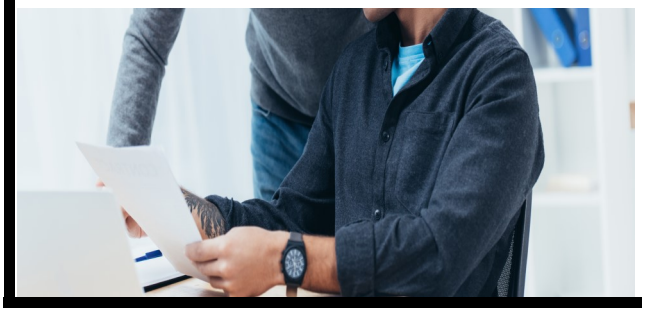
Simply call us at 267-381-2025 or e-mail us at info@canoncapital.com

with your referral's name and contact information today!

Stay Connected While Working Remotely

- Communicate: It may seem obvious, but communicating as much, if not more than you do in person, is proven to help decrease the sense of isolation and loneliness. Enterprise messaging solutions like Slack, Teams or Goolge Hangouts are easy solutions for keeping communication open and instant.
- Outcomes vs. Activity: Micromanaging is not an effective solution in an office, or as a remote leadership technic. Remain focused on outcomes as opposed to trying to monitor hourly activity. You'll remain on top of necessary tasks and can help triage items which aren't getting completed in a timely manner. This also speaks to the amount of trust that you need to have in your team—and that they need to have in you!
- Flexibility: When you can, allow flexibility for your employees. Team members may need to focus on kids or sick family members but with block scheduling and communication you are likely to find that your business unit is more effective when the stress of other responsibilities is acknowledged by the entire team and given its own dedicated time.

Benefits Of A Mastermind Group



I believe no man is an island—if you're an entrepreneur, you need to be in a mastermind. Being in a mastermind group is a powerful tool which can help you increase profitability.

1. What is a mastermind group? If you aren't familiar with them, a mastermind is a group for entrepreneurs to help mentor each other and grow their businesses. It can be an important catalyst for growth and shaping your business. The mastermind I run is called the Edison Collective. We get together face-to-face every quarter to expand our business (and occasional musical) knowledge. We share our ideas, solutions, best practices, successes and challenges as entrepreneurs. Most of all, we motivate and inspire each other.

2. What are the benefits of belonging to a mastermind? While some mastermind groups run on a digital platform, face-to-face meetings are also important. What I love is the connection. We are truly there to learn from each other. No one walks in with their ego. We gather to benefit ourselves and each other by sharing and learning from other experiences. To benefit from a mastermind, you must be willing to collaborate, share and learn. At times, it's almost like free coaching. You get sneak peeks at how businesses run behind the scenes, and oftentimes, we take those ideas and implement them in our own practices. Trust is imperative. There is total confidentiality, so feel free to not be a boss for a bit. I have found that meeting with this group has raised the bar for me. My business is more profitable. I find support from my peers as well as education and resources I may not have been exposed to in the past. Even better, I have another venue for accountability (yup, even I need it!) and a place to share my goals. So next quarter when we meet, I better bring the results!

3. Who can be in a mastermind? The beautiful thing is that you don't have to join an established mastermind. You can start your own. Find like-minded entrepreneurs who are driven to achieve similar goals. Get together once a quarter face-to-face, have open discussions about your business and get your insights from each other. That right there? Priceless!

MIKE MICHALOWICZ started his first business at the age of 24, with no experience, no contacts and no savings, he bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he helps other entrepreneurs. Mike is the CEO of Provendus Group, a former columnist for The Wall Street Journal, a keynote speaker on entrepreneurship and the author of The Toilet Paper Entrepreneur*. His newest book,* The Pumpkin Plan*, has already been called "the next* E-Myth*!" For more information, visit MikeMichalowicz.com.*