TECHMinutes
October 2025
Your Technology Information Source!

This Issue:

Quiet Cracking: The Silent Erosion of Employee Well-Being

Business owners like to talk about things like time theft and quiet quitting as reasons why they wring their hands over lost productivity, and unfortunately, it's almost always their view that it is the erosion of a strong work ethic. What if the real problem isn't about employees checking out, but rather, something far more on the nose? Let's talk about quiet cracking...

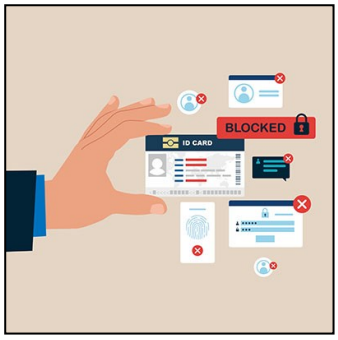
Read the Rest Online!
https://dti.io/shhcracking

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

The One Thing Standing Between Your Business and a Ransomware Attack



What's the one thing protecting your business from a ransomware attack? If your answer is *"our antivirus software*," we seriously need to discuss this further. While well-intentioned, that belief is a dangerous gamble.

Modern cyber threats are too sophisticated, and the stakes—your data, your reputation, your entire business—are too high. The hopefully-correct answer to that *"one thing"* question is much more powerful.

Many small business owners across Central New York believe they're too small to be a target. *"What would a hacker want with my little operation in Oneonta?*" The answer is simple: your **data** and your **money**.

It's nothing personal; it's just business for them.

Hackers see small and medium-sized businesses as soft targets, often holding valuable data but lacking the robust defenses of a major corporation. They know you need your client lists, financial records, and operational data to function, and they're betting you'll pay to get it back.

(Continued on page 2)

Digital Tug-of-War: Achieving Both Productivity and Cybersecurity

Do you feel like you're walking a tightrope between getting things done and maintaining the security of your network and data? You're not alone. Ultimately, we're all trying to be as productive as possible, and we want to use all the cool collaboration tools, work from anywhere, and get things done fast.

Unfortunately, there's the other side of the coin, too; and maintaining security can throw a wrench in those plans if not considered completely. Obviously, the Internet is a wild place, full of hackers, scammers, and all sorts of other digital dangers. That's why every organization that cares deploys firewalls, multi-factor authentication (MFA), and complex password rules to keep us safe.

It's a classic tug-of-war. If you are too aggressive and set up too many roadblocks, it can be frustrating to users, but if you leave things too open, you set yourself up for problems.

With everything going on, how do we find a happy medium? The trick isn't to choose one over the other. It's about making security and productivity work together.

Don't Just Dictate Rules, Explain Them

Instead of just telling people what to do, help them understand why it's important.

(Continued on page 3)

Is Your Business Covered? What SMBs Need to Know About Cyber Insurance

Cyberthreats are a constant, evolving risk. While robust cybersecurity measures are the first line of defense, they are not a silver bullet. This is where cyber insurance comes in—not as a replacement for security, but as a critical component of a comprehensive risk management strategy.

For small-to-medium-sized businesses (SMBs), the financial fallout from a data breach or cyberattack can be catastrophic, including legal fees, regulatory fines, and the devastating loss of revenue due to business interruption. Cyber insurance provides a financial safety net against these potential liabilities.

What Cyber Insurance Covers
Cyber insurance is a specialized policy that addresses the unique risks of the digital world. While standard business liability insurance typically excludes cyber incidents, a dedicated cyber policy can cover a wide range of costs, often separated into two categories...

Read the Rest Online!
https://dti.io/cyberinsure

Cybersecurity Made Easy: Four Tips for Every User

From online banking and shopping to social media and remote work, we're constantly sharing information. While our digital lives offer incredible convenience, they also expose us to a growing number of cyberthreats.

Cybercriminals are always looking for new ways to exploit vulnerabilities and steal personal information. Fortunately, by adopting a few key habits, you can significantly reduce your risk and protect your data. Here are four things every user needs to remember to help them avoid cyberthreats.

Master the Art of the Strong Password

Your password is the first line of defense for your online accounts. A weak, easily guessable password is an open invitation for hackers. Stop using common passwords and avoid using personal information that is readily available, like birthdays or pet names.

A strong password is a combination of:

- **Length** - Aim for at least 12-to-16 characters.
- **Complexity** - Use a mix of uppercase and lowercase letters, numbers, and special symbols.

Uniqueness - Use a different, unique password for every single account. This is crucial because if one of your accounts is compromised in a data breach, your other accounts will...

Read the Rest Online!
https://dti.io/easysecurity

The One Thing Standing Between Your Business and a Ransomware Attack

(Continued from page 1)

Why Your Antivirus Isn't the Silver Bullet You Think It Is

For decades, antivirus software was the go-to solution for computer security. It worked by identifying the digital *"signatures"* of known viruses, much like a detective matching fingerprints to a database of known criminals.

Modern ransomware is designed to be unrecognizable. Hackers constantly change their code to evade signature-based detection. Relying solely on basic antivirus software is like locking your front door while leaving every window on the ground floor wide open. It might stop a casual intruder, but it won't stop a determined professional.

Building a Proactive, Layered Defense is the Only Effective Strategy

The *"one thing"* that truly protects your business from ransomware isn't a single product. It's a strategy. A modern, proactive, and layered security strategy that works like a medieval castle's defenses. You don't just have a wall; you have a moat, a drawbridge, high walls, watchtowers, and guards patrolling the interior. Each layer makes it harder for the enemy to succeed.

This is the approach we take at Directive:

Advanced Threat Detection

You can't rely solely on identifying known issues. You need to actively monitor for any suspicious behavior. This is accomplished through Endpoint Detection and Response (EDR), a technology that constantly monitors your systems for unusual activity—a program attempting to encrypt files, for example—and can stop an attack in...

Read the Rest Online!
https://dti.io/ransomattack

Digital Tug-of-War: Achieving Both Productivity and Cybersecurity

(Continued from page 1)

When your team knows why a strong password or a security update is necessary, they're more likely to follow the rules willingly. Think of it like teaching someone to look both ways before crossing the street; once they understand the danger, it becomes second nature.

Make Security Simple to Use

Security doesn't have to be a headache. Look for tools that are both effective and easy to use. A password manager can create and remember strong passwords for you, and single sign-on (SSO) lets you access all your apps with one login. The easier it is, the more likely people will use it.

Give People Only What They Need

This is a simple but powerful idea. Only give people access to the files and programs they need to do their job. This way, if someone's account ever gets compromised, the damage is contained.

Automate the Boring Stuff

The less people have to think about security, the better. Use tools that can handle things automatically, like updating software or scanning for...

Read the Rest Online!
https://dti.io/bestofboth

The Basic Dos & Don'ts of Business Continuity Planning

Any business can face a variety of disruptions, from natural disasters to cyberattacks. While many organizations understand the importance of preparing for the unexpected, not all of them have a solid plan in place. A well-crafted business continuity plan (BCP) is crucial for protecting your employees, customers, and bottom line.

Here are some key dos and don'ts to consider when creating your business continuity strategy.

The Dos

Conduct a Thorough Risk Assessment.

Before you can build a plan, you need to know what you're up against. Identify potential threats and vulnerabilities specific to your business, such as your location, size, and services. A risk assessment will help you determine the most likely scenarios and the resources you need to mitigate them.

Test Your Plan Regularly

A plan that sits on a shelf is useless. Regularly test your BCP through drills and simulations to find any gaps or weaknesses. This practice ensures your employees know their roles and responsibilities in a crisis and that the plan is viable in a real-world situation.

Include All Employees

Business continuity is not just for senior management or the IT department. Every employee plays a part in the plan's success. Make sure all staff are aware of the protocols, communication channels, and what to do during an emergency.

Have a Communication Strategy

During a crisis, clear and consistent communication is paramount...

Read the Rest Online!
https://dti.io/plan4disaster

CYBERSECURITY TIPS

Attack Surfaces: Physical and Digital

If attack vectors are the method that cybercriminals use to infiltrate a network, an attack surface is the number of potential entry points.

In this Micro Training, we will learn more about attack surfaces and their physical and digital states.

View this tip and others at:
https://dti.io/pdattack

Get our Cybersecurity Tips directly to your inbox!

Sign up to receive our **FREE** cybersecurity tips to help you to avoid a data breach or other compromise. These tips can be used to educate yourself and your employees on security best practices.

Sign up today!
https://dti.io/gettips

REVIEW US ON Google

We would ***love*** to hear your feedback, and would be incredibly grateful if you could take a couple of minutes to write a quick Google review for us. This will allow us to improve our service and let others recognize the value we provide.

Thanks in advance!

https://directive.com/review

Marketing Ideas & Tips for Your SMB

It Pays to Team Up with Other Businesses

While marketing may feel like a fiercely independent endeavor for every business, this is only half true. Sure, you may not want to promote one of your direct competitors… but why not work with another company, in a different industry, to meet both your goals?

This approach is almost a marketing cheat code, the rising tide that raises all ships.

Let's talk about why such partnerships are so valuable and how to take advantage of the marketing advantages for yourself.

Why are Inter-Industry Marketing Partnerships Worth Pursuing?

There are numerous reasons why joining forces with another business to pursue marketing opportunities is an excellent strategy to follow. For instance:

You Grow Your Audience without Shrinking Your Available Funds

Growing your business is, typically speaking, an expensive endeavor. To effectively publicize your services and attract those who would benefit from them, you need to invest in outreach and lead generation. At least, that's typically the case.

However, if you form a partnership with another business, you can effectively share these costs and both benefit from building an audience. This also allows you...

Read the Rest Online!
https://dti.io/bizteamup

Community Spotlight: Otsego County Conservation Association

We're lucky to have our base of operations here in Otsego County, where we can not only serve our community but also appreciate the other organizations around us who do the same. Take the Otsego County Conservation Association, for example.

The OCCA is a conservation organization dedicated to promoting sustainability and environmental appreciation, offering programs to protect the air, land, and water. First established in 1968, OCCA has spent the past few decades working to address nearly every environmental issue we face today. From water quality, the environmental impacts of development, and land-use planning, the efforts of the OCCA have made quite a difference… and the association has plans to continue moving forward.

We recommend that you learn more about their mission and see opportunities to support them by visiting their website at **occainfo.org.**

HAVING AN IT ISSUE?

EMAIL SUPPORT
support@directive.com

CHAT WITH US
chat.directive.com
607-433-2200.

TICKET PORTAL
support.directive.com

MANAGED RESOURCES
Use the icon in your desktop system tray for support options, quick links!

Charlotte & Chris Chase

Tech Trivia
Google blocks around 100 million phishing emails daily.

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
x.directive.com
instagram.directive.com
blog.directive.com