A Special Edition Of MSP Success

MSP CYBERSECURITY MAGAZINE

How ThreatLocker Is Using 'Zero Trust' To Change The Cybersecurity Game

The 5 Cybersecurity Protections

That Will Save Your Business

Greg Brainerd, Founder And CEO Of Braintek

5 Ways Top MSPs Are Utilizing Malwarebytes Partner Program

To Capitalize On The Growth Of Investment In Managed Security Services

As Phishing Evolves, So Does The Need For Prevention Strategies

MSP SUCCESS

MSPSuccessMagazine.com/cyber2022

CONTENTS

Special Edition Of MSP Success Magazine

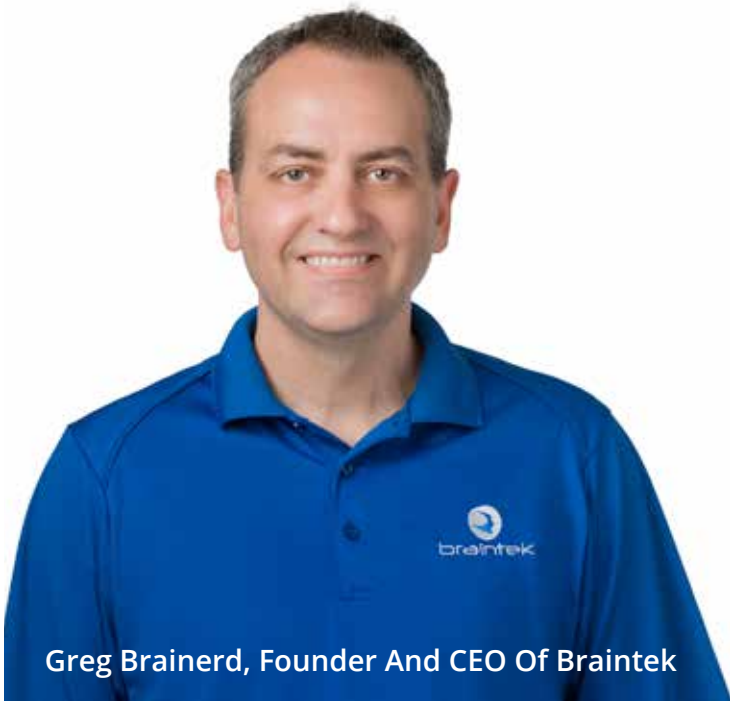
The paper used in the production of MSP Success Magazine includes post-consumer waste and is produced using sound environmental practices and operations. Our paper has FSC certification and passes the SFI Chain-of-Custody Standard. Read more at WFPaperCo.com/sustainability.html.

10

The 5 Cybersecurity Protections That Will Save Your Business

THE 5 CYBERSECURITY PROTECTIONS

THAT WILL SAVE YOUR BUSINESS



Greg Brainerd, Founder And CEO Of Braintek

Everyone knows they shouldn't be using the same password for all their accounts, e-mail addresses and social media. Or that their passwords should be strong, with a combination of letters, numbers and symbols. Or that they need to switch up their usernames instead of using their e-mail address. So, why do they keep doing it? The same reason they continue to click on phishing scams they've been warned about so often. They don't take cyber security seriously. But who is *they*?

"Most of us," says Greg Brainerd, founder and CEO of Braintek, one of Houston's most successful IT support and managed IT services companies. "Especially small to medium businesses that think they aren't worth a cybercriminal's time. It's been said more than once, and there is a reason for that – if you're an SMB, it's not a matter of *if* you suffer a cyber-attack but *when*."

Forty-three percent of cyber-attacks happen to small businesses because they aren't prepared to defend themselves. And at the end of the day, it's less effort with a bigger payday for hackers to go after 20 SMBs and demand ransom than try to penetrate ONE larger company's cyber security systems.

While it's true that bigger businesses may face security threats on a larger scale, SMBs are more susceptible to hacking, e-mail phishing, malware and ransomware. But there are tools to help combat some of today's most pressing threats.

First Things First There Is No SINGLE Solution

For Greg Brainerd, cyber security is a layered approach.

"Think about your house," he says. "So, you've got the front door and the back door, your most common entry points. But then there are the windows. You've got your motion sensors, your cameras, your alarms. Maybe you've got flood detection or fire detection. Maybe you even have a guard dog and community watch program. You've got all these different layers of protection for your house. Think of it the same way for your computer systems. Multiple points of entry require multiple protections."

Implement Two-Factor Authentication

"Yes, it's a pain in the ass, but it's necessary. And before long, most apps, e-mails and online businesses we do business with will require it," says Greg.

Two-factor authentication is a simple precaution, an added layer of protection that's used to ensure the security of your online accounts beyond a username and password. 2FA, as it's commonly known, cross-verifies users with two different forms of identification – most commonly, knowledge of an e-mail address and proof of ownership of a mobile phone.

"When I hear the pushback and grumblings from business owners, I always ask, 'What are you willing to risk? And is that worth it for a few seconds of your time to verify a 2FA?'" Greg says. "It happens over and over in different scenarios. For example, you have an accounts payable person who just got an e-mail from someone she believes is a vendor, asking her to verify her account on Microsoft. Turns out it's a phishing scam, and now they've gained access to her account. Two-factor can stop this problem. Well before it becomes a requirement, companies should start practicing it now."

Take Advantage Of Password Managers

Keeping up with passwords is a hassle. So, to combat their frustration at trying to remember them all, most people come up with easy, weak ones and share them across all their accounts. It's just one password to remember for every login. Convenient, right?

"Convenient for cybercriminals, that's for sure, if you use the same password and username for everything," says Greg. "Once

a hacker can unlock one of your passwords, he's potentially gained access to every account that uses that same password. And if he gets into your e-mail, he can reset passwords to various systems and applications you might be using."

Having a password manager that helps generate complex passwords and stores login information for all the websites you use not only keeps your password safe with encryption but logs you in automatically – eliminating the need to remember all your password and username combinations. "All you have to do is remember the master password for the password manager," says Greg.

Embrace Robust Malware Protection

"Some SMBs have a set-it-and-forget-it mentality when it comes to malware protection. They install basic or free antivirus software on their computers and systems and expect that to be the only line of defense they need for threat protection," says Greg. "But as threats become more sophisticated as the days go by, cybercriminals have already gotten around it. That's why businesses today need whitelisting software to stop malware practices."

Whitelisting applications is a "Zero Trust" security approach. It specifies an index of approved software applications and executable files that are allowed to be present and active on a computer system. The goal is to protect computers and networks from potentially harmful applications.

"By the way, everybody hates it because it doesn't trust anything. But everybody loves it because it doesn't trust anything," says Greg. "Essentially, if you are installing new software and you haven't told the computer it's OK, the computer doesn't 'see it' on its 'whitelist' so it blocks it. Our clients just have to call us up and say, 'Hey, I'm trying to use this legit software, can you whitelist it for me?' Sometimes having that extra level of security can be a pain, but just keep asking yourself this: what are you willing to risk?"

Don't Forget About Backups

Hackers attack every 39 seconds. With a potential security breach just seconds away, backing up your sensitive data routinely is a no-brainer.

"The best time to prepare for these types of threats is always before they happen," says Greg. "It can protect sensitive business data, not to mention help reduce management stress levels during an emergency response phase."

With nearly everything living online or in the cloud these days – personal identification numbers, competitor information, financials – everything is susceptible to potential harm if not fully protected. Backups should be a routine part of any cyber security plan.

Make Security Awareness Training Mandatory

Make cyber security an ingrained part of your company culture. Getting your entire team on the same cyber security page is essential to keeping your systems safe from attacks. Security awareness training should be an important part of your culture.

"At Braintek, we make education a priority with our clients," says Greg. "We offer training, videos for spotting and recognizing threats, we do phishing simulation tests, we send out monthly two-minute-read e-mails with little quizzes. It helps keep the possible threats REAL.

"We know cybercriminals are working overtime to steal data from SMBs. That's why we offer a full range of cyber security protections for every budget. It starts with a security risk assessment from Braintek," Greg adds.

At no cost or obligation, Braintek will send you a link that you will run on five computers, which will simulate a phishing attempt and conduct a noninvasive, CONFIDENTIAL investigation of your computer's network and security protocols. Your current IT company or guy DOES NOT NEED TO KNOW we are conducting this assessment. Your time investment is minimal once the scans are completed: a one-hour meeting to go over our Report Of Findings.

You've spent a lifetime working hard to get where you are today. Don't let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don't "hope" your IT guy has you covered. Get the facts and be certain you are protected.

Learn more at www.braintek.com/services/cyber-security-risk-assessment. ■

braintek
Business Computer Solutions