www.CDTechnology.com

August 2024

TECHNOLOGY TIMES

Insider Tips to Help Your Business Run Faster, Easier and More Profitably

Thomas Hill, President & Founder

“In everything we do, we work to help small businesses maximize technology for long-term success!

TRIVIA

CONGRATULATIONS

Tiffany Garner, CPC

with

WellKey URGENT CARE

Who knew that the average person unlocks their smart phone 150 times a day!

TURN TO PAGE 3 FOR THIS MONTHS TRIVIA

WHAT DO YOU DO WHEN A COMPANY COMPROMISES YOUR DATA?

With the rise in cyber-attacks worldwide, you’ve likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can’t control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers’ personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent example is ChangeHealthcare, breached in February of this year. Due to this breach alone, it’s estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, “Whoops, we got breached.” It’s more than upsetting to think that your data is now in the hands of criminals.

When sensitive information leaks, you’ll have to do some recon to protect your accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

Here’s What To Do After Your Data’s Been Leaked

1. First, make sure the breach is legit. One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an

continued on pg.2

continued from cover

alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen.
After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.
After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.
Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.
If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.
Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even *more* sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

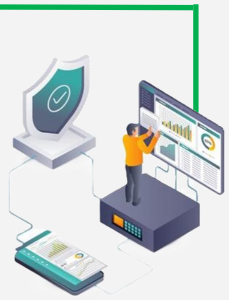
"The single biggest benefit for our company since working with CD Technology is peace of mind. Their responsiveness and availability is far better than our previous IT company. I tell people, you will not regret switching to CD Technology!"

SMARTSITE COMMERCIAL REAL ESTATE ~Jake Brewer
Principal
Broker
SmartSite Commercial Real Estate

7. Consider identity theft and data breach protection.
Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an

Free Cyber Security Assessment 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 assessment to uncover loopholes in your company's IT security.

After this 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 865-909-7606.
www.CDTechnology.com/ITsurvey

MICHAEL MICHALOWICZ

EXPLAINS HOW TO BUILD A TEAM THAT CARES ABOUT YOUR COMPANY'S SUCCESS AS MUCH AS YOU DO

Early in his career, Mike Michalowicz was eager to announce to his team a new corporate vision for the year: a $10 million revenue goal. However, what he imagined would be one of his greatest visionary moments as a leader was one of his biggest mistakes.

After revealing the vision to his team, "it was total silence," Michalowicz explained to a room of business leaders at a recent industry conference. "A colleague came over to me and said, 'Mike, if we achieve $10 million in revenue, you get the bigger house. You get the new car. That's your vision. What about our vision?'" This was a transformative learning moment for Michalowicz, who committed himself to learning what it takes to be a GREAT leader.

Today, Michalowicz is the author of several books, including Profit First, Get Different, The Pumpkin Plan and other small business must-reads. He's an entrepreneur and speaker teaching other leaders how to build and retain unstoppable teams who care about the company's success as much as you do, so you'll be happier, grow faster and create an environment where everyone flourishes.

How To Build An Unstoppable Team

1. Most leaders tell their team what to do. Great leaders ask their team what they could do.

One of the Baltimore Museum of Art's most successful exhibits was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn't unique to the one guard, and a group was assembled to create "Guarding the Art." Michalowicz explains that great leaders encourage ownership by asking, "What could we do ?" rather than always telling their employees what to do.

2. Great leadership assembles and unifies.

The movie The Boys in the Boat recounts how an inexperienced US rowing team won gold in the 1936 Olympics. The leader helped the team connect, communicate and work together to win against all odds. He fostered deep trust within the team, which Michalowicz says distinguishes great leadership in any circumstance.

3. Great leaders follow a FASO model.

Michalowicz's research and experience in leadership culminate in a four-part model he calls "FASO." Leaders who want to be great can use FASO to assemble an unstoppable team.

F – "Fit." When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.

A – "Ability." Great leaders look for people's raw potential. Do they have curiosity, desire and a thirst for the role? That's what great leaders hire and recruit for, not simply experience and innate ability.

S – "Safety." Great leaders account for their team's physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.

O – "Ownership." "When we're forced to comply, we'll seek to defy," Michalowicz says. Great leaders encourage their team to personalize, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, "No one cares how you care; they care THAT you care." Show your team you care by working to incorporate these great leadership approaches in your organization.

Top 5 Reasons to Choose CD TECHNOLOGY

Call (865) 909-7606
To schedule a FREE
10 minute discovery call

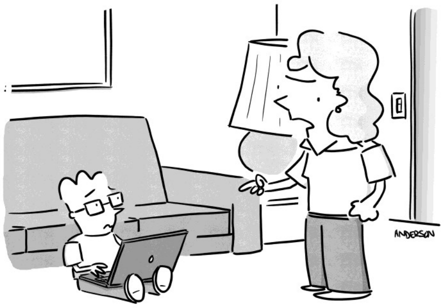
1. **Prompt Response Time**
We begin working on your issue in 20 minutes or less during normal service hours.

2. **We Have Been Serving East Tennessee for almost 3decades.**
As a locally owned and operated business, you are our neighbor!

3. **We Are Your IT Service Department**
WE take care of it. No blaming, no finger-pointing. We Focus on the Fix.

4.**Freedom of Choice**
There are No Long-Term Contracts to sign.

5. **90-Day Test Drive**
What is better than risk-free?!



"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

Here is your chance to win
Lunch On Us!
This Month's

TRIVIA

Worldwide, more people have access to cell phones than to toilets. True or False?

Email your answer to
RHill@CDTechnology.com

CD TECHNOLOGY
10721 Chapman Hwy #30
Seymour, TN 37865

PLACE
STAMP

August 2024

INSIDE THIS ISSUE

CD TECHNOLOGY - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

Don't Make This Mistake With Your Home's Smart Tech

Smart devices are so pervasive in our homes, it's hard to imagine what life was like before them. From door cams to AI-powered devices, we truly live in "smart" homes.

But unlike devices of the past, you can't "set and forget" smart devices. These tools are connected to the Internet, where hackers keep a close eye out for unprotected devices. When hackers find an unprotected device – like an indoor cam that you never bothered to change the default password, they can access sensitive information including your address, birth date, e-mail address and phone number. They use this information to create a profile about you and carry out targeted attacks. When they access a devise with a weak password, they can carry out terrifying crimes like watching your family through a home camera. A family in Mississippi even had a hacker taunt their young daughter through their ring camera. Before you plug in your smart device, follow these simple steps to make sure it's not an open door for peering eyes.

Steps To Keep Your Smart Home Safe

1. Change the default login information immediately. Default passwords are low-hanging fruit for hackers, so be sure to change this to a new, stronger password right away.

2. Make sure your WiFi is secure. If your WiFi password is a few years old or you use the same password on other accounts, change it to a stronger password.

3. Enable multifactor authentication (MFA) in security settings. This way, users can only log in with a security code or authenticator app, making it nearly impossible for hackers to get in.

4. Regularly update the device. Updates fix issues or add new features that may improve your security. Don't skip these updates. If your smart device doesn't update automatically, set a reminder in your phone to check for updates periodically.

5. Consider separate networks. Many WiFi providers offer guest networks. Consider connecting smart devices to a home guest network separate from the one that your phones or laptops are on. This way, if a smart device is hacked, it's not a straight shot to devices holding more valuable information.

The biggest mistake smart-device users make is thinking they can plug in their devices and walk away. Make sure your devices are not an open door to creepy criminals.

Contact Us

CD TECHNOLOGY

Serving our
East Tennessee
Neighbors

For over 25 years

5416 S Middlebrook Pike
Knoxville, TN 37921
Phone: (865) 692-4247

or

10721 Chapman Hwy
Seymour, TN 37865

Phone: (865) 577-4775

Email: thill@CDTechnology.com

Visit us on the web at
www.CDTechnology.com