TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

Quest Diagnostics Suffers Massive Data Breach

Chances are good that you or someone you know has had some type of medical testing done by the US Clinical Laboratory, Quest Diagnostics. If that's the case, then there's bad news.

The company recently announced that they've suffered a massive data breach that exposed personal, confidential patient information of more than 11.9 million people.

Read More Here:

www.optistartech.com/quest/

July 2019

This monthly publication provided courtesy of Mark Jordan, President of Optistar Technology Consultants

Our Mission :

To help small businesses succeed by providing the highest quality IT CONSULTING, solutions and support money can buy.

The Shocking Truth Behind The Growing Cybercrime Threats You Face...

And What You Can Do NOW To Protect Your Company

Are businesses losing the war on cybercrime? One recent article on *ZDNet* says yes. The number of security breaches has risen by 11% just in the last year. This is costing businesses even more in lost revenue dealing with these kinds of attacks. It's wasting their time and resources.

In 2016, Cybersecurity Ventures stated that by 2021, digital crime will cost businesses a total of $6 trillion. So far, this projection seems on point as hackers continue to chip away at businesses around the world. They don't care about the damage they're doing.

Right now, the Internet is flooded with sensitive data. From passwords to financial information – it's out there. Some of it is secure, some of it isn't. Either way, because of the sheer amount of data floating out there, cybercriminals have a greater chance to get what they want. And over time, it becomes harder to protect that data.

But the cyber security industry has also grown in response. People are fighting back. In 2018, the investment into cyber security totaled $37 billion. However, it seems like it's just not enough. When you look at small and medium-sized businesses – the targets of nearly 70% of cyber-attacks, according to SMB Group – cyber security isn't taken as seriously as it should be.

In 2017, *Harvard Business Review* looked at the reasons behind why many businesses don't take cyber security seriously. The results were interesting. It turned out, businesses don't treat cyber security as "the ongoing process that it is." Instead, it's typically treated as a "finite problem that can be solved." In other words, if you do the bare minimum for security today, the thinking goes, you'll be protected tomorrow.

Continued on pg.2

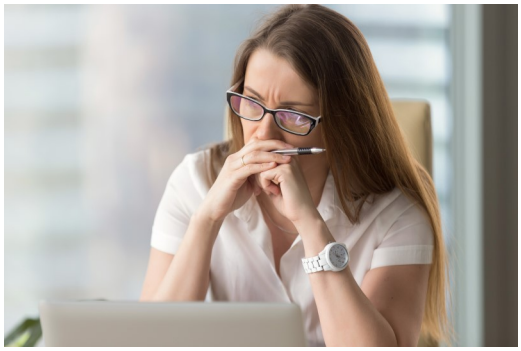
Continued from pg.1

The problem is as the Internet changes and evolves, so do the threats against its users. It's pretty much impossible to set up a one-and-done security solution. If you were to set up something like an SMB "quick fix" and walk away, there's a good chance your business would be the successful target of an attack within a matter of months.

This kind of thinking is far more costly than many business owners realize. A study by Akouto and Alpha Logistics found that businesses that underinvest in cyber security end up spending more on cyber security in the long run as they deal with attacks – up to 58% more. These costs don't even include downtime or lost wages caused by data breaches. In short, recovering from an attack is FAR more expensive than investing in security now.

So what can you do to protect your business? You can start with changing the way you think about cyber security. You have to accept that the threats are out there and will always be out there. But there are things you can do to minimize those threats.

Start with your people. For many businesses, especially those smaller than Fortune 500 companies, your biggest threat is right inside your organization. For those of us who are Internet-savvy, most would never dream of clicking on a scammy link or responding to a phishing e-mail. We've been around the cyber block and we know what to look for.



However, people still fall for even the most basic scams. There will always be someone on your team who isn't informed about these kinds of threats, or those who use obvious passwords. *ZDNet* points out that "only 26% of workers know what to do in the event of a breach" and that "7% openly acknowledge that they ignore or go around security policy."

It pays to invest in a thorough and ongoing training program. It's crucial to outline clear and firm security protocols so your team knows EXACTLY what to do. No one's left guessing or clicking on anything they don't recognize.

It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider who is up-to-date on the threats you're facing. Having a partner means you don't have to assume your business is protected. You'll *know* your business is protected.

Contact us at 888.782.7003 so we can ensure your organization is protected.

"It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider ..."

Are Your Digital Credentials For Sale On The DARK WEB?

Visit

www.optistartech.com/darkweb/

For A Free Dark Web Scan!

Shiny New Gadget Of The Month:

Logitech's Circle 2 Home Security Camera

The Internet age has made home security a straightforward affair, and with Logitech's popular Circle 2 home security camera, it's easier than ever to get in on the action. Equipped with 1080p livestreaming, a wide 180-degree viewing angle, free 24-hour event-based cloud storage and rated for both indoor or outdoor use, it's a powerful tool for keeping your home safe, whether you're there or not.

The device works seamlessly with all the popular smart home platforms, including Amazon Alexa, Apple HomeKit and Google Assistant, and it is easy to set up. It offers crystal-clear video night or day and is easily viewable from your phone wherever you are. If you're in the market for a smart home security system, this is the place to start.

Florida City Paid Big Bucks To Hackers Using Ransomware

The city of Riviera Beach, Florida is the latest high-profile victim of a ransomware attack.

Recently, the city council voted to pay more than $600,000 to a hacking group to regain access to data that had been locked and encrypted via ransomware nearly a month ago. That is in addition to the $941,000 the city will be paying for new computers.

An investigation into the hack revealed that the trouble began when a Riviera Beach police department employee opened an email from an unrecognized, un-trusted sender. That's all it took to bring the entire city government network to its knees. Since May 29th, all city services have been suspended except for 911 services, which have been able to continue in limited fashion.

The city council didn't initially plan to pay the hackers off. Their first move was to vote to spend the money to get new computers and rebuild their IT infrastructure. Since that time, however, the city's IT staff has been unable to decrypt the files on their own. In light of the lack of progress, the city council reconvened and voted 5-0 to pay 65 Bitcoins to the hackers (which amounts to a little over $600,00 USD at the time this piece was written).

Riviera Beach, a suburb north of Palm Beach, Florida, isn't the only local government to fall victim to hacking groups or ransomware attacks. Earlier this year, officials in Jackson County, Georgia paid more than $400,000 to regain access to their files. To date, the highest ransom paid to hackers employing this tactic was $1.14 million USD, paid by South Korean web hosting firm Internet Nayana.

Last year was a record-setting year for the number of successful hacks. This year is on track to beat it by a wide margin. Your company could be next.

Call us at 888.782.7003 for information on how you can secure your data, thus avoiding losing anything to ransomware attacks!

At Optistar Technology Consultants, we believe that referrals are the greatest form of flattery. If you know of someone who is worried about any aspect of their business technology, do them a favor and put them in touch with us!

Visit www.optistartech.com/referral/
or call us at (888)782-7003

45-18 Court Square, Suite 602
Long Island City, NY 11101, USA

Optistar Technology Consultants has been providing expert Information technology advice, help and services to small and medium businesses since 1996.

Most of our clients hire us to support their network because they do not want to incur the overhead and cost of full time IT staff and they do not want to burden their employees with the responsibility of troubleshooting the company network.

For over 20 years, Optistar has built a reputation for providing superior strategic IT consulting and solutions for its customers which has set us apart from the typical computer consultant and other providers.

Need help or have a question? Call us at 888-782-7003 or shoot us an email at ask@optistartech.com

"Wow. What a week, huh?"