Dimensional Dispatch

7th Dimension Newsletter

7th Dimension
5005 Windplay Drive, Ste. 1
El Dorado Hills, CA 95762
(916) 221-0855

March 2018

"INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY"

IN THIS ISSUE

"Lucky Charm" Keeps Hackers Out

What you need to know to keep you and your employees safe while browsing online.

Whether you are already monitoring user activity on your network or not, it is imperative to stay vigilant about evolving risks—and content filtering is key.

If your business is like many, you may already be doing some filtering. However, is it enough? As technology evolves, hackers drum up ever-stealthier ways to invade your network.

Cloud-based filtering, for example, becomes necessary when mobile devices tap into your network. The old concept of a static, location-based "firewall" just does not cut it anymore when your staff goes mobile.

Then there is social media. It is like a big window into the personal lives of your personnel. It lets cybercriminals "case the joint" before breaking in. For instance, when users log into a personal Facebook account at work and talk about vacations, favorite hangouts or weekend activities, hackers can use that information for social engineering and other ploys.

The number of ways your network is exposed to potentially damaging content grows daily. It is no wonder that 90% of companies and government agencies surveyed by IDC detected computer security breaches within the previous 12 months.

Eighty percent of those organizations acknowledged financial losses due to these breaches. With odds like that against you, an up-to-date content filtering system could well be THE "Lucky Charm" that keeps your company—and your data—safe from all kinds of harm.

How do you know if your hardware and software is prepared for modern security threats? Speak with your I.T. professional today about a complete security audit of your network.

Another Reminder of Why You Cannot Use Home Routers in Your Business

We break down the security flaws in home use hardware.

Page 2

How Cybercrime is Hurting Businesses

Cybercrime is costing worldwide business $600 billion.

Page 2

Another Reminder of Why You Cannot Use Home Routers in Your Business

A hacker reportedly stumbled upon a back door to Linksys and Netgear DSL modems last year, which allowed an attacker to reset the router's configuration and gain Admin access. Not good!

Some routers have this "back door" open to the local computer network while others are open to the Internet side of things, opening up users of these devices to remote Internet attacks. This essentially means that someone could easily gain access to the network and all files located on it.

In the past, this may have taken weeks or months to get out, leaving plenty of time for the manufacturer to get in contact with their clients, right? Not so anymore. In this instance, the exploit was promptly posted up to GitHub in a PowerPoint explaining all of the details and how to exploit the devices. Many others started trying this out (just for fun, of course), and confirmations started flooding in immediately for all to see.

The Bottom Line: If you are concerned at all about the security of the data on your network, you need to have a real, business-class firewall and router in your office. These days, it doesn't pay to go cheap on IT security.

Password Tip! Want an easy-to-remember password that's super-secure? Try mixed-entry passwords. While JohnSmith12345 could fairly easily be broken, J102h3n4S5mith (inserting the same numbers between each letter in the password) would take about 1,800 years to crack, and is almost as easy to remember!

UNSURE IF YOUR NETWORK EQUIPMENT IS PROTECTING YOUR BUSINESS, CLIENTS AND EMPLOYEES?
CALL US AT (916) 221-0855 FOR A FREE CONSULTATION

How Cybercrime is Hurting Businesses

A recent report from McAfee details how cybercrime is getting easier for criminals daily.

In February, McAfee and the Center for Strategic and International Studies released a report explaining that cybercrime may be costing businesses worldwide about $600 billion.

How is this happening? Ransomware is the biggest culprit and fastest growing technology crime. Ransomware is a malicious software that can lock your computers, servers and even any external devices. Once you are locked out, hackers hold your files ransom. Even if victims pay the hefty price to their attackers, there is no guarantee of getting their files back.

Cybercriminals often demand this payment in a virtual currency, such as bitcoin.

So, what can be done about this huge cost for businesses? According to the report, "Cybercrime is relepntless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low."

Unfortunately, these criminals are not going anywhere and their attacks will continue to increase. It is important to take every precaution you can to keep you company's information, your employees' information, and your customers' information secure.

The report goes on to explain that, "Uniform implementation of basic security measures (like regular updating and patching and open security architectures) and investment in defensive technologies—from device to cloud—remain crucial."

By speaking with your trusted IT partner, you can design a security plan within your budget. (Economic Impact of Cybercrime No Slowing Down, McAfee)

Keep Your Network Safe

Don't let your company become another statistic. Call us (916) 221-0855.

Protecting Personal Information

What steps are you taking to keep your personal information secure? The Federal Trade Commission (FTC) has provide some guidelines to safeguarding your information.

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

A sound data security plan is built on 5 key principles:

TAKE STOCK. Know what personal information you have in your files and on your computers. Evaluate your processes and levels of access and assess if there are any risks you can remove.

SCALE DOWN. Keep only what you need for your business. If you don't have a legitimate business need for sensitive personally identifying information, don't keep it!

LOCK IT. Protect the information that you keep. Your business should have physical securities on for paper documents and electronic securities for all files stored on computers and servers. Audit your security frequently for any potential threats or weaknesses.

PITCH IT. Properly dispose of what you no longer need. Trash can be a goldmine for an identity thief. Properly disposed information cannot be read or reconstructed.

PLAN AHEAD. Create a plan to respond to security incidents. Taking steps to protect data in your possession can go a long way toward preventing a security breach. (FTC 10.2016)

Ready to audit your securities? Is your password information for sale on the Dark Web?
Call us at (916) 221-0855 to schedule a Dimensional Dark Web Scan and Security Audit.

7TH DIMENSION

IT without limits

5005 Windplay Drive, Suite 1, El Dorado Hills, CA 95762
(916) 221-0855
support@7thdi.com

We love having you as a customer, and quite honestly, we wish we had more like you!

Simply refer any company and earn up to $100 when your referral becomes our client.