1991 – 2021
30
YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

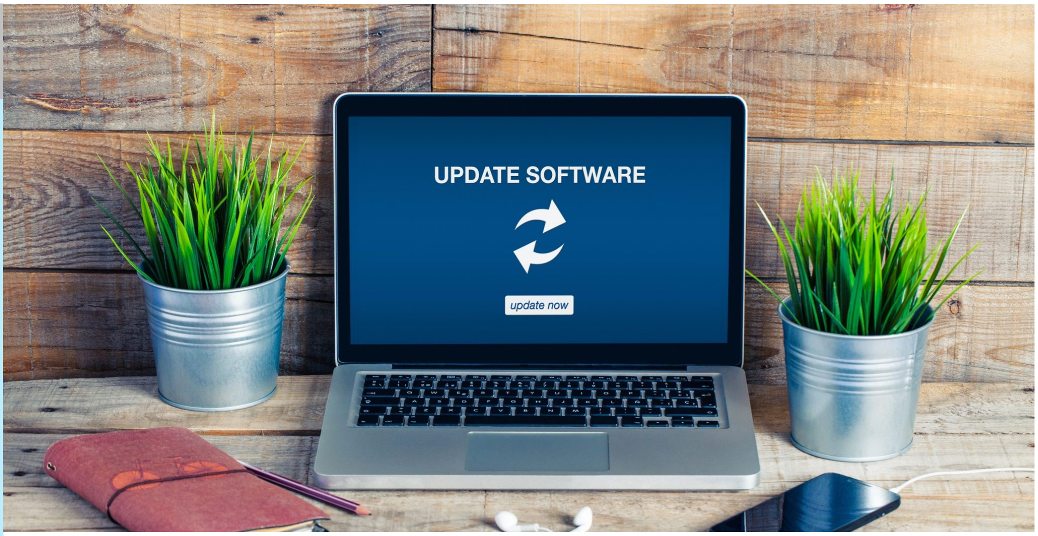
"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

October 2022

Kim Nielsen, CISSP
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



Do I Really Need To Update My Software ASAP?

When you use the Internet every day, whether for work or personal use, you get into a personal routine. Just like you get up in the morning, eat breakfast, brush your teeth and dress, every time you log into your computer you may follow a pattern too. You open your browser to the tabs you last used, where Cookies keep you automatically signed in (do you even know your password anymore?) so you can add to your online shopping cart. The saved carts make one-click checkout a breeze.

You like the way your accounts look and run. When your browser needs to install updates and relaunch, you could lose your work. If the whole system needs to update, it can be time-consuming too. At the end of all that, the layout that you carefully designed for your account may no longer exist in the new update.

In general, people can be very resistant to these better versions when they're announced, because change is frustrating and and time consuming. So why is it really necessary to ensure that you make these changes as soon as they become available?

Security

When a vendor to one of your applications or services announces that they've patched a vulnerability in a new update, it lets you know that you have a security risk within your system. Whenever you use that old software, you're at risk. The vulnerability will remain a potential entryway for hackers until you fix it – namely, by installing the update with the patch.

Continued on pg.2

Continued from pg.1

You're not the only one who just got that notification, though. By warning you, they also inform cybercriminals that there are weak spots that can be penetrated. Now, it's not a problem for people who update immediately – but what about all the users who hesitate and delay to make these crucial changes to their applications? They're chum in the water for threat actors.

Speed

Let's look at Apple for a moment: Their customers have long spread rumor that the phone slows down, stops taking messages and generally has issues until you update to the new IOS. By mistake or design, this prompts users to download the newest versions ASAP so as to keep getting optimal functionality from their most-used device. At some point, older iPhones stop supporting IOS updates completely.

It's not just Apple. Old software can cause new platforms and systems to lag, simply because they're incompatible. Newer updates will always be more efficient, because that's the nature of technology: It's constantly evolving always pushing forward.

Synergy

Think about all the different software, applications and systems that need to come together to provide you a smooth online experience, from the time you start up your computer at the beginning of a workday to when you shut down for the evening. When designing upgrades to all of these things, developers will use the latest and greatest resources available so as to create the best (and safest) result possible.

When all these systems interconnect, however, they need to operate compatibly with each other. Imagine it's the summer of 2010 trying to run any given video without the latest version of Adobe Flash Player: Your browser can be the most advanced out there, but everything needs to be upgraded in order to run as a functional ecosystem.

Conclusion

If you've had a habit of letting updates lie in the past, there's good news: It's never too late to get serious about cybersecurity. It's easy, too. The superior cybersecurity teams (and best-prepared systems) automatically update as soon as one becomes available and can usually perform them during the company's off-hours so as not to disrupt the flow of business. Automation and vigilance are key in preventing breaches and stopping attacks before they happen.

Your competition is surely upgrading their technology and systems as often as possible, so why let them get a needless head start? Making necessary changes to your systems not only provides protection against coordinated cyber-threats looking to exploit the same vulnerability that the update came out to patch, but makes your systems run smoother and more effectively alongside other programs. For the most efficient systems and services, accept updates as soon as they become available. Change is what guides progress.

Free Cyber Risk Audit 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 risk audit to uncover any loopholes that may exist in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk 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 exposed to various threats in a number of areas.

Claim Your FREE Assessment Today At:

https://www.cti-mi.com/cyber-security-audit-1022/

Or Call Our Office At: 248-362-3800

Security Corner

Should I Delete My Old Apps And Programs?

If you combed through your computer or phone, you would probably find a lot of programs that you don't even remember downloading. It can be frustrating to take time out of your day to search out old programs and wait for them to uninstall, and besides, does it even actually matter? Yes! And here are a few reasons why.

Save Space
Your phone only has a so much space to installed which means there's limited space to go around before you have to pay for extra storage space. Meanwhile, computers require an external drive to get any more storage space, perhaps some Cloud server or a USB.

Save Memory
Now, you may be thinking: Isn't that the same thing as space? Although people often use it interchangeably, *space* is the data stored in the hard drive. RAM is kind of like how much you can handle on your plate. The more memory you have, the better your computer's performance and speed.

Keep your computer and phone running optimally and easily handling all of your files and data by uninstalling old apps that you don't have use for anymore. These programs and their stored data might be taking up more room than you even know!

For more information about email security, call us at 248-362-3800 or visit: https://bit.ly/3xSPcKY

Small Businesses Are Attacked By Hackers 3x More Than Larger Ones

Do you feel more secure from cyberattacks because you have a smaller business? Maybe you thought that you couldn't possibly have anything that a hacker could want? Didn't think they even knew about your small business.

Well, a new report out by cybersecurity firm Barracuda Networks debunks this myth. Their report analyzed millions of emails across thousands of organizations. It found that small companies have a lot to worry about when it comes to their IT security.

Barracuda Networks found something alarming. Employees at small companies **saw 350% more social engineering attacks** than those at larger ones. It defines a small company as less than 100 employees. This puts small businesses at a higher risk of falling victim to a cyberattack. We'll explore why below.

Why Are Smaller Companies Targeted More?

There are many reasons why hackers see small businesses as low-hanging fruit. And why they are becoming larger targets of hackers out to score a quick illicit buck.

Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritize your cash. You may know cybersecurity is important, but it may not be at the top of your list. So, at the end of the month, cash runs out, and it's inevitably moved to the "next month" wish list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. They may buy an antivirus program and think that's enough to cover them. But with the expansion of technology to the cloud, that's just one small layer. You need several more for adequate security.

Hackers know all this and see small businesses as an easier target. They can do much less work to get a payout than they would trying to hack into an enterprise corporation.

Every Business Has "Hack- Worthy" Resources

Every business, even a 1-person shop, has data that's worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cybercriminals can sell these on the Dark Web. From there, other criminals buy the information and use it for identity theft.

Here are some of the data that hackers will go after:

- Customer records
- Employee records
- Bank account information
- Emails and passwords
- Payment card details

Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach the network of a small business, they can often make a larger score. Many smaller companies provide services to larger companies including digital marketing, website management, accounting, and more.

Vendors are often digitally connected to their client's systems. This type of relationship can enable a multi-company breach. While hackers don't need that connection to hack you, it is a nice bonus.

Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest-growing cyberattacks of the last decade. So far in 2022, over 71% of surveyed organizations experienced ransomware attacks.

The percentage of victims that pay the ransom to attackers has also been increasing. Now, an average of 63% of companies will pay the attacker money in hopes of getting a key to decrypt the ransomware.

5 Mistakes Companies Are Making In The Digital Workplace

The pandemic has been a reality that companies around the world have shared. It required major changes in how they operate. No longer, did the status quo of having everyone work in the office make sense for everyone.

Many organizations had to quickly evolve to working through remote means. Overcoming the challenges and reaping the benefits takes time and effort. It also often takes the help of a trained IT professional, so you avoid costly mistakes such as:

- Poor Cloud File Organization
- Leaving Remote Workers Out of the Conversation
- Not Addressing Unauthorized Cloud App Use
- Not Realizing Remote Doesn't Always Mean From Home
- Using Communication

Internet Explorer Has Lost All Support (What You Need To Know)

After being the main entry to the internet in the late 1990s and early 2000s, Internet Explorer (IE) is gone.

As of June 15, 2022, Microsoft dropped the web browser from support.

To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organizations to still use legacy sites that may have worked best in IE. It uses the Trident MSHTML engine from IE11 to do this.

If you haven't yet addressed old copies of IE on your computers, your network could be at risk due to vulnerabilities in the browser no longer being fixed. Here's what you should do:

Migrate Browser Data to Microsoft Edge from IE

1. Uninstall the IE Browser
2. Ensure Employees Know How to Use IE Mode in Edge
3. Train Employees on Microsoft Edge Features

Save Recurring Email Text In Outlook's Quick Parts

Do you have certain emails you send to customers that have the same paragraphs of text in them? For example, it might be directions to your building or how to contact support.

Stop retyping the same info every time. Outlook has a feature called Quick Parts that saves and then inserts blocks of text into emails.

- Create a Quick Part by highlighting the text to save in an email.
- On the Insert Menu, click Quick Parts.
- Save Quick Part.

When ready to insert that text into another email, just use the same menu and click to insert the Quick Part.

"We're playing teleconference."