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

July 2022

Kim Nielsen
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!"

How Ransomware Is Changing

You know it, you fear it and you may even have experienced it: The particularly vicious kind of malware that we know as ransomware. All kinds of cyber threats pose a problem for any business with a vested interest in their internet presence or the smart devices they use to connect to the company networks. Anywhere/anything that connects online is a potential target for a hacker.

With digital capabilities come risk, like newfound opportunities for theft. Your company bank account is likely more padded than that of the average Joe or the hacker. That's what makes any size business a potential target for a ransomware attack.

What is Ransomware?
Ransomware encrypts files and information, then sends an alert to notify the user that their computer has been hacked. To get your files back, you'll need a special key that only the cyber criminals have. In exchange for thousands of dollars, these threat actors will release this private decryption key to get back those files which would otherwise be unrecoverable.
This is one major factor in why cybersecurity experts recommend regularly backing up all of your files. That way if something does happen, critical work isn't lost forever – and you don't have to pay the thief.

And yes, people really pay the fee. Sometimes it's simply to recover their files, but cybercriminals may also demand a second ransom to stop them from leaking the files online (this is called **double extortion**). Just because you have access to your files again doesn't mean that that information hasn't been compromised already, which is also why it's so important to update your security and change your passwords after a potential breach.

Ransomware in 2022
Ransomware is one of the most prevalent threats to organizations this year, and has been a rising issue for awhile. The use of the Dark Web and increasing digitization of society has given cybercriminals new opportunities for theft. For example, ransomware kits (also

Continued on pg.2

Continued from pg.1

known as ransomware-as-a-service) are just what they sound like: Code that can be bought and executed against a victim, some complex and worth thousands but others as cheap as $10.

Other facts about the dangers of ransomware that you should keep in mind:

- On average, ransomware payments amount to $570K
- Average payments experienced an over 80% increase in 2021
- Ransomware is fast; it executes, on average, in under half an hour
- Double extortion is when the threat actor demands payment for the return of your files AND to stop further distribution, and was responsible for nearly 1000% more data leakage in 2021
- Even payment is no guarantee – 35% who pay the ransom never recover their data regardless
- The US Treasury credits ransomware with $5.2B bitcoin transactions, which shows how entwined cryptocurrency is with the latest cyber threats

Given how difficult some of the more advanced ransomware can be to combat, taking proper precautions and keeping an updated security posture will preemptively strengthen the protection of the business.

On average, ransomware payments amount to $570K

Defending Against Ransomware

How can you reduce your risk of falling victim and paying huge sums of money to recover files and begin to recuperate from the attack?

- Regularly change your password into hard-to-guess alphanumerical combinations that you don't use for any other site
- Keep work files within your company's secure server
- Lock your workstation when you're away
- Restrict access to secure files by establishing different clearance levels throughout the organization
- Invest in business class firewalls and remote access solutions
- Automate processes to scan for abnormalities on the network
- Test for and patch vulnerabilities to prevent zero-day exploits
- Regularly back up data, and check that backup to ensure the files are actually recoverable

Ransomware has big consequences if it finds its way onto your system and you don't have a back up plan or up-to-date defenses on your side. Staying apprised of what tactics cybercriminals are using, the stakes at risk, and what you can do to stay safe will protect your company as technology advances and ransomware attacks evolve.

Conclusion

Ransomware seems set to stay on track as a growing threat to businesses just like yours. New versions continue to devastate software, compromise information, and steal and sell data. In 2021, a new company was affected by ransomware every eleven seconds, down from fourteen in 2019. Now is the time to stop that trend from continuing, by equipping ourselves with the knowledge needed to stay cyber-safe on a day to day basis.

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at

https://www.cti-mi.com/itbuyersguide722

Security Corner

Do I Really Need To Update Software ASAP?

When you use the Internet every day, 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.

People can be very resistant to these updated versions when they're announced, because change is frustrating and scary. So why is it really necessary to make these changes as soon as they become available to you?

Security
When the provider of 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 – by installing the update with the patch.

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. 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 always pushing forward.

For more information on updating software, call us at 248-362-3800 or visit: **https://bit.ly/3OcMSoi**

Which Form Of MFA Is The Most Secure? Which Is The Most Convenient?

Credential theft is now at an all time high and is responsible for more data breaches than any other type of attack.

With data and business processes now largely cloud-based, a user's password is the quickest and easiest way to conduct many different types of dangerous activities.

One of the best ways to protect your online accounts, data, and business operations is with multifactor authentication (MFA). It provides a significant barrier to cybercriminals even if they have a legitimate user credential to log in. This is because they most likely will not have access to the device that receives the MFA code required to complete the authentication process.

What Are the Three Main Methods of MFA?
When you implement multi-factor authentication at your business, it's important to compare the three main methods of MFA and not just assume all methods are the same.

There are key differences that make some more secure than others and some more convenient for the end-user.

Let's take a closer look at what these three methods are:

SMS-based -The form of MFA that people are most familiar with is SMS-based.

This one uses text messaging to authenticate the user. The user will typically enter their mobile number when setting up MFA. Then, whenever they log into their account, they will receive a text message with a time sensitive code that must be entered.

On-device Prompt in an App -Another type of multi-factor authentication will use a special app to push through the code.

The user still generates the MFA code at log in, but rather than receiving the code via SMS, it's received through the app. This is usually done via a push notification, and it can be used with a mobile app or desktop app in many cases.

Security Key- The third key method of MFA involves using a separate security key that you can insert into a PC or mobile device to authenticate the login.

The key itself is purchased at the time the MFA solution is set up and will be the thing that receives the authentication code and implements it automatically. The MFA security key is typically smaller than a traditional thumb drive and must be carried by the user to authenticate when they log into a system.

Now, let's look at the differences between these three methods.

Most Convenient Form of MFA?

The most convenient form of MFA, would be the SMS-based MFA.

Most people are already used to getting text messages on their phones so there is no new interface to learn and no app they have to install.

The SMS-based is actually the least secure because there is malware out there now that can clone a SIM card, which would allow a hacker to easily get those MFA text messages.

Most Secure Form of MFA?

If your company handles sensitive data in a cloud platform then it may be in your best interest to go for better security.

The most secure form of MFA is the security key.

The security key, being a separate device altogether, won't leave your accounts unprotected in the event of a mobile phone being lost or stolen. Both the SMS-based and app-based versions would leave your accounts most at risk in this type of scenario.

Top 6 Mobile Device Hacks You Want To Watch Out For

Smartphones and tablets are often the preferred device for communications, web searching, and accessing many types of apps. They're more portable and can be used from virtually anywhere.

You need to be on the lookout for the most prevalent mobile device threats that allow your data to be leaked or breached.

Here's a roundup of what those are:

- Mobile malware hidden in apps
- Public Wi-Fi & Man-in-the-Middle attacks
- Juice Jacking on public USB charging stations
- Non-updated devices
- Text-based phishing (smishing)

Should I Consider Switching To Microsoft Edge Browser?

Microsoft Edge recently surpassed Firefox in worldwide desktop browser market share and is now the #3 Desktop browser in the world behind Chrome and Safari.

Why has Edge become so popular? One reason is that it adopted the Chromium framework in 2020, the same one that Chrome uses.

Edge is the replacement for Internet Explorer, but it's taken a while for it to become mainstream. It seems that now is its time. With that, should you switch to Edge?

Here are a few features to help you decide.

- Make saved websites easier to find using Collections
- Coupons are served up for you as you shop online
- Get instant price comparisons
- See pricing history for best-price trends
- Great security features, like Defender SmartScreen
- Grab quick screenshots with Web Capture

Signs That Your Computer May Be Infected With Malware

Approximately 34% of businesses take a week or longer to regain access to their data and systems once hit with a malware attack.

Keep an eye out for these key warning signs of malware infection so you can jump into action and reduce your risk.

- Strange popups on your desktop
- New sluggish behavior
- Applications start crashing
- Your browser home page is redirected
- Sudden reboots
- You are missing hard drive space
- You run across corrupted files
- PC "processing sounds" when there shouldn't be