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

April 2024

Kim Nielsen, CISSP, CCSA
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!"

Behind The Average Ransomware Attack

Introduction

If you've been following this blog for a while, then you've probably heard about the dangers of ransomware a lot. Hopefully, you've even picked up a few tips about how to recognize, handle and report ransomware schemes. Just how bad can these attacks really get, though?

That's exactly what we're going to explore here.

Walk Through an Average Ransomware Attack

The way that cybercriminals first approach their victims varies. They may use phishing tricks, which remain one of the most popular methods because of how effective it is, or they could use brute force to break in and do whatever they want with your system and devices; there's no limit to the ways cybercriminals approach their targets.

Once the attacker has access to the victim's system, they will install ransomware software. This software can be disguised as a legitimate program, or it can be hidden in a file that you open, thinking it's trustworthy.

After the victim's files have been encrypted, the attacker will

Continued on pg.2

Continued from pg.1

demand a ransom payment in exchange for the decryption key. The ransom payment is typically demanded in cryptocurrency, such as Bitcoin, to make it more difficult to track the attacker when one of their victims inevitably reports the theft to authorities.

Remember, *most people never see their data again* even if they pay the ransom! That's why you're advised NEVER to pay for your files; backups should be tested regularly in order to restore your data in any situation.

Even if they do return your data, cybercriminals often demand **double extortion** to prevent them from publishing your private information all over the Internet. Of course, that's no guarantee it won't still wind up on the Dark Web!

Fighting Ransomware $7.2M and 560K records are impacted in an average ransomware attack. Don't let yours be one of them!

- Unplug affected machines to prevent the infection from spreading through the local network.
- NEVER pay the fee.
- Report ransomware to your IT team and all the appropriate authorities as designated by your company's incident response plan.

What would YOU do if you got hit with a ransomware attack? If you're even a little unsure or hesitant, then take the time today to ask your superiors so you're 100% ready to act when disaster strikes!

Conclusion

Nearly 500M ransomware attacks occurred in 2023. Statistics show that they're happening more often and demanding more money each time. The best defense is educating yourself on the latest ransomware threats and the consequences that lay in wait if you fall for bad actors' persistent tactics.

Ransomware isn't going away. If anything, it's getting more prevalent and harder to handle. Know what to do when the worst happens before it happens. Your private data will thank you!

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata424/
or call our office at (248) 362-3800

Security Corner

23andMe and Threat Actors Too!

Introduction
Are you familiar with the ancestry and biotechnology service, 23andMe? More than 14M people around the world use their website! In December 2023, 23andMe confirmed a data breach that affected 6.9 million users.

What Happened?
When a breach like this occurs, it's important to first find out *what data was accessed*. If you opted into the DNA Relatives feature, for example, then hackers could potentially access information about your ancestry and relatives. For some users, health data was also compromised.

If you use 23andMe, or ever have, then find out ASAP if you were affected! Check your email for any notifications from the service; they contacted affected users directly about this compromise. You can also log in to your account and see if there's any information about the breach.

If You've Been Affected
What should you do if your data has been exposed either in this particular data breach, or one just like it?

- Change your password: Use a strong, unique password
- Review your privacy settings: Limit the information you share
- Be cautious of suspicious emails or calls: Don't click on links or share personal information unless you're sure it's legitimate.

Remember, staying informed and taking proactive steps can help mitigate the risks associated with this data breach and any others that might involve your PII in the future.

For more information about the dangers of misinformation, call us at 248-362-3800 or visit: https://tinyurl.com/58hd6v8k

Be Careful When Scanning QR Codes

QR codes are everywhere these days. You can find them on restaurant menus, flyers, and posters. They're used both offline and online. QR codes are convenient and easy to use. You just scan them with your smartphone camera. You're then directed to a link, a coupon, a video, or some other online content.

With the rise in popularity of QR codes comes an unfortunate dark side. Cybercriminals are exploiting this technology for nefarious purposes. Scammers create fake QR codes. They can steal your personal information. They can also infect your device with malware or trick you into paying money.

It's crucial to exercise caution when scanning QR codes. This emerging scam highlights the potential dangers lurking behind those seemingly innocent squares.

The QR Code Resurgence
QR codes were originally designed for tracking parts in the automotive industry. They have experienced a renaissance in recent years as a result, they're used as a form of marketing today.

They offer the convenience of instant access to information. You simply scan a code. Unfortunately, cybercriminals are quick to adapt. A new phishing scam has emerged, exploiting the trust we place in QR codes.

How the Scam Works
The scammer prints out a fake QR code. They place it over a legitimate one. For example, they might stick it on a poster that advertises a product discount.

You come along and scan the fake QR code, thinking it's legitimate. The fake code may direct you to a phishing website. These sites may ask you to enter sensitive data such as your credit card details, or login credentials,.

Or scanning the QR code may prompt you to download a malicious app. One that contains malware that can do one or more of the following:

- Spy on your activity
- Access your copy/paste history
- Access your contacts
- Lock your device until you pay a ransom

The code could also direct you to a payment page. A page that charges you a fee for something supposedly free.

Here are some tactics to watch out for.

Malicious Codes Concealed
Cybercriminals tamper with legitimate QR codes. They often add a fake QR code sticker over a real one. They embed malicious content or redirect users to fraudulent websites.

Fake Promotions and Contests
Scammers often use QR codes to lure users into fake promotions or contests. When users scan the code, it may direct them to a counterfeit website.

Malware Distribution
Some malicious QR codes immediately start downloads of malware onto the user's device.

STAY VIGILANT: TIPS FOR SAFE QR CODE SCANNING

Verify the Source – Verify the legitimacy of the code and its source.

Inspect the URL Before Clicking – Before visiting a website prompted by a QR code, review the URL.

Be Wary of Websites Accessed via QR Code – Don't enter any personal information on a website that you accessed through a QR code. This includes things like your address, credit card details, login information, etc. Don't pay any money or make any donations through a QR code.

Eye Opening Insights From The 2023 Annual Cybersecurity Attitudes And Behaviors Report

Often, it's our own actions that leave us most at risk of a cyberattack or online scam. Risky behaviors include weak passwords and lax security policies and also thinking, *This won't happen to me.*

The National Cybersecurity Alliance and CybSafe published a report on cybersecurity attitudes and behaviors. The goal is to educate both people and businesses. The report reveals some eye-opening insights.

Here are some of the key findings from the report:

- We are online a lot: 93% of respondents are online daily.
- We store sensitive stuff online: 47% of respondents have ten or more sensitive online accounts.
- Online security makes people frustrated: 39% of people feel frustrated when trying to stay safe online.
- People need more access to training: Just 26% of the survey respondents had access to cybersecurity training.

Tactics To Reduce Cloud Waste At Your Business

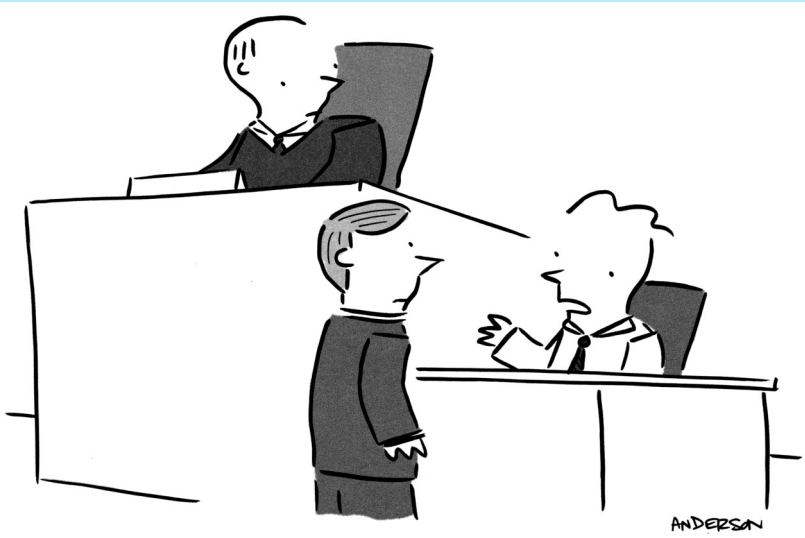
Cloud computing has completely revolutionized the way businesses operate. It offers scalability, flexibility, and cost efficiency.

But cloud services also come with a downside: cloud waste. Cloud waste is the unnecessary spending of money on cloud services. About 32% of cloud spending is wasted and this leads to budget concerns as spending skyrockets.

But that figure also holds opportunity. It means that you can reduce nearly a third of cloud spending by optimizing how you use cloud tools.

Here are some tactics to reduce cloud waste and save money:

- *Conduct a Comprehensive Cloud Audit* – Before implementing any cost-cutting strategies, conduct an audit.
- *Put in Place Right-Sizing Strategies* – Analyze your workload requirements and resize instances accordingly.
- *Use Reserved Instances and Savings Plans* – Cloud providers offer cost-saving options like Reserved Instances (RIs) and Savings Plans.
- *Track and Optimize Storage* – Regularly review and delete unnecessary data to free up storage space.
- *Schedule Your Cloud Resources* Schedule your cloud resources to run only when you need to use them.
- *Delete Unused or Orphaned Cloud Resources* – Regularly audit your cloud environment to delete any unused or orphaned resources your business is not using.



"I wouldn't call it identity theft, I just self-identify as other people."