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

TECHNOLOGY TIMES

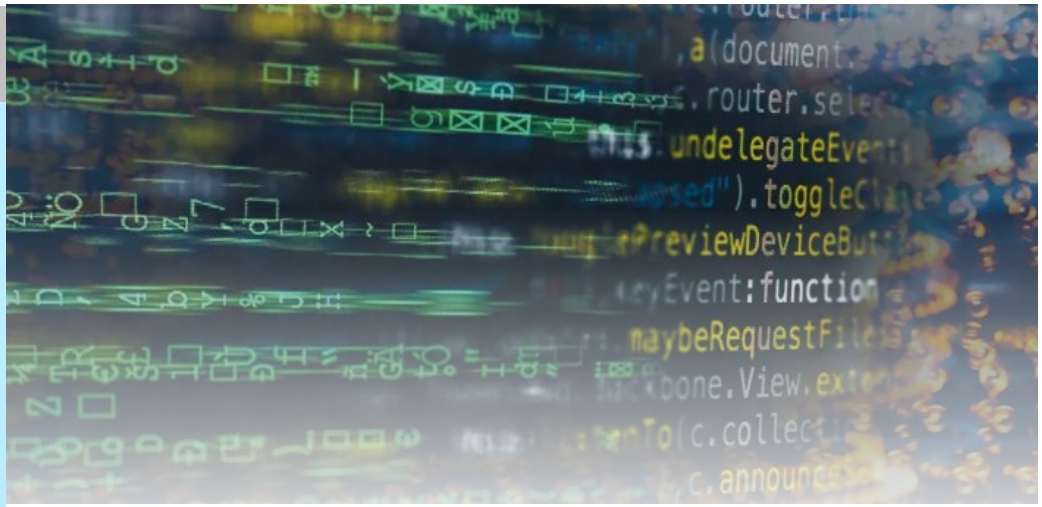
"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

January 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!"



How Encryption Really Works: A Beginner's Guide

Introduction

Encryption is one of the most commonly misunderstood subjects when it comes to protecting sensitive data. Even those with a basic understanding of encryption often misidentify certain components, use the wrong algorithm, and fail to understand how they are used in practice. These myths and misunderstandings are not only frustrating—they can also put your personal security at risk.

This article offers a comprehensive introduction to encryption designed for beginners. If you're new to encryption, you will learn everything from common terms and definitions to how encryption works in practice.

What Is Encryption?

Encryption is a process of encoding data or information in such a way that only authorized parties can access it. It is used to protect data from unauthorized access, modification, and theft. Encryption is an important tool for keeping sensitive information secure and ensuring the privacy of users. It can also be used to verify the integrity of data by providing an authentication mechanism and is thus widely used in industries such as banking, healthcare, and government agencies.

Encryption is an important tool for protecting data and ensuring privacy. It helps to ensure that information sent over the internet remains confidential and secure, preventing unauthorized access

Continued on pg.2

Continued from pg.1

and tampering; but it also helps protect against malicious actors who may try to gain access to sensitive data or networks. In this way, encryption serves as a powerful defense against cybercrime, fraud, and other online threats. By encrypting data before it is transmitted or stored, organizations can reduce the risk of a breach or attack on their systems. This will also help ensure compliance with regulations such as the General Data Protection Regulation (GDPR) and various U.S. state data privacy laws.

You should encrypt all sensitive data, no matter where it's stored or whether you think anyone else might access it (or try to). This is simply a best practice and will also ensure you pass your compliance audit in the event of a data breach.

Common Threats to Encrypted Data

Unfortunately, cyber-threats to encryption are on the rise. Everyone in the organization must remain vigilant and understand how bad actors may target your private communications, so as to take steps to protect your data from these threats.

Hackers are constantly looking for ways to break encryption codes and gain access to sensitive data. Guard your encryption closely, and with as much caution as you use on your private credentials like your passwords. You should also assess your data encryption software performance regularly to ensure it continues working efficiently.

Additionally, some AI tools exist for the main purpose of encryption protection, and they can help organizations stay ahead of the curve when it comes to protecting their data.

In addition, governments around the world are increasingly demanding access to encrypted data, which can put user privacy at risk. You can use Global Privacy Control (GPC) features on certain systems, which automatically tell those pesky pop-ups that you don't want to sell your cookies on every website you visit. This will minimize how much of your data is made public so you only give up information that you ABSOLUTELY have to.

Conclusion

Encryption is a powerful tool for protecting data and communications. It is used by individuals and organizations to protect sensitive information from unauthorized access and malicious actors. However, encryption technology has its limitations and can be vulnerable to attack if not properly implemented or managed.

Keep your private communications confidential! Data encryption is not foolproof, but it's a huge step closer to data privacy than going without.

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-124/
Or Call Our Office At: 248-362-3800

Security Corner

Is Google Wiretapping Your Calls?

In October 2023, a class-action lawsuit was filed against Google alleging that the company's "human-like" customer service product powered by generative artificial intelligence (AI) wiretapped customers without their knowledge or consent.

The product, known as Google Cloud Contact Center AI (GCCCAI), is used to provide customer service support.

Wiretapping received its name because, historically, the monitoring connection was an actual electrical tap on an analog telephone or telegraph line. These days, it's much easier.

It can now be done without having to physically connect to the device the perpetrator wants to spy on. Law enforcement and government agencies can electronically investigate and prevent crimes…but people can illegally wiretap, too. Businesses might do it to spy on competitors, while individuals might use it to spy on and blackmail others in their lives.

This lawsuit against Google raises important questions about the use of AI in customer service, and the privacy implications therein. In addition to the lawsuit against Google, there have also been lawsuits filed against other companies that use AI to listen to and transcribe customer service calls, such as Verizon and H&R Block.

We already know that people all over the world care deeply about data privacy and support legislation that protects them online. Whether that means from cybercriminals, or from the companies that we connect with over the internet or phone.

For more information about wiretapping, call us at 248-362-3800 or visit: https://tinyurl.com/37knk8jp

How Can Your Business Be Impacted By The New SEC Cybersecurity Requirements?

Cybersecurity has become paramount for businesses across the globe. As technology advances, so do the threats. Recognizing this, the U.S. Securities and Exchange Commission (SEC) has introduced new rules. They revolve around cybersecurity. These new requirements are set to significantly impact businesses.

Understanding the New SEC Requirements: The SEC's new cybersecurity rules emphasize the importance of proactive cybersecurity measures. These are for businesses operating in the digital landscape. One of the central requirements is the timely reporting of cybersecurity incidents. The other is the disclosure of comprehensive cybersecurity programs.

The rules impact U.S. registered companies. As well as foreign private issuers registered with the SEC.

Reporting of Cybersecurity Incidents
The first rule is the disclosure of cybersecurity incidents deemed to be "material." Companies disclose these on a new item 1.05 of Form 8-K. Companies have a time limit for disclosure. This is within four days of the determination that an incident is material. The company should disclose the nature, scope, and timing of the impact. It also must include the material impact of the breach. One exception to the rule is where disclosure poses a national safety or security risk.

Disclosure of Cybersecurity Protocols
This rule requires extra information that companies must report. They report this on their annual Form 10-K filing. The extra information companies now must disclose includes:

- Their processes for assessing, identifying, and managing material risks from cybersecurity threats.
- Risks from cyber threats that have or are likely to materially affect the company.
- The board of directors' oversight of cybersecurity risks.
- Management's role and expertise in assessing and managing cybersecurity threats.

Potential Impact On Your Business:
Here are some of the potential areas of impact on businesses from these new SEC rules.

1. **Increased Compliance Burden –** Businesses will now face an increased compliance burden as they work to align their cybersecurity policies with the new SEC requirements.
2. **Focus on Incident Response –** The new regulations underscore the importance of incident response plans. Businesses will need to invest in robust protocols. These are protocols to detect, respond to, and recover from cybersecurity incidents promptly. This includes having clear procedures for notifying regulatory authorities, customers, and stakeholders.
3. **Heightened Emphasis on Vendor Management –** Companies often rely on third party vendors for various services. The SEC's new rules emphasize the need for businesses to assess vendor practices. Meaning, how vendors handle cybersecurity. This shift in focus necessitates a comprehensive review.
4. **Impact on Investor Confidence –** Cybersecurity breaches can erode investor confidence and damage a company's reputation. With the SEC's spotlight on cybersecurity, investors are likely to take note. This includes scrutinizing businesses' security measures more closely. Companies with robust cybersecurity programs may instill greater confidence among investors. cybersecurity sector.

14 Helpful Tips For New Year Digital Decluttering

These days, it's easy to feel overwhelmed at the sight of an endless inbox or app library.

As the new year begins, it's the perfect time for a digital declutter. A clean and organized digital environment can help you improve your productivity. It also reduces stress. Here are some practical tips to help you declutter your digital space:

- Start with a digital inventory
- Focus on your most-used digital spaces
- Organize your files and folders
- Clean up your email inbox
- Clean up your social media
- Review your subscriptions
- Review and delete unused apps
- Clear your desktop and downloads folder
- Secure your digital identity
- Evaluate your digital habits
- Create digital detox days
- Streamline notifications
- Invest in digital tools
- Practice regular maintenance

11 Ways To Responsibly Get Rid Of E-Waste At Your Home Or Office

In our tech-driven world, electronic devices have become indispensable. But with constant upgrades, what happens to the old gadgets? They tend to pile up and eat up storage space. But you can't just throw them in the trash.

E-waste poses a significant environmental threat if not disposed of responsibly. E-waste can contain hazardous materials. Such as lead, mercury, cadmium, and brominated flame retardants. These can harm the environment and negatively impact human health.

Here are some tips to responsibly get rid of e-waste at your home or office:

- Understand what makes up e-waste
- Reduce your e-waste
- Explore retailer recycling programs
- Use e-waste recycling centers
- Consider donating or selling functioning devices
- Dispose of batteries separately
- Try manufacturer take-back programs
- Opt for certified e-waste recyclers
- Educate your office or household
- Repurpose or upcycle
- Encourage manufacturer responsibility