TECHNOLOGY TIMES

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

What's Inside

June 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!"

The Truth About Third-Party Data Collection

Introduction

Ever feel like the internet is following you around? You browse for vintage cocktail shakers, and suddenly every ad screams "shaken, not stirred"? You search for a new stroller on your phone and suddenly every Instagram ad is about pacifiers and cribs?

That is both the magic and mayhem of those considered to be third-party data collectors.

Who Is Behind Third-Party Data Collection?

It doesn't matter what search engine you use…Whether it's Google, Safari or Firefox, these platforms are designed not only to help you find relevant information based on everything from your demographic to your location; but they also help the rest of the Internet cater to your particular needs and interests.

They gather crumbs of your digital life – websites you visit, links that you click on, apps downloaded, and even what you buy online. This intel gets thrown into a big database, forming a profile all about *you*. Aside from the potential for hackers to exploit one of these massive databases directly, there's also the much more likely chance that all that information will be sold to third-party collectors that want to use it for advertisements and their own financial gain.

Sound like a phishing scheme? It's actually completely legal.

Now, maybe you already try to stay one step ahead by toggling on different settings to limit data collection to certain information or websites. What you may not

Continued on pg.2

Continued from pg.1

expect, however, is that fine print, which declares that the search engine (or other website) is allowed to collect and sell your *cookies* to outside businesses. These are the third-party companies accessing and leveraging your Internet history and personal data, usually to generate revenue.

So, the next time you see laser-targeted ads, you can thank these shadowy data collectors (and at the same time, update all of your privacy settings).

Protecting Your Search Data

What exactly are they gathering, anyway?

Collected information may include:

- Demographics (age, location, income)
- Browsing habits (websites you visit, things you click on)
- Purchase history (what you buy online)
- Interests (hobbies, favorite brands)

The good news is that more and more data privacy regulations, like GDPR and CCPA, give users more control over their information. It's a fight, but we're slowly moving in the right direction.

Remember, technology always evolves faster than the legislation surrounding it!

You can take steps toward greater data privacy on your own, too.

- **Manage your own online privacy.** Those cookies and trackers websites use to follow you? You can adjust your browser settings to block them and exercise more control over who can see, sell and exploit your online data.
- **Review policies before signing off.** When you're flying past those terms and conditions, don't just click "accept" blindly. Read those privacy policies to understand how your data is being collected and used. Knowledge is power
- **Install more privacy tools:** There are tools out there that block tracking and help you manage your online privacy. Be a tech-savvy data defender by getting to know the weapons that could be in your arsenal.

Conclusion

By understanding third-party data collectors and their tactics, you can become a data defense champion and protect your privacy in this wide and wild online world. Stay safe, stay informed, and keep enjoying all your favorite websites without fear of being digitally stalked by hungry third-party data collectors.

Security Corner

Why You Shouldn't Reuse Passwords

Reduce, reuse, recycle. It's usually good advice; unfortunately, when it comes to your login credentials, it's dangerous!

Why is it dangerous to reuse a password?

If one account gets compromised in a data breach, hackers can try that same password on all your other accounts. This can give them access to your email, bank accounts, social media and more depending on where you reused the same password.

What's more, cybercriminals often use stolen login information from breaches to try logging into other accounts in an automated process called ***credential stuffing.*** Reusing passwords makes you more susceptible to this kind of attack.

Statistics show that over 80% of data breaches happen because of weak, stolen or compromised passwords.

By using unique passwords for every account, you make it much harder for hackers to gain access to your personal information, finances, and other sensitive data. That means at least ***12 characters, with a combination of numbers, letters and symbols*** to prevent unwanted access to your accounts!

A breach of your passwords and accounts can lead to hackers phishing your friends lists from your real account, device and network compromise, and even identity theft! By simply changing your passwords so that they are varied and complex, your risk of a data breach plummets.

For more information about the dangers of misinformation, call us at 248-362-3800 or visit: https://tinyurl.com/ytzkse34

Don't Skip It! Why You Shouldn't Skip Vulnerability Assessments

Cyber threats are a perpetual reality for business owners. Hackers are constantly innovating. They devise new ways to exploit vulnerabilities in computer systems and networks.

For businesses of all sizes, a proactive approach to cybersecurity is essential. One of the most crucial elements of this approach is regular vulnerability assessments. A vulnerability assessment is a systematic process. It identifies and prioritizes weaknesses in your IT infrastructure that attackers can exploit.

Some businesses may be tempted to forego vulnerability assessments. They might think it's too costly or inconvenient. Small business leaders may also feel it's just for the "big companies." But vulnerability assessments are for everyone. No matter the company size. The risks associated with skipping them can be costly.

Why Vulnerability Assessments Matter
The internet has become a minefield for businesses. Cybercriminals are constantly on the lookout for vulnerabilities to exploit. Once they do, they typically aim for one or more of the following:

- Gain unauthorized access to sensitive data
- Deploy ransomware attacks
- Disrupt critical operations

Here are just some of the reason vulnerability assessments are crucial in this ever-evolving threat landscape:

- **Unseen Weaknesses:** Many vulnerabilities remain hidden within complex IT environments.
- **Compliance Requirements:** Many industries have regulations mandating regular vulnerability assessments. (and hefty fines if you are found to be non-compliant.
- **Proactive Approach vs. Reactive Response:** Identifying vulnerabilities proactively allows for timely remediation. This significantly reduces the risk of a costly security breach. A reactive approach is where you only address security issues after an attack.– and by then, it's too late.

The High Cost of Skipping Vulnerability Assessments

- **Data Breaches** – Unidentified vulnerabilities leave your systems exposed to breaches.
- **Financial Losses** – Data breaches can lead to hefty fines and legal repercussions as well as the cost of data recovery and remediation.
- **Reputational Damage** – A security breach can severely damage your company's reputation. It can erode customer trust and potentially impact future business prospects.

The Benefits of Regular Vulnerability Assessments

- **Improved Security Posture:** Vulnerability assessments identify and address vulnerabilities.
- **Enhanced Compliance:** Regular assessments help you stay compliant with relevant industry regulations.
- **Peace of Mind:** Knowing your network is secure from vulnerabilities gives you peace of mind.
- **Reduced Risk of Costly Breaches:** Proactive vulnerability management helps prevent costly data breaches.

Investing in Security is Investing in Your Future
Vulnerability assessments are not a one-time fix. Your business should conduct them regularly to maintain a robust cybersecurity posture.

By proactively identifying and addressing vulnerabilities, you can:

- Significantly reduce your risk of cyberattacks
- Protect sensitive data
- Ensure business continuity

Remember, cybersecurity is an ongoing process.

Guide To Improving Your Company's Data Management

Data is the lifeblood of modern businesses. It fuels insights, drives decision-making, and ultimately shapes your company's success. But in today's information age, data can quickly become overwhelming if its not properly managed.

Here are some strategies for effective data management:

- **Conduct a data inventory** – Identify all the data your company collects, stores, and uses. Understand the purpose of each data set and how the organization is using it.
- **Invest in data management tools** – Technology can be your ally in data management. Explore data management solutions.
- **Develop data policies and procedures** – Document your data management policies and procedures.
- **Foster a data-driven culture-** Encourage a data-driven culture within your organization. Emphasize the importance of data quality and responsible data usage.
- **Embrace continuous improvement** – Data management is an ongoing process. Regularly review your data management practices.

STUFF THAT HAPPENED YESTERDAY THAT YOU PROBABLY ALREADY HEARD ABOUT
TRASH
ANDERSON

Leverage Microsoft 365 Copilot For Your Business

Microsoft has expanded the availability of one of its most dynamic tools to SMBs. A tool that can be a real game-changer for growth.

Copilot for Microsoft 365 is a powerful new addition to the M365 suite. It was first offered to enterprise customers only. But Copilot is now open to businesses of all sizes as long as they have Microsoft 365 Business Standard or Business Premium licenses.

How Copilot Streamlines Workflows

- ***Effortless Content Creation*** – Copilot can suggest text responses and complete sentences. It can even draft entire emails and presentations based on your initial input.

- ***Enhanced Productivity*** – Copilot automates repetitive tasks and streamlines workflows by offering intelligent suggestions.

- ***Improved Communication and Collaboration*** – Clear communication is vital for any successful business.

- ***Reduced Learning Curve for New Technologies*** – Copilot provides context-aware guidance and suggestions. All while you work with your familiar Microsoft 365 applications. This can significantly reduce the learning curve for new staff.