FREE

Tech Source News

FREE

First Edition

A Flickertronics Technical News Publication

www.techsourcenews.com

Essential Tips For Asthma Sufferers

by Flicker, CEO, Flickertronics

Living with Asthma can be very challenging at times, but with the right strategies and a few lifestyle adjustments, many individuals can significantly reduce the impact of this chronic respiratory condition.

Here are some essential tips for people with moderate to severe asthma:

1. Always follow your doctor's prescribed treatment plan: Taking your medications as prescribed by your health care provider, including long-term control medications and quick-relief inhalers, can help maintain good health, minimize symptoms and reduce the need for emergency care.

2: Identify and Avoid Triggers: Beware of common triggers such as allergens, smoke, exercise or certain weather conditions.

Continued on Page 6

Screen Impact on Infants and Toddlers:

Long-Term Consequences

by Flicker, CEO, Flickertronics

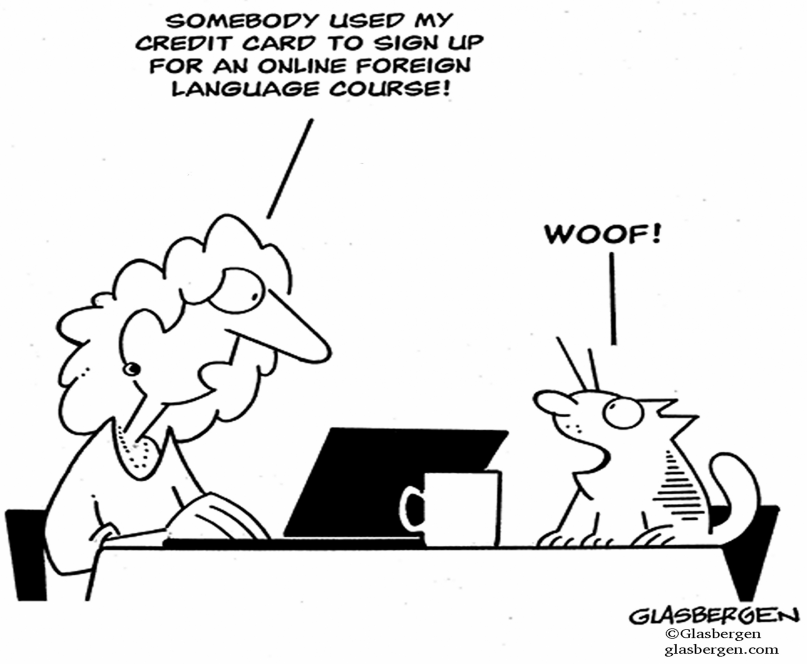
The extensive use of cell phone and tablet screen use among infants and toddlers has raised concerns about long-term effects on their brain development and ***cognitive skills***.

Cognitive Skills *are the mental abilities involving problem-solving, perception, learning, and memory.*

Research suggests that excessive screen time during these crucial years can lead to disruptions in brain development, attention span, social interactions with others, and affect language skills.

Prolonged exposure to screens may impede the formations of critical neural connections necessary for optimal cognitive growth.

Continued on Page 5



Optimize Your PC's Performance Settings

by Flicker, CEO, Flickertronics

Windows 10 and Windows 11 operating systems have "Power Saving" features enabled that reduce the performance and power consumption of your laptop or desktop PC. This also includes Windows 7.

I have some performance and optimizing steps to assist you with those settings and improve your PC's performance.

Open Control Panel

Press the Windows Key + R and type control panel in the "***Run***" dialog box then press enter to open control panel.

Open Power Options

If the control panel window is in the "***Category***" view click "***System and Security***". In the window that opens click "***Power Options***".

If the control panel is in the "***Large Icon***" or "***Small Icon***" view click "***Power Options***". The "***Power Options***" window appears.

Then the "***Select a Power Plan***" window appears. There are usually several power plans in this windows such as "***Balanced***" and "***Power Saver***" among others.

Next to the currently selected power plan click "***Change Plan Settings***".

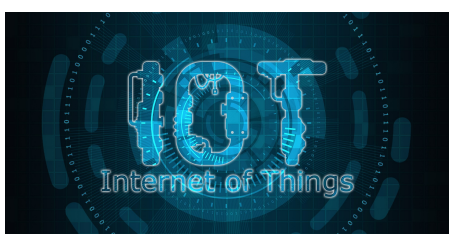
Continued on Page 2

The Internet of Things (IoT)

by Flicker, CEO, Flickertronics

The Internet of Things (IoT) is the network of interconnected physical devices that collect and exchange data over the Internet.

These devices are equipped with sensors, software, and Internet connectivity, allowing them to communicate and interact with each other.



In simple terms, (IoT) involves connecting everyday objects to the Internet, enabling them to communicate and interact with one another.

This concept has revolutionized our lives and work by creating a vast network of interconnected devices, ranging from smart thermostats, and security cameras to industrial machinery and even smart cities.

IoT devices collect and analyze data from various sources, automating processes, providing valuable insights, and improving convenience and efficiency in various areas.

The fundamental idea behind **IoT** is to enhance device connectivity

Continued on Page 8

The Brain-Computer AI Semantic Decoder

by Flicker, CEO, Flickertronics

One of the latest breakthroughs is the amazing development of a new **B**rain-**C**omputer **I**nterface system (**BCI**) called a ***Semantic Decoder***, which has the ability to translate a person's brain activity while listening to or imagining telling a story into a continuous stream of words and phrases that can be outputted as text.

This technology has the potential to revolutionize the way we communicate and interact with computers and operate machines, revolutionizing the field of neuroscience.

Continued on Page 4

The Risks of Using Free VPNs

by Flicker, CEO, Flickertronics

Virtual Private Networks (***VPNs***) have gained significant popularity as tools to enhance online privacy and security.

While *VPNs* can offer several benefits, it is crucial to exercise caution, especially when using ***FREE VPN*** services.

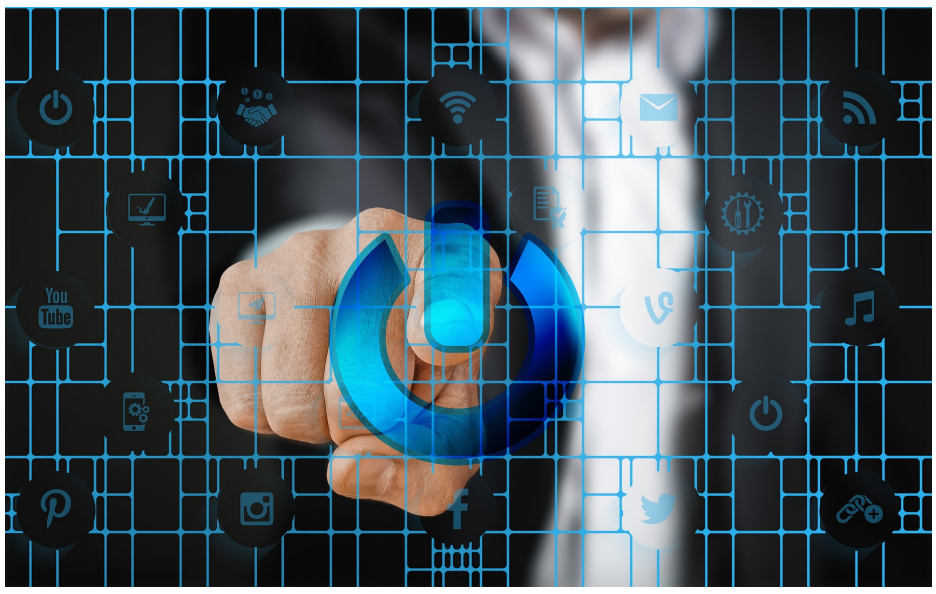
Although tempting, Using a ***FREE VPN*** can expose users to a range of potential risks and as well as dangers that may undermine the very purpose of using a ***VPN***.

Most *FREE VPN* providers are actually operating on a business model that involves collecting and selling user data to third parties.

Most *FREE VPN* Providers use insidious tactics to gather data, which they can then sell to data brokers, and may be operated by malicious operators who gather login credentials and other data.

Continued on Page 3

Optimize Your PC's Performance Settings



Continued from Page 1 *by Flicker, CEO, Flickertronics*

Edit Power Plan Settings

The "*Change Settings for the Plan*" window appears. Here you can choose the preferred length of time to turn off the display or put your computer to sleep.

Click on the "*Change Advanced Power Settings*" link to customize advanced settings for your current power plan.

The Power Options will pop up

Click the + sign next to "***Turn Off Hard Disk After***" to expand the menu and change it to whatever length of time you desire.

Click the + sign next to "***Wireless Adapter Settings***" to expand the menu and change thepower saving mode to "***Maximum Performance***".

Click the + sign next to "***Sleep Settings***". These settings control the different power saving modes such as "***Sleep***" or "***Hibernate***".

If you do not want the computer to go into sleep or hibernate mode you can type the word "***Never***" in the time slot.

This is one of the few times when you can type text in a numbers-only field.

Click the + sign next to "***USB Settings***" to expand the menu, then click the + sign next to "***USB Selective Suspend Setting***" and change it to "***Disabled***".

Click the + sign next to "***Graphics Power Plan***" to expand the menu and change the plan to "***Maximum Performance***".

The "*Power Button and Lid*" menu controls what happens when you close the lid on your laptop and has no effect on desktop PC's.

Click the + sign that is next to "***Processor Power Management***" to expand the menu, then click on the + sign next to "***Minimum Processor State***" to expand the menu and change the value from 5% to 100%.

These tips will ensure that your computer is able to run without the operating system reducing, or throttling and limiting, the speed and performance of your PC to save a few pennies a day on your desktop or workstation PC.

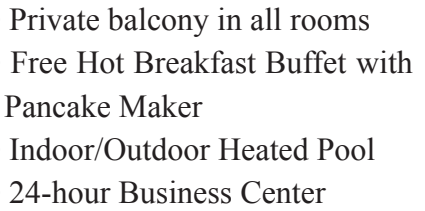
If you have a laptop PC, you can optimize these settings depending on whether you want maximum performance or battery life.

The Stingray Method: Unveiling the Controversial Use of Fake Cell Towers for Surveillance

by Flicker, CEO, Flickertronics

Cell-Site Simulators, or **IMSI** catchers are portable ***Cell-site simulators*** that trick nearby cell phones into connecting to them, instead of a legitimate cell tower.

Devices such as the ***Harris Corporations Stingray II*** and ***Shenzhen Action Technologies CO., LTD's*** model "***In Vehicle IMSI Catcher ATIP -234-02"*** are two examples.



These devices are expensive !
The ***Harris Kingfish*** Package sells for $*157,300* and another ***Harris Stingray package*** for $*148,000.*

The ***Stingray*** series has been upgraded to a newer device called the ***Crossbow***, no info available.

As well as being a product model, *Stingray* is the generic name for an electronic surveillance tool that simulates a legitimate cell-tower.

The *Stingray*, and other devices like it, "***cell-Site***" simulators or "***IMSI catchers***", are cell phone surveillance devices that simulate a cell phone tower in order to trick, or force, mobile phones and devices to connect to it.

*International Mobile Subscriber Identity (**IMSI**) is a unique number issued to every phone that cell providers use to identify and validate devices and allow them to connect to the cellular network.*

These cell tower simulators are used by law enforcement agencies, criminals, other countries as well as in the area of international espionage by rouge agents.

Continued on Page 4

LMIT Managed IT Services

LMIT, is a ***SentinelOne*** and ***SonicWall*** Global Partner.

With a vast portfolio LMIT provides IT and network infrastructure to corporations in multiple different fields. Services including network printing and scanning, Wi-FI connectivity, Server & Workstation installation, Firewall installation and full-time managed services.

LMIT currently manages the IT and network infrastructure for a car dealership with 5 locations that has over 410 computers, multiple network printers and scanners and Wi-FI connectivity.

LMIT follows **HIPAA**, **PCI** and **FTC** guidelines along with all other standards that represent the best practice standards.

LMIT provides IT for a number of doctors offices including hospital staff physicians and several other industries as well, bringing to you the experience gained managing thousands of devices in real time.

LMIT takes a personal approach to each client's needs, working with them to understand their unique challenges to develop customized solutions.

LMIT's Mission is to provide top-notch, enterprise class services to small to medium sized businesses, striving to make technology work for their clients.

LMIT Managed IT Services
(904)579-7905
info@lmitusa.com

Understanding Cell Phone VPNs

What They Protect and What They Don't Protect

by Flicker, CEO, Flickertronics

In today's digital era, privacy and security are serious concerns for smartphone users. **V**irtual **P**rivate **N**etworks (***VPNs***) have become popular tools to safeguard our online activities, encrypting data and shielding us from prying eyes.

When you connect to a *VPN* server, your device establishes an encrypted tunnel with the server. This encryption ensures that all data transmitted between your device and the ***VPN Server*** remains secure and private.

Once your device is connected to the ***VPN*** server, it acts as an intermediary between your device and the ***Internet***. All the ***Internet traffic*** between your device and the ***Internet*** passes through the ***VPN Server*** to the ***Internet Backbone***.

The *VPN* server assigns you a new *IP address* based on the city and country the ***VPN*** server you are connected to is hosted in, masking your true *Internet IP address*, as well as your true physical location from websites and online services you visit.

It is very important to realize it's limitations. The ***VPN*** only protects your data until it reaches the ***VPN*** server. Once the data leaves the ***VPN*** server and connects to the ***Internet Backbone***, it is no longer encrypted or protected by the ***VPN***.

Additionally, if you download files or click on links that contain malware or malicious content, a ***VPN*** cannot provide you protection, prevent you from falling victim to Phishing scams or from downloading malicious files.

While VPNs offer significant protection, it's very important to understand what they can and cannot safeguard on your cell phone or wireless devices.

What *Cell Phone VPNs* Protect:

1. Internet Traffic Encryption: One of the primary functions of a ***VPN*** is to encrypt your *Internet traffic*. When you connect to a ***VPN*** server, all data exchanged between your device and the ***VPN*** server is encrypted.

2. IP Address Masking: A ***VPN*** masks your real IP address with the *IP address* of the ***VPN*** server you connect to. This ensures your *real IP address* and location remain hidden to Internet-connected traffic.

3. Public Wi-FI Security: When you connect to a public Wi-Fi network, such as those in cafes, hotels, or airports you expose your device to potential risks. Without a ***VPN*** hackers can intercept your data or set up fake Wi-Fi Hot Spots to gain access to your sensitive information.

The hacker cannot access your data locally because you have an encrypted "*Tunnel*" to the ***VPN Server*** that connects you to the ***Internet Backbone*** in another city or country.

Continued on Page 6

The Risks of Using Free VPNs

Continued from page 1

by Flicker, CEO, Flickertronics

The vast amounts of user data collected includes the device's browsing history, IP addresses, device information, and even personal details.

This data is then stored and then it is processed, often with minimal or no regard for user content or privacy protection.

Once these *FREE VPN* providers have accumulated a substantial amount of user data they can sell this information to third parties.

Browsing History and Activity: *FREE VPN* providers track their user's browsing history and activity such as websites visited, pages viewed and the length of time spent on each one, and search queries entered. This information can then be analyzed and sold to third-parties.

These providers can also collect Personally Identifiable Information (**PII**). This can include names, email addresses and even payment details.

***FREE VPN* providers** often track and collect location data about their user's access and use of servers in different cities and countries.

***FREE VPN* providers** frequently employ tracking cookies that are stored on user's devices and track their online behaviour across websites.

***PAID VPN* providers** often have clear and transparent privacy policies, undergo regular audits, and implement security measures to protect user data. While they involve a cost, the peace of mind and enhanced privacy they offer is worth the investment.

It is vital for users to exercise caution and choose reputable, ***PAID VPN*** services that prioritize data protection and user privacy.

To summarize, ***PAID VPNs*** provide better security and often have faster, more secure and reliable connections.

Securing Your Cell Phone Against Hacking

by Flicker, CEO, Flickertronics

Safeguarding your cell phone's security demands well thought-out measures. The following actions will assist in your phone's protection.

1. Log Out from Email Accounts: The foremost measure is logging out from email accounts. This prevents unauthorized access even if the device is compromised physically or remotely.

2. App Authentication: Implement stringent security for apps. ***Always log out and avoid saving passwords for social media, banking, messaging, cloud storage and other apps.***

3. Strong Unlock Methods: Employ robust PINs, passwords with capitals and symbols, or Biometric authentication like fingerprint or facial recognition to unlock your device.

4. Two-Factor Authentication (2FA): Opt for 2FA to heighten security. It requires a unique code sent to your device.

5. Offline 2FA Apps: Utilize reliable offline 2FA apps like Google Authenticator, Duo Mobile, Microsoft Authenticator, or Authy. Avoid SMS, text-based, 2FA due to its vulnerability.

6. Device Encryption: Enable device encryption to shield your data even when the device is lost or stolen.

7. Regular Updates: Regularly update your phone's OS and apps. These updates often contain crucial security patches to address vulnerabilities.

8. Antivirus Software: Install reputable mobile Antivirus software to detect and counter potential threats.

9. Safe App Downloads: Download apps solely from trusted sources such as Google Play or the Apple Store. Review user feedback and scrutinize app permissions prior to installation.

10. Caution with Links and Info: Exercise caution when interacting with unsolicited emails or messages, refrain from clicking on links or sharing personal data.

11. Frequent Backups: Regularly back up your device to ensure data recovery in case of loss, theft, or compromise.

12. Public Wi-Fi Vigilance: Avoid unsecured or public Wi-Fi networks vulnerable to hacking. If using public Wi-Fi, consider a paid VPN for protection.

13. Public Charging Stations: Power off your device when using public charging stations. You can use USB data blockers or charge-only cables to prevent data transfer.

14. Account Activity Monitoring: Routinely scrutinize accounts for unusual activity and promptly address any discrepancies.

15. App Permissions Audit: Regularly review and revoke unnecessary app permissions that might jeopardize privacy and security.

By adhering to these enhanced measures, you significantly enhance the security of your cell phone and devices against potential hacking threats.

The Stingray Method: Unveiling the Controversial Use of Fake Cell Towers for Surveillance

Continued from page 2

by Flicker, CEO, Flickertronics

Cell-Site simulators operate by mimicking a legitimate cell tower so nearby mobile devices will connect to it instead of the providers actual tower.

These fake towers can be mounted on vehicles or deployed in fixed locations, be mounted in airplanes and is even being carried on the Predator **U**AV (**U**nmanned **A**erial **V**ehicle) drones.

When a cell phone, car Wi-Fi or other cell-connected device is turned on it continuously searches for the strongest available signal from nearby cell towers.

A cell-site simulator uses this behaviour and takes advantage by actively broadcasting signals that are stronger than those emitted by legitimate cell towers in the area.

To maintain the illusion that they are connecting to a legitimate cell tower, the ***Stingray Device*** forwards the device's signal to the nearest service providers tower, ensuring the user experiences uninterrupted service. This feature helps prevent suspicion or detection by the user.

Once a phone connects to the ***Stingray***, the ***Stingray device*** can capture a wealth of information from connected phones, including IMSI numbers, location data, call logs, phone conversations and real-time text message content.

More advanced versions known as ***Hailstorm*** or ***Kingfish*** provides additional capabilities such as injecting malware or spyware into targeted devices.

Cell-site simulators are deployed by Law enforcement agencies to track and capture suspects involved in criminal activities, aids in locating fugitives, and gathering vital evidence in riots and unrest.

These simulators have played a crucial role in combating organized crime, drug trafficking, terrorism, and kidnapping, and has resulted in the resolution of numerous cases.

Furthermore the data can be used to track and monitor rioters during and after demonstrations.

The military also uses these devices jamming abilities to prevent mobile phones from triggering explosive devices.

Military-grade IMSI catchers can imitate text messages, secretly intercept and relay messages and manipulate phone settings through silent SMS messages.

Military along with intelligence agencies have the ability to inject malware into the targeted phones by redirecting the web browser to a malicious website or by directly injecting it into the phones baseband processor.

Baseband malware is difficult to detect and can transform the phone into a listening device as well.

The baseband processor handles communication functions like voice calls, text messages and data transfers.

The most common use of Stingray devices is mounted in low flying, fixed-wing aircraft. The lower to the ground they fly, the stronger the fake cell-site's signal is.

In conclusion, Stingray devices are truly a marvel of modern technology and science and is a vlauble tool for law enforcement.

Brain Computer Interface - The Artificial Intelligence - Based Semantic Decoder

Continued from Page 1

by Flicker, CEO, Flickertronics

It will also enable more effective communication with people who cannot speak or have lost their ability to do so due to injury and disease.

The ***Semantic Decoder*** uses a combination of advanced machine learning algorithms and neural network models to interpret patterns of brain activity and translate them into coherent sentences associated with specific words and phrases.

In one particular test, Someone read the following text to a person who was connected to the **B**rain **C**omputer **I**nterface (**BCI**).

They heard the speaker read out loud to them, "***That night I went upstairs to what had been our bedroom and not knowing what else to do I turned out the lights and lay down on the floor***"

The Semantic Decoder text output read " ***We got back to my dorm room I had no idea where my bed was I just assumed I would sleep on it but instead I lay down on the floor***".

It works by analyzing the brain's electrical signals while the person is listening to a story or silently imagining telling a story, and then matches those signals to a vast database of of language patterns.

To develop the *Semantic Decoder* researchers trained the deep neural network on a large dataset of stories and their associated brain activity patters.

This training allowed the system to learn how to recognize the patterns of neural activity that correspond to different words and phrases.

Once the system has been trained, it can then be used to predict the words and phrases that a person is thinking about based on their brain activity patterns.

Researchers use the technology of ***fMRI*, or F**unctional **M**agnetic **R**esonance **I**maging, to measure the activity in different parts of the brain while a person listens to a story or imagines telling a story silently.

The data collected from the ***fMRI*** is then fed into a deep neural network, which can recognize the patters of activity associated with particular words and phrases.

Rather than capture a word-for-word transcript of participant's thoughts, The AI of the **B**rain-**C**omputer **I**nterface (**BCI**) summarizes their thoughts to produce a transcript illustrating the main point.

One potential application for this technology will be helping people who are unable to communicate due to conditions such as ***ALS***, or ***Locked-In Syndrome***.

ALS, also known as ***Lou Gehrig's Disease*** after famous baseball's ***Lou Gehrig*** passed away from it, is a rare neurological disorder usually caused by damage to the brain stem due to stroke, trauma, or disease.

ALS - Acronym for *Amyotrophic Lateral Sclerosis*.

ALS leaves a person concious and aware, but unable to move or speak except for eye movements or blinking.

With a *Semantic Decoder* they could think about what they want to say and the system could translate their thoughts into words and phrases that could be spoken aloud or displayed on a screen.

A *BCI* can one day enable the control of artificial limbs, exoskeletons or robotic prostheses for amputees , paralasys or other motor disabilities.

The potential for this technology to enable better quality of life to disabled individuals is truly amazing!

In closing, the *Semantic Decoder* has the potential to significantly advance our understanding of the human brain and its functions.

Thank you for reading, Flicker

Ensuring Safety: Essential Precautions and Tips for Women

by Flicker, CEO, Flickertronics

Personal Safety is a paramount concern for women in today's world. While everyone should feel secure, today women face unique challenges and vulnerabilities.

Here are some essential tips to consider and precautions that can significantly contribute to their safety.

1. Trust your instincts: Stay alert, avoid distractions, pay attention to your surroundings and trust your instincts, and remove yourself from any situation that makes you apprehensive. If you feel unsafe or unsure of your safety, dial 911 and inform them of your concerns. Do not confront other drivers.

2. Avoid Distractions: when you walk scan your environment, look confident and make eye contact to deter potential threats. Avoid excessive, intense cell phone use when walking alone or walking in unfamiliar places.

3. Use Well-Lit and Populated Areas: Stick to well-lit streets and areas with a significant amount of people, especially at night. Avoid shortcuts through secluded or unfamiliar locations.

4. Plan and Communicate: Tell a trusted friend or family member about your plans and estimated return time, especially when going out alone or traveling.

Include details such as the destination, estimated time of arrival, and update them about any changes in your plans. Stay in touch regularly and keep them updated.

5. Be Cautious With Personal Information: Be selective about sharing personal details online and offline. Limit The information that you put out on social media platforms to minimize the risk of being a target.

6. Be Cautious When Going Out and Meeting New People: keep your friends close and alert. Drink responsibly and guard your drinks. Do not give out your address or say where you live to someone you've just met.

7. Get a Google Phone Number: Do not give out your main phone number. You can get a free phone number and Google Voice app for your phone at **voice.google.com**

7. Trustworthy Transportation: Opt for reliable and licensed transportation services, especially during late hours. Having someone else with you provides an extra layer of security.

Screen Impact on Infants and Toddlers:

Long-Term Consequences

Continued from Page 1 *by Flicker, CEO, Flickertronics*

Prolonged exposure to tablet and cell phone screens can result in the following:

1. Disruptions to high order cognitive skills: Several different studies suggest that excessive screen time use for infants and toddlers can be associated with difficulties in problem-solving, perception, learning, and memory.

2. Brain Electrical Activity: A study, published in the **JAMA** Pediatric Journal, found that infant screen use was associated with altered ***Cortical ECG*** activity in children before age 2 years.

Cortical ECG activity is the electrical activity of the brain, specifically the ***neocortex***, which is the outermost layer of the brain.

The *neocortex* is the outermost layer of the brain responsible for higher ***cognitive functions*** and ***sensory processing***, or ***cognition***,

Cognition encompasses mental processes like perception, attention and memory, language, problem-solving, decision-making, shaping our understanding of the world, and guiding our actions through acquiring, processing, storing and using information.

4. Attention Deficit: Excessive screen time during early childhood has been associated with an increased risk of attention deficit problems.

A study published in **JAMA** Pediatrics found that each additional hour of daily screen time at 24 and 36 months was associated with a 10% increased risk of developing **ADHD**, ***Attention Deficit Hyperactive Disorder*** related symptoms by the age of 7.

5. Sleep Problems: Blue light emitted by cell phone and tablet screens can disrupt the sleep-wake cycle, particularly in infants and toddlers.

Exposure to screens blue light before bedtime can suppress the production of ***melatonin,*** the hormone that regulates sleep.

This can also lead to difficulties falling asleep, disrupted sleep pattern and shorter sleep duration.

Conclusion:

The effects of cell phone and tablet screens on infant and toddler's developing brains are a topic of growing concern.

It is critical for parents and care givers be aware of these potential long term consequences.

Broadband Cable and Fiber Optic Internet

Flickertronics is a Comcast Business and AT&T Solution Provider

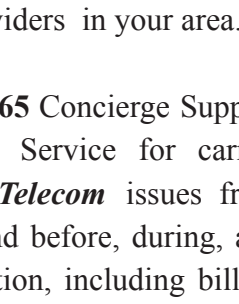
by Flicker, CEO, Flickertronics

Ever used an Insurance Broker, or a Real Estate Broker?

Why not a Telecom Broker?

Let an unbiased broker work on your behalf to find the optimal services for your company.

We may be able to improve your existing *Internet* and *Telecom* services while *lowering your monthly bills.*



Flickertronics* Represents Over 75 *Internet*, *Data*, *Telecom*, *VoIP, and ***Cloud Service providers***, offering businesses lower costs by cutting out the "***Middleman***", your local ***Reseller*** or ***Phone Man***.

Representing the major carriers directly, acting as their agent, we can provide the following services at no cost to you**:**

Free unbiased analysis of your current ***Internet*** and ***Telephone* services**.

Free unbiased quotes from all the current ***Telecommunications*** and ***Internet*** providers in your area.

Free 24x**7**x**365** Concierge Support and On-Site Service for carrier ***Internet*** or ***Telecom*** issues from pre-quote, and before, during, and after installation, including billing

We work with senior channel partners at the corporate level from ***Comcast***, ***AT&T***, ***Lumen***, ***HughesNet Satellite***, ***T-Mobile Business***, ***ViaSaT, Time Warner Business Class***, ***Verizon Business***, ***Airespring***, ***Level3***, ***Spectrum Business***, ***Lumen***, *as well as* ***DirecTV For Business***, *along with* ***RackSpace***, who are among some of our 75 + partners, and are serving our local area.

Flickertronics works through high level ***Dedicated Partner Channel Managers***, and ***Senior Partner Relationship Managers***.

Working through *Corporate Officers* assigned to ***Partner Relations***, ***Flickertronics*** bypasses their sales departments, which operates from a "***Canned***" script and has company sales incentives to get you to purchase additional products and services, ***and have no authority***.

A *Comcast Business Solution Provider* brings immense value to businesses by serving as their single point-of-contact for their connectivity and technology needs.

We are also an *AT&T Solution Provider* as well and hold similar positions with all 75+ providers.

For more information please contact Flicker Thomas:
(904)825-6708
flicker@flickertronics.com

Essential Tips For Asthma Sufferers

Continued from page 1 *by Flicker, CEO, Flickertronics*

3. Keep a Clean Indoor Living Environment: Keep your home clean and dust free and vacuum regularly. This helps to minimize exposure to potential allergens such as ***Dust Mites***, ***Pet Dander*** and other irritants that can aggravate asthma.

Dust Mites *- tiny microscopic organisms that live in bedding, upholstered furniture and carpets.*

Pet Dander *- proteins found in pet hair, saliva and skin cells can act as asthma triggers.*

4: Have a pest control plan: Common pests like cockroaches, rats, and other vermin can trigger asthma symptoms and aggravate respiratory conditions. Remove clutter, seal entry points into the building, and store food properly.

5. Mold Remediation: In Florida as well as other tropical and sub-tropical regions, mold poses a significant health threat. Exposure to mold spores can lead to respiratory problems and severe asthma attacks.

6. Maintain proper ventilation: Keep moisture under control and keep humidity levels below 50% to inhibit mold growth. Avoid carpet in high moisture areas, and use mold resistant materials whenever possible.

7. Allergens: Are substances that trigger an allergic reaction in individuals with asthma.

Common allergens associated with asthma include pollen from trees, grasses, weeds and flowers that can aggravate asthma symptoms.

8. Environmental Factors: Air pollution can take many forms such as industrial emissions, vehicle exhaust, smoke and second hand cigarette smoke, certain perfumes, strong odors, cleaning chemicals as well as aerosol sprays of certain kinds.

9. Emotional Factors: Strong emotions and stress can contribute to asthma symptoms. Anxiety, anger, excitement, stressful situations, and fear can trigger *bronchoconstriction* and make it more difficult to control asthma.

Bronchoconstriction *is narrowing of the airways caused by the contraction of smooth muscles surrounding the airways that causes breathing difficulties and asthma symptoms.*

10. Educate those around you: Inform family and friends as well as coworkers about your condition, its triggers, and appropriate emergency response procedures.

I had the paper ready to go to press, the finished pdf was up on my website and I had sent links to a number of my Managed Services Customers and some others.

Then I got a response with what I consider a "*Stop The Presses moment*" and edited this article before going to print.

Dr. Patel at Monahan Chiropractic Medical Clinics has offices in St. Augustine, Palatka & Palm Coast, and has contributed greatly to this article with his email containing the following remarks:

"*...breathing exercises as a beneficial addition for for asthma management. Numerous studies have demonstrated the effectiveness of these exercises. Research findings indicate a remarkable improvement of 60 to 75% in asthma symptoms and a reduced reliance on medication.***"**

11. Breathing Exercises: Asthma sufferers should practice breathing exercises because they help improve lung function, increase respiratory muscle strength, reduce breathlessness, manage stress and anxiety and help enhance overall breathing control.

Breathing exercises can greatly help manage asthma symptoms and decrease the frequency of attacks.

Use web searches for breathing exercises such as *Diaphragmatic Breathing*, *Deep Breathing*, *Pursed Lip Breathing* among some suggestions.

I welcome such reader feedback and I will be happy to put your good ideas and thoughts in print.

I would like to thank Dr. Patel for his contribution.

Combating Mold in Florida

by Flicker, CEO, Flickertronics

In Florida's subtropical climate, combating mold requires specific strategies. To prevent and remedy mold growth I recommend the following:

Manage Humidity: Keep indoor humidity below 50% using dehumidifiers, proper ventilation, and timely repairs for leaks and water intrusion.

Regular Cleaning: Keep kitchens, bathrooms, basements and other moisture-prone areas clean and dry. Promptly remove visible mold traces with soap and water.

Enhance airflow: Maintain good airflow using fans, open windows, use air conditioning systems when possible.

Insulation and vapor barriers: Properly insulate walls, roofs, and floors. Install vapor barriers to prevent condensation and moisture buildup.

Regular Inspections: Check for mold signs like musty odors, water stains, or discoloration. Address any issues promptly.

Mold Remediation: Thoroughly clean mold-affected areas with suitable products and techniques, ensuring proper drying to discourage regrowth.

Use containment barriers to keep mold from spreading, repair any leaks or moisture intrusion to prevent recurrence, and consult a specialist for severe problems.

Understanding Cell Phone VPNs

What They Protect and What They Don't Protect

Continued from Page 3 *by Flicker, CEO, Flickertronics*

What Cell Phone VPNs Do Not Protect

1. Tracking and Data Collected by Apps: While a ***VPN*** helps protect your online activities from external parties, it does not prevent apps that are installed on your device from collecting data about your usage.

2. GPS Location Tracking Data is Not Hidden: While a ***VPN*** changes your *IP address*, it does not alter your ***GPS*** location tracking data.

Disabling the *GPS* settings on your phone offers only a partial solution since applications can access and use the device's ***GPS*** chip even when you have it "***Turned off***" in settings.

3. Malicious Apps and Malware: ***VPNs*** do not offer protection against installation of malicious apps or malware being installed, on your cell phone. ***Stingray Devices***, which are fake cell-towers, can still secretly inject those apps onto your cell phone.

4. Only download apps from ***Google Play*** or the ***Apple Store***. Keep all of your software up to date as the latest software patches will include security as well as performance updates as well as hardware or software bug-fixes.

5. Metadata Collection: Many apps collect and track user data for many various purposes, such as personalized advertisements or analytics.

Metadata is generated when we use digital devices and services. It includes details such as the date, time, the duration, location, and recipients of your communications, as well as the websites we visit, apps we use and more.

This *Metadata* can provide valuable insights into our digital activities, even if the content is encrypted with a ***VPN***.

6. Review app permissions as well as using additional tools like privacy oriented search engine apps like ***DuckDuckGo***.

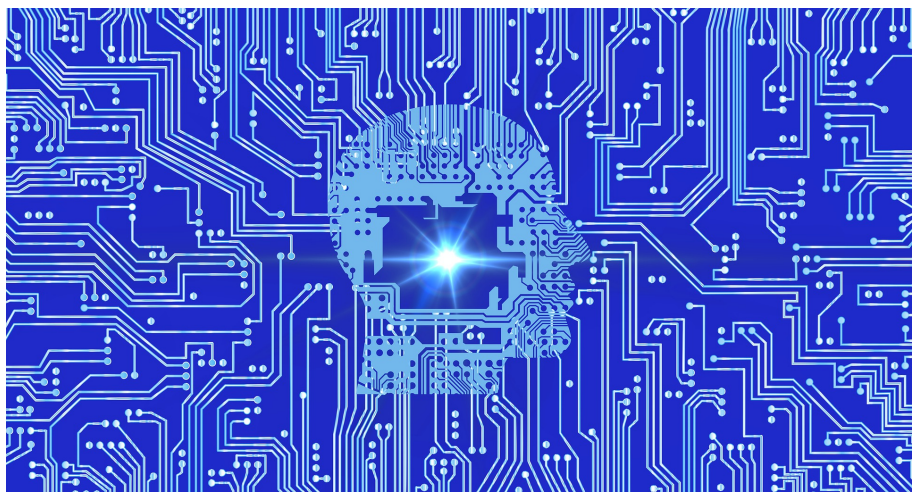
If an app or service has access to your ***GPS*** data and permissions, it can still track your physical location, and even covertly turn on your ***GPS*** tracking chip without your permission.

In conclusion, VPNs do not conceal metadata, guard against malicious apps or malware, or prevent app tracking and data collection or ***GPS*** data.

Flickertronics Managed Services

For Less Than The Price of a Cup of Coffee Day Per Computer
You can Have Your Own 24x7x365 IT Department PLUS
Have Your Computers Protected By Artificial Intelligence!

by Flicker, CEO, Flickertronics



Do you or your current IT provider use obsolete ***Antivirus*** Software to provide protection for your computers?

Commercial Antivirus Software was Invented in 1987 - While ***John McAfee*** did not write the first ***Antivirus*** software, he did create the first commercially available product.

The Artificial Intelligence and Machine Learning Technology of ***SentinelOne*** represents the latest state-of-the-art protection for your computers and networks.

Combining a hardware Firewall and *Antivirus* Software is no longer an adequate way to protect your computer or network.

False sense of security: The use of obsolete and outdated programs like ***Antivirus*** software to protect computers has led to devastating ***Ransomware*** attacks.

These now-obsolete methods of protection offer a *false sense of security* to the business clients who have entrusted their entire livelihood to IT organizations that make use of obsolescent, archaic and now proven dubious methods.

All Industries are Affected: Critical infrastructure such as power grids, government agencies, hospitals, as well as businesses of all types, have all suffered devastating losses from IT departments using these obsolete products.

We prioritize the ultimate in protection, choosing not to profit from obsolete *Antivirus* software. Avoid business failures caused by these outdated and questionable methods.

24x7x365 Support included: Our live, real time technical support operators are available 'round the clock, including holidays

Your employees will have the ability to have their problems resolved in ***real-time as they occur*** by simply by making a phone call to one of our remote support technicians when a problem occurs.

This allows your problems to be resolved quicker than other IT companies who do not operate in real time, using ticketing systems which are designed to add layers of complexity and cost to resolve simple, everyday issues.

These are the typical steps for your employees to obtain IT support:

Flickertronics: - Computer user has a problem with a printer and calls one of ***Flickertronics*** remote support operators, they remote in and resolve the problem in minutes, emailing their supervisor with no charges to your company.

Other IT Companies:

1. User has a problem with a printer.
2. User notifies supervisor they have a printer issue.
3. Supervisor starts a trouble ticket with their IT provider.
4. IT provider receives support request and puts it on the schedule as a low priority call.
5. A technician is assigned to the trouble ticket.
6. Technician Remotes in hours or days later to take care of problem.
7. IT provider sends report and a bill for $100.00 or more.

Continued above right

Flickertronics Managed Services (continued)

24x7x365 Remote Monitoring and management: Near real-time monitoring for all your devices. 60, 30, 15, or 5 minute checking intervals available for checks.

Emails you daily health check reports: Daily, weekly reports as well as a monthly Executive report available.

Backup Documents : is deployed automatically and finds all the business documents on your computer and backs them up automatically twice a day, with a retention time of 28 days.

Backs up over 90 different file extensions! Word, Excel, PDF.

The Backup Documents feature is engineered to automatically find business documents, spreadsheets, presentations, and word processing files wherever they are stored on your hard drive.

End user self-service - Users can log in via a system tray icon to search and select the backed-up document they need to recover from one of the up to 56 restore points in the past 28 days, without waiting on technical staff.

Vulnerability Scanning and Patch Management: Supports operating system updates as well as updates for multiple third-party software applications such as Chrome, Firefox, Adobe products among the hundreds of others.

Web Protection: Content filtering allows you to set times or prohibit social media and other sites on company computers.

Asset and Inventory Checking: Asset and inventory tracking creates an inventory of Windows, Mac, and Linux computers.

Besides our Remote Monitoring and Management offerings, the following Daily Safety Checks are run once per day:

Physical Disk Health Check: checks that your disks are healthy and there are no integrity issues.

Drive Space Check: Makes sure you have adequate disk space left. Running out of disk space can cause your computer to crash and may cause lengthy delays to repair the device.

Critical Events Check: Reviews critical event log entries and spots problems and issues.

Backup Check: Ensures your computer backup has been completed successfully.

Failed Login Check: Looks for unauthorized log in attempts.

File Size Check: Allows multiple files, folders and sub-folders to be monitored and generates an alert when the size of the group of files is greater or less than the specified size.

***Microsoft SQL Server* log files can easily grow to fill the entire disk** if it experiences problems, and unexpected changes can be indicative of other, serious problems.

Patch Status Check: Scan runs every day on the local machine and detects missing patches and vulnerabilities

Web Protection Bandwidth use Check: Monitor website download traffic on the computer and can be set so that you receive a warning when the amount of downloaded data exceeds a certain, specified amount.

Sentinelone Artificial Intelligence Engines

***DFI AI* : (D**eep **F**ile **Inspection)** preventative *AI Engine* scans for malicious files on disk. Scans on file execution and disk write.
***DFI AI-Suspicious*:** Static *AI Engine* scans for suspicious files.
DBT AI - Executables (**D**ynamic **B**ehavioural **T**racking): This is a behavioural *AI Engine* that implements *Advanced Machine Learning* tools & detects malicious activities.
***Documents/Scripts AI*:** Behavioural *AI Engine* for all documents and scripts types.
***Lateral Movement AI*:** Detects attacks from remote devices.
***AntiExploitation,Fileless AI*:** Behavioural *AI Engine* for exploits and fileless attacks.
***Potentially unwanted Applications AI*:** Static *AI Engine* inspects apps on macOS.

Contact Flicker: (904) 825-6708
flicker@flickertronics.com

Recycle St Johns County and St Augustine

What to Put in Your Recycling Cart and What Not To

Information compiled from the city and county websites by Flicker, CEO, Flickertronics

St Johns County

In St Johns County there are 5 categories of items that can be recycled, and put in your recycle bin.

Paper and Cardboard:
Newspapers, catalogs, magazines, cereal and food boxes, junk mail, flattened cardboard, & office paper

Plastic Containers:
Clean and empty food and beverage containers, soap bottles and jugs, empty pill bottles (Labels do not need to be removed). No Styrofoam and no plastic bags

Metal:
Aluminum and metal food and beverage containers only (clean and empty)

Glass:
Bottles and jars (clear, green, brown) only. No windows or ceramic containers

Cartons:
Clean and empty milk, juice, soup, broth, and wine cartons

Do Not Recycle the Following:

Recycling Equipment Tanglers:
No plastic bags or film wrapping, holiday lights, wire, fishing nets, electronics or bubble wrap

Non-Container Plastics:
No toys, hangers, packing peanuts, garden hoses, etc.

Contaminants:
No food waste, garbage, ceramic containers, Styrofoam, diapers, mirrors, window panes, tires, yard waste, or any item not listed on the acceptable recycling list.

Leave all recyclables loose in bin. Bagged recyclables are not sorted and plastic bags get tangled in the sorting equipment causing it to jam and shut down recycling.

For questions regarding the St Johns county "Recycle St. Johns" program and recycling **program here is the contact information:**

(904)827-6980
www.recyclestjohns.com
solidwaste@sjcfl.us

City of St. Augustine

The city of St. Augustine has a flyer "Recycle Right: A best practice guide to curbside collection". Here are the contents:

Milk and Juice Cartons:
Containers must be empty, clean, loose and dry.

Return plastic bags and egg cartons to retailer.

Aluminum, Tin, and Steel Cans:
Containers must be empty, clean loose and dry.

Plastic Bottles and Jugs: empty and clean.

Cardboard: Flattened

Paper:
Newspaper, Magazines, Office Paper, Junk Mail.

No Paper Towels, Napkins or Shredded Paper.

The Following are Not Accepted:

Glass Bottle and Jars

Equipment Tanglers:
Plastic Bags, Rope, Cables, Christmas Lights.

Styrofoam:
Egg Cartons, packaging material, bubble wrap, take out containers.

Light Bulbs, Electronics and batteries.

Hazardous Waste & Materials:
Paint Cans, Chemical Jugs or Cans, Propane Tanks.

For questions regarding the City of St Augustine's Recycling program contact them at:

(904)825-1049, Extension 2
recycle@citystaug.com

Manufacturers VIN Recall Search Tool

by Flicker, CEO, Flickertronics

Manufacturers Recall Search by VIN Number at:
www.nhtsa.gov/recalls

The VIN, (Vehicle Identification Number) can be used to look for safety and maintenance recalls and alerts on your vehicle.

The vehicle's VIN number is a 17-character alphanumeric code that provides specific information about a vehicle including its manufacturer, model and features.

The VIN number can be found by looking at the dashboard on the driver's side of the vehicle, or on the drive's side doorpost where the door latches when it is closed.

The information below has been transcribed from the website:
www.nhtsa.gov/recalls

What the VIN Search Tool Will Show:

1. An unrepaired vehicle affected by a vehicle safety recall in the past 15 calendar years.

2. Vehicle safety recalls from the major light car manufacturers, as well as motorcycle manufacturers and some medium/heavy truck manufacturers.

What the VIN Search Tool Will Not Show:

1. A vehicle with a repaired safety recall. If your vehicle has no unrepaired recalls, you will see the message: "***0 Unrepaired recall associated with this VIN***".

2. Manufacturer customer service or any other non-safety recall campaign.

3. International Vehicles.

4. There may be a delay with very recent announced safety recall for which not all VINs have been identified. VINs are added continuously so please check regularly.

5. Safety recalls that are more than 15 years old (except where a particular vehicle manufacturer offers more coverage).

6. Safety recalls that are conducted by some of the small vehicle manufacturers, including some ultra-luxury and specialty applications.

VIN Locations

The Internet of Things (Iot)

Continued from Page 1

allowing devices to seamlessly communicate as well as to share information.

This connectivity is made possible through sensors that gather data, network connectivity, for example a Wi-Fi or Ethernet connection for data transmission, and cloud-based platforms for storage and processing.

IoT enables businesses to optimize operations, improve productivity, and offer innovative services. Likewise, individuals can enjoy the benefits of smart homes, wearable devices, connected cars, and more.

However, the widespread use of IoT devices also raises concerns about security, privacy and data management.

As billions of devices become interconnected, it becomes crucial to ensure robust security measures are put into place to protect sensitive information.

IoT has the potential to revolutionize industries, enhance our quality of life, and drive automation.

As it continues to evolve, **IoT** will significantly shape the future by enabling smarter and more connected environments.

Artificially Intelligent Machines now have the ability to contact and can now control the **IoT** devices.

In conclusion, **IoT** is a technology that connects physical objects to the digital world, enabling data driven insights and automation.