FREE

Tech Source News

FREE

Third Edition | Flickertronics Technical News Publication | www.techsourcenews.com

The Beginning of the Internet and the History of Viruses

by Flicker

To understand the history of viruses and the creation of the first antivirus software, it's essential to understand the origins of the Internet.

While the first viruses were spread through floppy disks, the Internet is now the primary pathway for viruses and other malicious software.

During the cold war in 1969, ***ARPANET*** was established by the **DOD** (*United States **D**epartment **O**f **D**efense*).

Raytheon BBN Technologies (originally *Bolt Beranek and Newman Inc.*) developed the first packet-switching networks for ***ARPANET***, which stands for ***A**dvanced **R**esearch **P**rojects **A**gency **N**etwork*.

ARPANET primarily used leased telephone lines to connect remote computers, especially in its early days.

Continued on Page 4

What is a Rootkit

by Flicker

Rootkits are one of the most dangerous forms of *malware* because they are able to evade detection and maintain deep system control.

Malware is harmful software designed to damage, disrupt, or steal information from computers and devices.

Malware can take many forms such as **Rootkits**, **Ransomware,** V**iruses**, **Spyware**, **Keyloggers**, take advantage of vulnerabilities in hardware such as **BIOS**, **UEFI**, network cards, infect hard drives, GPUs (video cards), or devices attached to the computer.

Malware often spreads through infected files, emails, or websites and can take advantage of vulnerabilities in software or hardware.

Continued on Page 5

"Of course I watch television while I work. Why do you think it's called 'tele-commuting'?"

How Love Led To The Invention Of Cable TV

by Flicker

On June 19, 1986 Richard Barton interviewed *Leroy "Ed" Parsons*, the inventor of Cable TV, as part of the *Hauser Oral History Project.*

In the audio recording *Ed Parsons* tells his story. I read the transcript of audio recording and did extensive research then wrote the following article.

Ed Parsons **had owned** a refrigeration service in *Fairbanks, Alaska* before World War II. After the war started his business could not get civilian equipment because everything was designated for the military so he closed his business.

Continued on Page 6

The latest Online AI Scams

by Flicker

The goal of online criminals, mostly referred to as scammers or hackers, is to harvest your personal information or money.

The latest tricks used by these cybercriminals uses ***Artificial Intelligence***, commonly referred to as **AI**. The following from the **FBI** is the best presentation of these new dangers.

The FBI has released a bulletin which is the best presentation I have seen for making you aware of how serious a threat these new forms of attacks present.

Continued on Page 5

What is a Virus?

By Flicker

A computer Virus is a type of ***malicious software*** (***malware)*** that replicates and spreads to other computers.

It attaches itself to legitimate files or programs and performs malicious actions when the infected file is opened, such as slowing down the computer, deleting data, or stealing personal information.

Continued on Page 3

Prevent USB Flash Drive Data Loss

Several factors contribute to data loss on *USB drives*, including power spikes, read-write errors, and manufacturer defects.

When you move files to and from a *USB drive*, the computer doesn't write them to the disk immediately but instead caches them in the computer's memory (**RAM**).

Ejecting the drive signals the computer to finish writing all cached data to the *USB drive*, ensuring the files are fully saved.

If you remove the drive without ejecting it first, the computer may not have completed writing the data.
This can lead to file corruption, lost data, or even damage to the drive's file system.

Safely ejecting the drive ensures that all data is properly written, reducing the risk of these issues and the computer disconnects the 5.0 volts DC power to the *USB device*.

Continued on Page 2

What is a Bot? What are Botnets? What is a Zombie Computer?

by Flicker

You may have seen terms like **"Bots"**, **"Zombies," "Zombie Computers"** and **"Botnets"** in news reports about data breaches and cybersecurity threats.

A Bot, short for **"Internet Robot" or "Web Robot,"** is a software application or script that runs automated tasks online. When a device is infected by a **Bot**, an attacker has complete remote control over it.

Bots can target various devices, including computers, smartphones, routers, servers, gaming consoles, and Internet of Things (**IoT**) devices.

Continued on Page 7

Zombie Ants To discuss

by Flicker

Cordyceps "Zombie Fungus" takes over *Carpenter Ants'* bodies

From Zombie computers to Zombie ants - this article covers an interesting and very terrifying phenomenon.

The Thailand and Brazilian rainforests are inhabited by a species of ***Carpenter ants*** known as ***Camponotus leonardi***.

When they descend to the rainforest floor to forage for food they may encounter a parasitic fungus called ***Ophiocordyceps unilateralis.***

Ophiocordyceps unilateralis is a species parasitic fungus that infects ants and manipulates their behavior to benefit the fungus's reproduction. And when it does, it turns the ants into "**Zombies**".

Species specific means that this particular fungus affects only the members of a particular species, i.e. ***Camponotus leonardi,*** the Carpenter ant.

Continued on Page 7

Flicker's Story or "Mom, I hear Voices in The Oven" *Page 2*

What is a Virus? *Page 3*

Essential Precautions and Tips for Women *Page 4*

Manufacturers VIN Recall Search Tool *Page 8*

continued from page 1

Prevent USB Flash Drive Data Loss

by Flicker

As you use the drive, processes like reading and writing data are happening in the background that are unknown to you.

For example, when you access a file, the computer may modify certain metadata, such as the last modified date and time.

These changes are handled in batches, first stored in the computer's cache memory and later written to your *USB drive*.

The "*Safely Remove Hardware*" command (*or ejecting*) resolves this issue in the following ways**:**

- It ensures that all cached data in the computer's memory (**RAM**) is written to the *USB drive*, preventing data loss.
- It sends a notifications to programs (*that can respond*) notifying them that the disk is about to be removed, allowing them to take appropriate action.
- If any programs fail to close files or release resources, the system alerts the user, thus preventing potential file corruption.
- Ejecting the *USB drive* properly ensures that files are safely closed, preserving data, pointers, and file size indicators.

Without ejecting the USB drive, the computer might not fully "*flush*" the buffer, meaning only part of the data may be written to disk. Following the proper procedure guarantees that the data is written to the USB device and saved without corruption of the files.

Ejecting the USB drive properly ensures that files are safely closed, preserving data, pointers, and file size indicators.

Without this process, the computer might not fully "flush" the buffer, meaning only part of the data may be written to disk. Following the proper procedure guarantees that the data and pointers are correctly saved.

Ejecting a *USB drive* signals the system to stop supplying 5V power after all of the data in the cache is written.

USB drives need stable power for 0.25 seconds to ensure proper data saving. Without it, incomplete writes can cause corruption, potentially leading to the loss of an entire directory.

Not ejecting a USB drive before disconnecting can also cause what are called ***transient spikes*** in the 5.0 volts DC power supply that can overload, or burn out, some of the memory components on the un-ejected *USB drive*.

A ***transient spike*** is a brief surge in electrical voltage that can occur when a device is disconnected improperly.

These *transient spikes* can overload circuits, potentially damaging or destroying sensitive components like memory chips.

When a USB drive is not ejected properly, it can lead to unstable power conditions that create transient these voltage spikes.

In a 5.0 VDC circuit that powers a USB device, transient spikes can theoretically range from 15-30 volts up to 100 volts or more.

The duration of these spikes is usually very short, often lasting from microseconds to milliseconds.

Even though they are brief, their high voltage levels can still damage sensitive components like memory chips, microcontrollers, or other integrated circuits.

Properly ejecting a USB drive is much more than a simple precaution it's a way to avoid potential damage that could ruin the drive or data stored on it.

Flicker's Story or "*Mom, I hear Voices in The Oven*"

by Flicker

Being in business for over 25 years I have had hundreds and hundreds of people ask me how I became interested in electronics.

This is the wondrous tale that started me upon my path.

I was almost 6 years old, and we had just moved to Jacksonville, Florida.

As a child I was always into everything, reading, poking and prying into things. One day I opened the door to our electric oven and heard voices.

I ran into the other room and yelled for my mom to come into the kitchen and told her I heard voices coming from the oven.

We walked into the kitchen and opened the oven door and there was complete silence. My mom just gave me a puzzled look and walked back into the living room and sat back down and continued to watch TV.

Over the next few weeks I kept hearing music and voices in the oven, and each time I summoned my mom, dad or my sister the music would stop.

Mom, Dad and my sister were finally convinced that I had some mental illness or affliction that was getting worse.

Then one day my mom was standing in the kitchen near me when I decided to open the oven door and see what would happen.

I heard people talking and called for my mom to come over. She just stood there and gave me a look of sorrow and pity for her poor sick child.

In desperation I went to her and dragged her by the arm and screamed for her to listen.

She stuck her head in the open oven door and heard music for a few seconds. The look on her face was utter shock since she was experiencing the same delusions her poor, sick child had been.

During the next few days or so everyone was sticking their heads in the oven to hear the people talking and the music playing briefly for a few seconds.

Then one day we heard them announce WAPE and discovered we were hearing the local AM radio station less than one half mile away.

I was mesmerized by the thought that you could hear a radio station in your electric oven.

I had to find out how this could possibly happen so I went to the library and started my quest for knowledge (which has never ended)

I learned that when two pieces of metal are touching and are oxidized (corroded) they can actually function as a rectifier, which is a diode detector. This would generate sound like a Cat's Whisker Crystal Radio Detector, which was used in early radio Sets (*The Cat's Whisker was a small piece of wire – no cats were ever harmed!*).

The close proximity of the local AM radio station and a rusty connection in the stove is what made this feat possible! This phenomenon only occurs with AM (Amplitude Modulated) radio signals, and not in FM radio (Frequency Modulated) signals.

The term "Cats' Whisker" refers to a thin wire that lightly touches a crystal of semiconducting mineral (a rectifier or Diode Detector, which is usually made from galena) to make a crude point-contact rectifier.

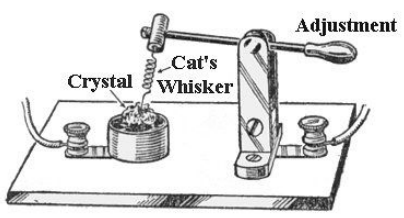

Diagram of a crystal radio from 1922 using a cat's-whisker detector.

From then on I read everything I could about electronics and electricity that was available. This is a prime example of how children can be affected by things they are exposed to early in life.

What is a Virus?

by Flicker

The Origins of the Terms "Virus" and "Worm"

The term "virus" was first introduced in 1983 by *Fred Cohen* during his study of self-replicating programs. He defined a **virus** as a program capable of infecting other programs by modifying them to include a copy of itself.

The term "worm" predates "**virus**" and was first used in 1975 by *John Shoch* and *Jon Hupp* at **Xerox PARC**. They described it as a self-replicating program that spreads across networks between computers, similar to how a biological worm moves through the ground

How a Virus Infects a File or Computer:

Infection: A **virus** enters your computer when you accidentally open an infected file, often from email attachments, downloads, or a USB drive.

The infected file could be a program (.exe) or a document with harmful *macros*. A *macro* is an automated sequence of commands used to perform repetitive tasks, especially in applications like Microsoft Word or Excel where they can record a series of keystrokes.

Activation: Once the infected file is opened, the **virus** activates. It searches for other files to infect, often targeting programs because they are executed frequently and can spread the **virus** easily.

How a Virus Infects a File:

Opening the File: Similar to how you open a file to read it, a **virus** uses special system functions provided by the operating system which allow programs to interact with files, memory, and hardware, allowing the **virus** to "open" and infect them.

Finding the Entry Point: The **virus** locates the program's entry point, which is the location where the computer begins running the program. This entry point is found in the file's structure, specifically in the *Portable Executable (PE) header*, which acts like a table of contents for the program.

Injecting Malicious Code:

The virus can either:

Overwrite: The **virus** replaces parts of the original program with its own malicious code.
Or
Append: The **virus** adds its code to the end of the program and changes the program's entry point so the **virus** runs first.

Restoring Control:
Once the virus has run its malicious code, the **virus** transfers control back to the original program, allowing the program to operate as usual and keeping the infection hidden.

Spreading the Infection:

Once the virus infects one file, it searches for other files on the same computer, and network-aware viruses may even try to access other devices across a network to repeat the process.

Staying Hidden or Persistence :

To avoid detection or removal, viruses often:

Copy themselves into critical system files that load when the computer starts.

Modify the boot sector or create registry entries to ensure the **virus** runs when the computer starts.

The boot sector is a critical part of your hard drive that launches the operating system during startup. Additionally, **viruses** may create entries in the system's startup files to ensure they automatically execute when the computer boots.

Advanced Virus Tricks:

Viruses are using sophisticated techniques to avoid detection:

Encryption: They encrypt, or scramble their code to prevent antivirus software from recognizing them.

Polymorphism: They change part of their code structure each time they replicate (make copies of themselves), making them harder to detect.

Metamorphism: The **viruses** can completely rewrite themselves, making them appear as entirely new programs with each infection.

Types of Computer Viruses:

File Infector Viruses: Attach to executable files (**.EXE**), becoming active when the infected program runs.

Macro Viruses: macro viruses target applications that use macros (*like Microsoft Word*), embedding themselves in documents.

Boot Sector Viruses: Infect the boot sector of storage devices, activating during system startup.

Polymorphic and Metamorphic Viruses: Modify or rewrite their code structure entirely to avoid detection.

Resident Viruses: Embed themselves in the computer's memory, allowing them to infect files even when the original host program is not running.

Impact of Computer Viruses

The effects of a virus can include:

Data Loss: Corruption, deletion, or encryption of data.

System Performance: High resource consumption leading to slow performance or crashes.

Security Breaches: Creation of backdoors which can allow unauthorized access to the system.

Financial Cost: Expenses for data recovery, system repairs, and potential legal liabilities.

Reputation Damage: Harm to organizations experiencing **virus** outbreaks, especially if customer data is compromised

Prevention and Protection Against Viruses:

To defend against computer viruses, consider the following strategies:

Antivirus Software: Scans for known **viruses** and provides real-time protection.

Anti-Rootkit scans: Scan your computer with programs designed to detect and remove **Root-Kits** since **Root-Kits** are designed to evade traditional antivirus programs.

Regular Updates: Keep operating systems and applications updated to protect against vulnerabilities.

User Education: Inform users about safe computing practices, such as not opening unknown email attachments.

Firewalls: Implement hardware firewalls to block unauthorized access to your network.

Regular Backups: Maintain up-to-date backups of important data.

Conclusion

Understanding computer viruses and their methods of infection, types, and impacts is essential for effective prevention and response.

By using antivirus software and keeping systems updated, you can significantly reduce the risk of infection and lessen the potential impact of computer viruses.

Poem to my Dear Sweet Love

by Flicker

Your heart was heavy and your soul was worn,
burdened by life and feeling torn.

When I entered your world, a ray of light,
My heart felt your struggles, your endless fight.

You saw something in me, and I in you,
Our souls connected in a bond so true.

Together, at each others side,
we can fight the world and find our stride.

Though time may separate us, our souls entwine,
Aligned in spirit, our bond divine.

The Beginning of the Internet and the History of Viruses

continued from page 1

by Flicker

The U.S. military, through the ***Defense Advanced Research Projects Agency*** (**DARPA**), aimed to create resilient remotely connected computer networks that could withstand partial outages, such as in the event of a nuclear strike.

Similarly, universities sought to develop a fault-tolerant network over unreliable leased connections to share data and computing resources between different locations. This need led to the development of **ARPANET**, the precursor to the modern internet.

***ARPANET* was also one of the first** networks to use the **TCP/ IP Protocol Suite** which laid the foundational framework for how data is transmitted across networks today.

TCP/ IP stands for (**T**ransmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol)

Viruses and Worms

The first computer virus, known as **"Creeper"** was created in 1971 by ***Bob Thomas***, a programmer at **Raytheon BBN Technologies** in the United States.

Its purpose was to explore the concept of a self-replicating program that could move between computers, though it is more accurately classified as a **Worm** rather than a **Virus**. The terms "**Virus**" and "**Worm**" came later.

In the same year, ***Ray Tomlinso***n, a fellow scientist and collaborator of ***Bob Thomas***, developed an updated version of **Creeper** that replicated itself as it moved across the network, making it the first computer **Worm**.

When Creeper infected a system, it displayed the message**: "I'm the Creeper, catch me if you can!"** on the terminal of the infected computer.

It would then seek out another system running the **TENEX operating system**, establish a connection, and transfer itself to the new machine, continuing its movement through the network and attempting to delete itself from the previous host while displaying its message.

Creeper didn't install multiple instances of itself on several targets instead, it moved around the network. The Techniques developed in **Creeper** would later be used in the ***Multi-computer Route Oriented Simulation System*** (**McROSS**), an air traffic simulation program that allowed parts of the simulation to move across networks.

Although Creeper caused some disruptions, it wasn't considered malware by today's standards, as it didn't destroy data or render systems inoperable. Its only effect was the display of its message.

To remove Creeper from infected systems on ***ARPANET***, ***Ray Tomlinson*** then developed a program called **Reaper**. This program moved through the network, detecting and removing instances of **Creeper**.

Although not a traditional antivirus, **Reaper** *functioned* as a virus designed specifically to delete the self-replicating **Creeper** program. This highlighted the experimental and innovative spirit of early networked computing.

Pakistani Brain Virus

In 1986, the "Brain" virus, which is actually a **Boot Sector Virus,** was created by Pakistani brothers ***Basit*** *and* ***Amjad Farooq Alvi***, who owned a computer store in *Lahore, Pakistan.*

The boot sector is located at the beginning of the storage device and initializes the operating system

Frustrated by the unauthorized copying of their heart monitoring software, they developed the software program to protect their medical software from illegal distribution.

Targeting IBM PCs, the "**Brain Virus"** slowed down floppy disk drives, reduced available system memory, and altered disk labels to read **"©Brain"** .

It also inserted a message in the floppy disk's boot sector, providing the brothers' contact information and offering a *Vaccination service*.

The Brain virus was the first widespread malware infection, with estimates indicating around 100,000 compromised devices within just a couple of years of its release.

While the virus slowed down infected devices, it did not cause any damage, and it was not programmed to delete files.

Instead, it featured a mechanism that automatically copied its files to disks, allowing it to infect more computers whenever the same disk was used.

In 1987, a number of antivirus solutions emerged in response to the Brain virus.

The German company G Data Software AG, founded by security experts ***Andreas Lüning*** and ***Kai Figge,*** launched an antivirus solution specifically for **Atari ST computers.**

In 1987, cybersecurity experts ***Peter Paško, Miroslav Trnka,*** and ***Rudolf Hrubý*** developed the first **NOD32 Antivirus**.

That same year, ***John McAfee*** successfully decrypted the operation of the "**Brain Virus"** and developed **VirusScan** to remove it.

He founded McAfee Associates and released ***VirusScan***, which became the first antivirus program specifically designed to neutralize the "**Brain Virus**", achieving over 1 million users within two weeks.

The early Creeper and Brain viruses were pivotal in prompting the development of antivirus solutions.

Robert Morris, a computer science student at ***Cornell University***, released a worm onto the Internet from the ***Massachusetts Institute of Technology*** on November 2, 1988.

The worm was an experimental self-replicating program that exploited email flaws.

A programming error caused the program to endlessly replicate itself, overwhelming memory and disabling 6,000 computers - about one-tenth of the Internet at that time - before a fix was found.

This is how it all began - others exploited these technologies to create evolving threats, and are now using artificial intelligence for increasingly insidious attacks.

Ensuring Safety: Essential Precautions and Tips for Women

by Flicker

On page 5 of Tech Source News First Edition I wrote an article about safety tips for women.

Several hours after I ordered 2500 newspapers to be printed I saw in the news several items regarding women whose cars had been hijacked because their doors were unlocked.

Please read the article I mentioned and follow these additional precautions:

- Park in well-lit populated areas
- Keep car doors locked at all times
- Keep the doors to your home locked - opportunistic criminals take advantage of unlocked residences every day. Lock the doors where you work if practical.
- Stay alert and aware of your surroundings
- Keep your phone fully charged and accessible
- Carry a portable charger in case your phone dies
- Avoid letting other people use your phone, especially strangers. This is the most common way for scammers or untrustworthy acquaintances to be able to gain remote access to your devices.
- Accept drinks only from trusted sources like friends or bartenders
- Avoid accepting drinks or open containers, especially from strangers or if the seal is broken
- Go out with a trusted friend and keep an eye on each other, each one looking for signs of being too intoxicated.

I hope these additional precautions help you to be more aware of your surroundings.
Thank you, Flicker

What is a Rootkit (continued) by Flicker

The BIOS (***B**asic **I**nput-**o**utput **S**ystem*) serves as the interface between the operating system itself and the computer's hardware, initializing hardware components and loading the operating system.

The **BIOS** runs when the computer starts, communicating with all internal components and peripherals, checking their status, and then loading the operating system to ensure the system functions properly.

UEFI (***U**nified **E**xtensible **F**irmware **I**nterface***)*** is a modern replacement for the traditional **BIOS** (***B**asic **I**nput-**O**utput **S**ystem***)*** firmware found in computers with faster boot times and more features than **BIOS**.

A Rootkit is a type of malicious software designed to gain unauthorized access to a computer system and remain hidden from users and security software allowing them to spy, steal data, or manipulate the system without the user knowing.

It buries itself deep in the system, often evading *antivirus* detection and making it extremely difficult to remove.

Rootkits allow attackers to take control of a system at a deep level, often with administrator (*or "root"*)privileges, hence the name "**Rootkit**."

By using various techniques they conceal their presence by hiding processes, files, or system data, making them difficult to detect.

Rootkits give attackers the ability to control the infected system remotely, often allowing them to steal data, install more malware, or manipulate system functions.

Rootkits are built to avoid being detected by antivirus software and remain in the system even after reboots, often by integrating themselves into core system files or the operating system itself.

They also give attackers complete control over a system.

Rootkits are particularly dangerous because of their ability to evade detection while giving attackers ongoing control over the system.

To protect against them use antivirus and use anti-malware software that specializes in detecting rootkits and other advanced threats. Look for increased CPU usage or other signs of unusual activity.

Enabling secure boot in the BIOS blocks rootkits that specifically target the boot process by preventing unauthorized code from running during system startup.

Make regular backups of critical files and do s monthly image backup of critical computer systems, such as servers.

Use a physical firewall that comes with a subscription for intrusion detection and prevention software. Limit physical access since it only takes a matter of seconds to infect a system with a USB drive.

Rootkits are dangerous because they remain hidden, giving attackers deep control over systems.

Prevention requires strong security practices and using caution with suspicious files to protect against these persistent threats.

In conclusion, Rootkits are a significant threat due to their ability to remain hidden while providing attackers with deep system control.

Strong security measures such as antivirus software, use utilities specifically designed to look for Rootkits, apply regular updates, and look for unusual or suspicious behavior is essential for protection.

Continued from page 1 *Unedited from FBI.gov*

The latest Online AI Scams

On December 3, 2024 the FBI issued Alert Number: I-120324-PSA which has the following warning:

The FBI is warning the public that criminals exploit generative ***Artificial Intelligence*** **(AI)** to commit fraud on a larger scale which increases the believably of their schemes.

Generative AI reduces the time and effort criminals must expend to deceive their targets.

Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information.

These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud.

The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion

Since it can be difficult to identify when content is ***AI-generated***, the **FBI** is providing the following examples of how criminals may use ***Generative AI*** in their fraud schemes to increase public recognition and scrutiny.

AI-Generated Text:

Criminals use AI-generated text to appear believable to a reader in of social engineering attacks, spear phishing, and financial fraud schemes such as romance, investment, and other confidence schemes, or to evade common fraud detection signs.

- **Criminals use *Generative AI*** to create countless fictitious social media profiles used to trick victims into sending money.
- **Criminals create messages** to send to victims faster allowing them to reach a wider audience with believable content.
- **Criminals use *Generative AI*** tools to assist with language translations to limit grammatical or spelling errors for foreign criminal actors targeting US victims.
- **Criminals generate malicious code** for websites involved in fraudulent cryptocurrency investments and other fraudulent investment schemes.
- **Criminals embed *AI-powered Chatbots*** in fraudulent websites to prompt victims to click on malicious links.

AI-Generated Images:

Criminals use *AI-generated images* to create believable social media confidence fraud, and investment fraud.

- **Criminals generate fraudulent identification documents,** such as fake driver's licenses or counterfeit credentials (*law enforcement, banking or government banking*) for identity fraud and impersonation schemes.
- **Criminals use *Generative AI*** to produce photos to share with victims to convince victims they are speaking to a real person.
- **Criminals use *Generative AI*** tools to create images of celebrities or social media personas promoting counterfeit products or non-delivery schemes.
- **Criminals use *Generative AI*** tools to create images of natural disaster or global conflict to elicit donations to fraudulent charities.
- **Criminals use *Generative AI*** tools to create images used in market manipulation schemes.
- **Criminals use *Generative AI*** tools to create pornographic photos of a victim to demand payment in *sextortion* schemes.

AI-Generated Audio, aka Vocal Cloning:

Criminals can use *AI-generated audio* to impersonate well-known, public figures or personal relations to elicit payments.

.• **Criminals generate short audio clips** containing a loved one's voice to impersonate a close relative in a crisis situation, asking for immediate financial assistance or demanding a ransom.

• **Criminals obtain access to bank accounts using *AI-generated audio clips*** of individuals and impersonating them.

AI-Generated Videos:

Criminals use *AI-generated videos* to create believable depictions of public figures to bolster their fraud schemes.

- **Criminals generate videos** for real time video chats with alleged company executives, impersonate law enforcement, or other authority figures.
- **Criminals create videos** for private communications to "prove" the online contact is a "real person."
- **Criminals use *Generative AI tools*** to create videos for fictitious or misleading promotional materials for investment fraud schemes.

Flicker:

In conclusion, Create a secret phrase with family for identity verification. Watch for image or video imperfections, listen carefully to phone calls, limit your online presence, verify callers directly, never share sensitive info or send money to strangers.

How Love Led To The Invention Of Cable TV

continued from page 1 *by Flicker*

***Ed Parsons* then worked for** the *Navy control plant* in *Portland,* which supported military operations and logistics, and provided his services to support the war effort, ensuring that essential equipment and facilities were maintained and operational.

While working at a local radio station, KGW-AM as an engineer , Ed Parsons heard that **KAST**, a news-paper owned broadcast station in *Astoria, Oregon* was losing money, and had petitioned the **FCC** to suspend operations during the war.

***Ed Parsons* talked to the Astoria Budget newspaper** about buying the radio station **KAST**. They hesitated, informing *Ed Parsons* they would rather just shut it down.

A few weeks later he found the newspaper was interested in selling him the station. He was able to leave his job as superintendent in the navy station.

Within 30 days he had the station back in the black, making money. ***Ed* said** "*the revenue shot up. Doing live newscasts was all it took to bring the station up to a profitable basis*".

After he bought the radio station he found out half the AM radio receivers in the town were inoperative.

Ed hired local ham radio operator, *Hano Ripola,* and set up a radio repair shop in the back of the radio station's studio.

When Hano would get caught up on repairs Ed would announce on the radio he had space available for more repairs. Ed said Hano had "*repaired, probably, thousands of sets*"

While at a broadcast convention in *Chicago* his wife saw a television demonstration in the basement of the hotel hosting the convention and on the way home she told him that she wanted a television.

He told her the only TV station that existed at that time was in *Chicago* and there was no station on the west coast where they lived, and that TV reception was physically impossible due to the great distance.

After they heard that Bob Priebe was going to build a TV station in *Portland, Oregon* Ed bought a 9" TV set from *Chicago*.

He bought it primarily because it was also a **HiFi set** with AM-FM radio and a record player.

In Ed's words, "*I told the wife we are wasting our money with the television addition, but at least I would try to get her television*"

When he found out that a TV station was going to be built in *Seattle, Washington*, where he lived, by radio station **KRSC** and his wife said "*Now I can have Television*".

KRSC-TV was the first television station in the Pacific Northwest and began broadcasting *November 25, 1948* on **VHF** channel 5.

Ed Parsons worked with Bob Priebe, manager of the **KRSC-TV Seattle** station; he arranged to be notified when they broadcast a carrier wave.

By going to different locations he found a good signal on top of the ***Astoria hotel*** located near the waterfront in downtown Seattle Washington.

Getting permission to mount an antenna on top of the ***Astoria hotel***, he picked up **KRSC** channel 5 and built a channel converter to change it to channel 2 for transmission across the street to his penthouse.

Ed parsons designed and built the channel 5 to channel 2 converters as well as amplifiers to boost the TV signal to make up for the signal loss in the coaxial cable the signals were run through.

He also designed the first Cable TV Splitter and the first broadband amplifier that amplified the whole range of TV channels.

In *Ed Parsons* words "*Well, I strung a cable from the top of the hotel roof over to the three-story building where my penthouse was, and we had the television set in our living room*".

Ed Parsons's penthouse was at the Seattle-Tacoma Hotel, which later became known as the *Pioneer Building* and was the first home to receive television signals via cable.

Ed designed and built a lot of the electronics needed himself such as the one which converted channel 5 to channel 2.

By this time too many people were coming into their penthouse apartment. *Ed Parsons* said "*People would drive for hundreds of miles to see television.*
We had gotten considerable publicity, as I will show you. And when people drove down from Portland or came from The Dalles or from Klamath Falls to see television, you couldn't tell them no".

So Ed approached the manager of the Astoria Hotel and said it would be a simple matter to run a cable down the elevator shaft.

The manager thought it was great idea so Ed ran the cable and installed it on the TV set in the lobby.

Very shortly the Hotel manager called and had the set removed because the hotel lobby was so full people could not get in to register.

Ed approached the owner of a local music store the next street over, Cliff Poole

Ed Parsons said "*So I approached Cliff Poole, who owned a music store the next street over, and suggested maybe he would like to have a set*".

Yes, he would and he would buy the set, figuring this was a good addition to a music store. So Cliff Poole was really the first customer for cable TV.

I sold him the wire and the necessary equipment and the output of this amplifier-converter gave an acceptable signal. I built the first splitter to split the signal. So he had this set in the music store.

The broadcast station was only on the air a few hours a day, usually starting in the evening for a few hours.

When Cliff closed the music store, he would put the TV set in the window. People would group around to see the television picture."

Ed connected a PA amplifier to the speaker of the TV set and put it out front of the store so people could hear the TV broadcasts when the music store was closed.

Very soon the police chief said, "*Ed, you've got to do something about that set down there at Cliff Poole's. People are blocking the street and we are just not going to stand for it. That's all there is to it*."

Ed asked the police chief for a suggestion of what he would do.

The police chief suggested that Ed put TV sets in the bars and run the cables along the same pathways as the telephone and power cables, which ran the whole length of the main downtown.

Ed Parsons : "*Well, we did that. We started out stringing wires across the streets as I mentioned. The city council looked askance to this type of business.*

As the cable system expanded we installed one amplifier on one side of the street where we had the cable, put another amplifier across the street, put an antenna on each side of the street, and transmitted the signal across the street, then ran house to house and covered a whole block.

The people had amplifiers in their attics and in their upstairs rooms. Each person supplied the power for the amplifier. We ended up covering practically the whole town with cable."

So that was how cable TV was invented. *Ed Parson's* desire to make his wife happy along with his excellent technical skills made this possible.

As an Cable TV installer in 1978 I was always facsinated by the story of Ed Parsons, never dreaming I would be writing about it.

Thank you for reading this article,
Flicker

continued from page 1

What is a Bot? A Zombie Computer?

by Flicker

In fact, any internet-connected device can be vulnerable, even unusual ones like a fish aquarium controller.

This was demonstrated in July 2017 when hackers breached the ***River City Casino's*** network through its smart fish tank controller, which was responsible for automated feeding, water quality monitoring, alerts, and other functions.

Devices compromised by bots are often called "**Zombie Computers**" or "**Zombies**"

A group of these infected devices is referred to as a **"Botnet"**. **Bots** can be programmed to carry out a wide range of functions and are used for both legitimate and malicious purposes.

Here are some of the different types of Internet Bots

Malicious Bots

Malicious Bots and Botnets are created with harmful intent.

Spam Distribution Bots send large volumes of unsolicited emails or post spam comments on forums and social media platforms, often promoting scams or phishing attempts.

Data Theft Bots harvest sensitive information such as financial data, login credentials, or personal details from compromised devices.

Account Takeover Bots use stolen usernames and passwords to gain unauthorized access to accounts across multiple platforms, taking advantage of users who reuse credentials

Cryptojacking Bots utilize the processing power of infected devices to mine cryptocurrencies without the owner's consent.

Social Media Manipulation Bots automate actions on social media, such as creating fake accounts, spreading misinformation, or amplifying specific content to influence public opinion.

Click Fraud Bots generate fake clicks on online ads to defraud advertisers, often leading to financial losses.

Remote Control Bots provide attackers with control over infected devices, allowing them to execute commands, install additional malware, or conduct surveillance.

Malware Spreading Bots use compromised devices to distribute other types of malware, further expanding the attacker's reach and control.

IoT Devices Bots target vulnerable **Internet of Things (IoT)** devices for various purposes, including launching attacks or creating a larger **Botnet**.

DDoS Attacks Bots overwhelm a target server, website, or network with traffic, rendering it inaccessible to legitimate users.

Useful Bots

Some Bots and Botnets are useful and make everyday life on the Internet easier.

Automated Task Bots are designed to perform tasks without human intervention. They can execute actions at a much faster rate and with greater precision compared to humans.

Web Crawler Bots are search engines which use web crawlers (also known as web spiders or web robots) to index web pages and gather information about websites. These bots follow links and collect data from websites to update search engine results.

Chatbots engage users in conversation on websites or messaging platforms. They can provide customer support, answer questions, or carry out simple tasks based on predefined rules or artificial intelligence algorithms.

Social Media Bots automate social media interactions. They can post content, like and share posts, follow or unfollow accounts, and engage with users. malicious versions can spread misinformation or amplify harmful messages.

E-commerce Bots malicious bots can automatically purchase limited-stock items for resale at inflated prices. An example is the **Sneaker Bots** used to buy limited-edition sneakers quickly, disrupting fair sales.

Data Collection Bots scrape data from websites for various purposes, such as market research or content aggregation. However, they can also be used to steal sensitive information.

Gaming Bots can automate gameplay, farm in-game resources, or perform repetitive tasks. Some bots are used to cheat, giving players an unfair advantage.

Utility Bots can provide useful services, like weather updates, news summaries, language translation, or math calculations, but they can also be misused to manipulate information.

IoT Bots manage and control **Internet of Things (IoT)** devices, allowing interaction with smart appliances and security systems.

Malicious IoT Bots can be part of botnets, such as those used in the Mirai botnet, which exploited poorly secured **IoT devices**.

In conclusion, Bots improve efficiency, but malicious ones threaten cybersecurity. Understanding their functions is crucial for protecting devices and ensuring online safety.

Continued from page 1

Zombie Ants

by Flicker

Once the ant(s) are infected by the fungal spores, the ***"Zombie Ant Fungus***" fungus begins attaching itself to muscle fibers and tissues throughout the ant's body.

Within two to three days after the infection the fungus begins to affect the ant's nervous system and begins releasing chemicals that controls the ant's behaviour.

A large proportion of these fungal cells will be connected, forming a network to control the host's behavior collectively.

This species specific parasite controls the behavior of the infected carpenter worker ants, compelling them to climb down to the forest floor, climb vegetation and clamp onto the underside of leaves or twigs with their mandibles to anchor themselves in place.

With the living "*Zombie Ant*" host ant is clamped down on a leaf, the fungus continues to grow. It weaves its way through the ant's body, through the abdomen and thorax, down the legs, and into its head.

Eventually, the fungus erupts from the ants' head, by way of a giant stalk, which then releases fungal spores into the air. These spores fall to the forest floor, ready to infect the next unfortunate ant victim that wanders by.

The whole process, from infection to the moment a giant spike erupts from the ants head to send out spores, takes around 10 days or so until the fungus consumes the ant from the inside and the ant dies.

Scientists have been studying this *Zombie Fungus* to try and figure out how it can control the behavior of ants.

At first, it was thought that the fungus attacked and took over the ants' brain.

It was more recently discovered that the ant's brain is the last part of the ant to be destroyed or taken over by the ***'Zombie Ant Fungus'!***

After taking over the ants' muscles and other parts of the ant's body, the brain is the last part of the ant to be destroyed. A high percentage of the cells in an infected ant-host are fungal cells turning the hapless victim into more fungus than ant.

It then uses the ant like a puppet, controlling the movement of the limbs and mouth, steering the ant towards the perfect place for the fungus to reproduce.

Normally behavior is controlled by the brain sending signals to the muscles, but the fungus appears to be controlling the ant-host's behavior like a puppet master controlling the ant's muscles to manipulate the host ant's mandibles and legs.

Manufacturers VIN Recall Search Tool

by Flicker

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.

VIN Locations:

www.nhtsa.gov/ recalls

January 24, 2025
Kia America is recalling more than 80,000 vehicles due to floor witing beneath the front passenger seat that can become damaged and prevent airbags and seat belts from deploying properly

January30, 2025
Chrysler is recalling certain *2016-2019 Ram 3500*, *Ram 1500*, *2016-2020 Ram 2500*, and *2016 Ram 3500 Cab Chassis* vehicles.

The right and left side curtain air bag inflators may rupture due to a manufacturing defect.

These are just two examples of the very serious nature of vehicle manufacturer recalls.

These recalls are almost always at no cost to the vehicle owner and can save lives and prevent uneccesary loss of life or accidents.

I urge you to look up your vehicles VIN number to keep you and others safe

Flickertronics sponsors our newspapers and our website at www.techsourcenews.com

Here are a few of our offerings that help sponsor our ad-free Tech Source News Website and News Papers

Flickertronics Managed Services

For Less Than The Price of a Cup of Coffee Per Day Per Computer You can Have Your Own 24x7x365 IT Department

24x7x365 Support included: Our live, real time technical support operators are available around 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 and 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 24x7 Support:

1. Computer user has a problem with a printer.
2. User calls one of Flickertronics' remote support operators, they remote in and resolve the problem in minutes and an emailed report to their supervisor. No Bill.

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 per hour.

For more information call Flicker's cell phone at (904)295-2224 or email flicker@flickertronics.com

Computer Repair Services

Flickertronics - 1550 US Highway 1 S, St Augustine, FL 32084

Our Computer Repair Depot offers walk-in sales and service as well as mail order computer repair

We have provided computer repair services for over 22 years.

Our Walk-in Repair services include:
- Computer Repair
- Computer Sales
- New Computer Setup
- Data Recovery
- Virus and Spyware Removal
- Computer Hardware Upgrade
- Software Upgrades Installation
- Operating System Updates
- PC Memory Upgrades
- Optimize your PC
- Fix Internet connectivity issues
- Repair and secure hacked PC's

Flickertronics has been repairing computers for 27 years.

Broadband Cable - VoIP - Fiber Internet

We Find the Best Enterprise-Class VoIP Providers and Internet Service Providers at the Best Rates in Your Area Nationwide!

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 24x7x365 *Concierge Support* and On-Site Service for carrier *Internet* or *Telecom* issues from pre-quote, and before, during, and after installation.

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***, ***Starlink*** *as well as* ***DirecTV For Business***, *along with* ***RackSpace***, who are among some of our partners, these partners are serving our local area.

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

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 postitions with all 75+ providers.

We also provide VoIP phone service only from Enterprise Class Carriers with recognized names - avoid VoIP resellers with their "Own" brand.

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