CSU Connection November 2023

You take care of running your business, we'll take care of your technology.

Watch Out for Ransomware Pretending To Be a Windows Update!

Imagine you're working away on your PC and see a Windows update prompt. Instead of ignoring it, you take action. But when you install what you think is a legitimate update, you're infected with ransomware.

Cybercriminals are constantly devising new ways to infiltrate systems. They encrypt valuable data, leaving victims with difficult choices.

One such variant that has emerged recently is the **"Big Head" ransomware.**

"Big Head Ransomware Deception":

Big Head ransomware presents victims with a convincing and fake Windows update alert.

Attackers design this fake alert to trick users. They think that their computer is undergoing a legitimate Windows update. The message may appear in a pop-up window or as a notification.

The deception goes even further. The ransomware uses a forged Microsoft digital signature. The attack fools the victim into thinking it's a legitimate Windows update. They then unknowingly download and execute the ransomware onto their sytem.

From there, the ransomware proceeds to encrypt the victim's files, and victims see a message demanding a ransom payment in exchange for the decryption key.

This is not okay!

Here are some strategies to safeguard yourself from ransomware attacks like Big Head:

Keep Software and Systems Updated
Big Head ransomware leverages the appearance of Windows updates. One way to be sure you're installing a real update is to automate.

Verify the Authenticity of Update
Genuine Windows updates will come directly from Microsoft's official website or through your IT service provider or Windows Update settings.

Backup Your Data
Regularly back up your important files. Use an external storage device or a secure cloud backup service. Backups of your data can allow you to restore your files without paying a ransom.

Use Robust Security Software
Install reputable antivirus and anti-malware software on your computer.

Educate Yourself and Others
Stay informed about the latest ransomware threats and tactics. Educate yourself and your colleagues or family members.

Use Email Security Measures
Put in place robust email security measures. Be cautious about opening email attachments or clicking on links.

Enable Firewall and Network Security
Activate your computer's firewall. Use network security solutions to prevent unauthorized access to your network and devices.

Disable Auto-Run Features
Configure your computer to disable auto-run functionality for external drives.

Be Wary of Pop-Up Alerts
Exercise caution when encountering pop-up alerts especially those that ask you to download or install software. Verify the legitimacy of such alerts before taking any action.

Keep an Eye on Your System
Keep an eye on your computer's performance and any unusual activity. If you notice anything suspicious, investigate immediately.

Have a Response Plan
In the unfortunate event of a ransomware attack, have a response plan in place. Know how to disconnect from the network. Report the incident to your IT department or a cybersecurity professional. Avoid paying the ransom if possible.

How To Stay Safe on Social Media: A Series

Part 7: WhatsApp

WhatsApp allows users to send texts and voice recordings, make video and voice calls, share documents and more.

Although we don't consider it a "business" app, we know that a lot of people use it, so we need to keep you and your data safe!

WhatsApp has made a change to their policy which allows them to share iformation with their other company-owned applications. (Meta owns Facebook, YouTube, and Instagram). This includes information like your cell phone number, status updates, profile pictures, locations and messaging activity depending on your settings. According to the privacy policy, messages remain encrypted and should not be accessed by other applications.

WhatsApp scams include **Family Emergency scams, Kidnapping scams, Account Takeover scams, Government Impersonator scams, Giveaway scams, Cryptocurrency scams, and Online Romance scams** to name some of the more prevalent. They will ask you to take immediate action, may include grammatical errors, come from unknown phone numbers, say you've won a random giveaway, include unfamiliar links, and may be sent from unusually long phone numbers. Before you do anything, verify the legitimacy of the request. Contact the person or company directly. Don't share any account or private information. **Block any suspicious accounts.**

Sources and additional information:

•**How To Avoid WhatsApp Scams** (https://money.com/how-to-avoid-whatsapp-scams/)

•**WhatsApp accessing microphone on Google Pixel 7, Galaxy S23 even when not in use**: reports (https://insiderpaper.com/whatsapp-using-microphone-on-google-pixel-7-galaxy-s23-even-when-not-in-use/

Gadget of the Month:

TickTime Cube

The Ticktime cube is a digital countdown timer that's **as easy to use as a light switch.** It's a stylish, user-friendly gadget that helps you **manage your time** to help boost your **efficiency and productivity.** It's perfect for any tasks that needs a timer. It also comes in a variety of cool colors to **match your style or mood!**

Get yours at: ***https://www.ticktime.store/***

Keep Your Smart Home from Turning Against You

Smart homes offer unparalleled convenience and efficiency.

But as we embrace the convenience, it's essential to consider the potential risks.

Recent headlines have shed light on the vulnerabilities of smart home technology. Such as the story in the New York Post's article titled: "Locked Out & Hacked: When Smart Homes Turn on Owners."

The article describes smart home nightmares. Including the new owner of a smart home that unexpectedly got locked in. The prior owner had left pre-programmed settings. Suddenly at 11:30 p.m., the home told him it was time to go to bed and locked every door in the house.

Another technology victim was a woman terrorized by lights and sounds at home. Her ex-partner was maliciously manipulating the smart technology.

As homes get smarter, how can you avoid a similar experience?

We'll explore some key strategies to protect your home and your privacy.

(continued on page 5)

Smart Home Safety Tips You Need to Use

1. Secure Your Network –

The foundation of any smart home is its network. Just as you wouldn't leave your front door wide open, you shouldn't neglect Wi-Fi security.

2. Strengthen Device Passwords –

Avoid using easily guessable information like "123456" or "password." Use a combination of upper and lower-case letters, numbers, and symbols.

3. Enable Two-Factor Authentication (2FA) –

Many smart home device manufacturers offer 2FA as an extra layer of security. This helps keep unwanted people out.

4. Regularly Update Firmware –

Firmware updates are essential for fixing security vulnerabilities in your smart devices. Make it a habit to check and apply firmware updates regularly.

5. Vet Your Devices –

Look for products that have a history of prompt updates and robust security features. Avoid purchasing devices from obscure or untrusted brands.

6. Isolate Sensitive Devices –

Consider segregating your most sensitive devices onto a separate network, if possible.

7. Review App Permissions –

Smart home apps often request access to various permissions on your devices. Before granting these, scrutinize what data the app is trying to access.

8. Be Cautious with Voice Assistants –

Review your voice assistant's privacy settings. Be cautious about what information you share with them.

9. Check Your Devices Regularly –

Regularly check the status and activity of your smart devices. Look for any unusual behavior.

10. Understand Your Device's Data Usage –

Review your smart device's privacy policy. Understand how it uses your data.

11. Stay Informed –

Finally, stay informed about the latest developments in smart home security. Subscribe to security newsletters.

What's Up With The CSU Team?

Can someone say "Paint Pour and Pizza Party" 10 times fast?!

Pour Paint PARTY
Julia Bay
(405) 420-1430 | pourpaintparty.com

Thanks to the talented Ms. Julia who founded and personally hosts Pour Paint Party, everyone was able to showcase their creative side!

Plan your party today! There are more than just pumpkins to paint.

Studious CSU staff

There's nothing like celebrating the season with some arts and crafts. The CSU team painted their own pumpkins. Check it out.

Having fun!

Would you have guessed everyone chose the colors they did? Mike's wife, Jami, guessed 4/8 on our Facebook competition. Alyssa called them all...

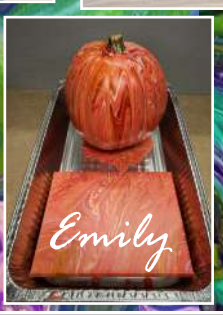
No breaks for Chuck!

Melvin

Michelle

Nina

Mike



Emily

Wanda

Heath

Chuck

Walking down the aisle as a proud father! Congratulations to Mike's daughter, Zoe!

Happy "Born Day" Wanda!

Birthday Time!

Happy Birthday month to Emily!!!

#borninnovember

Happy Birthday AND 3 year anniversary to our witty, talented tech, Will!!!!

No problem is too hard to be solved with this guy. CSU wouldn't be the same without you.

Stay connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Version of Newsletter:
www.csuinc.com/news

Our Services:

- -Data Backup & Recovery
- -Managed Services
- -IT Consulting
- -Network Security
- -Cloud Computing
- -Remote IT Services
- -Cyber Security Training
- -Mobile Device Management

We believe that experienced, reputable and fast responding IT support should be the standard.

CSU COMPUTER SERVICES UNLIMITED

Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity, and profitability.

CSU Connection November 2023

You take care of running your business, we'll take care of your technology.

in this issue...