

Sun City Computer Club

Cyber Security SIG

February 2, 2023

**Questions, Comments, Suggestions welcomed at
any time**

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

**SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law**

Apology & Welcome

S

Security Updates Firefox & Android 1-Feb-2023

Published • Feb 1

A

Apple Updates Today January 23, 2023

Published • Jan 23

T

T-Mobile Yet Another Data Breach

Published • Jan 19

F

Firefox browser Update 18-Jan-2023

Published • Jan 18

L

LastPass Customer Cloud Based Password Vaults Breach

Published • Dec 23, 2022

Cyber Security News Archive

- Computing environment changed
- Process, not a procedure
- You are the Problem You are the remedy
- Awareness, Preparedness, Understanding
- Computer Club resources
- Help Center, SIG presentations, Seminars
- Searchable:
 - Cyber Security News Archive
 - SIGs soon MUG
 - Cyber Security SIG Announcements
 - SCTX Computer Club Facebook

Safer

- Top 10
 - Passphrases and MFA
 - Strong network – WiFi settings, Firewall & filtering, MONITORING
 - Firewalls + Firewalls Facing both ways
 - Think, Pause, THINK, consider sandbox, IFF click
 - Slowdown Share
 - Setup Alerts
 - Awareness, Preparedness, Understanding
 - Disable macros
 - Paranoia, suspicious, FOMO
 - DNS
 - Administrator
 - eMail Images off
 - Multiple
 - ChromeOS Chromebook

Top 10 - Well I can't count

CYBER SECURITY

[My Profile](#)

[Account Statements](#)

[Resident Directory](#)

[My Neighborhood](#)

[My Memberships](#)

ANNOUNCEMENTS

- [Security Updates Firefox & Android](#)

Cyber Security SIG Announcements

[Securing Android Devices](#)

[Big Sur](#)

[ChromeOS Chromebooks](#)

[Cutting the Cord Alternatives to deliver video/audio content](#)

[Sun City Computer Club WEB site navigation and information](#)

[Computer Club Web Site Navigation - Update](#)

[Crypto Currencies](#)

[Cyber Warfare Part 1](#)

[Cyber Warfare Part 2](#)

[Files and Folders Generic](#)

[First Time SIG Safer Computing](#)

[Linux - What is it anyway?](#)

[Apple MacOS Monterey Release Notes and News](#)

[Apple MacOS Monterey preview](#)

[Safer WEB Browsing Class](#)

[Safer WEB Browsing Part one](#)

[Safer WEB Browsing Part two](#)

[Securing a Home Network September 2020](#)

[Semiconductor Chips](#)

[Social Media](#)

[Microsoft Defender](#)

[Sun City MAC Users Group MUG Securing your MAC](#)

- LastPass cloud based
- KeePass local storage based
- CVE-2023-24055

Write access to local storage

Modify KeePass XML configuration file

Export data to unencrypted file

Background process

Password Managers

- Windows Pro Insider Preview 25276
SMB insecure Guest authorization
Off by default
- GitLab releases 15.7.5, 15.6.6, 15.5.9
Git source code version control system
Exploits to achieve Remote Code Execution
- UK Royal Mail recovery
- NSA Security manual IPv6
- T-Mobile breach disclosure filed with SEC
November 2022 – Discovered Jan 5, 2023
8th breach in 5 years
Your info on T-Mobile home Internet wait list?

Current Issues



T-Mobile
Prices will
NEVER INCREASE.
DATA WILL ALWAYS LEAK.

Silent AirTag

🔊 x Speaker Disabled



Silent AirTag

4000 years later and we're back to the same language... 🤔 😂



- Computer system that you watch for TV
Got camera? Tape over check Working?

Tracking

Automatic Content Recognition (ACR)

Unique pattern of pixels => specific content

ANY content DVD, streamers, cable, WiFi, ...

Creepy? Helpful <-> Harmful?

Smart TV

- **Vizio** System > Reset & Admin > Smart Interactivity
> Reset & Admin > Viewing Data
- **Samsung** Smart Hub Menu > Settings > Support Terms & Policy > SyncPlus and Marketing
Settings > Support > Terms & Policy
Viewing Information Services
- **LG** Settings > All Settings > General > LivePlus
Settings > All Settings > General >
About This TV > User Agreements
Personal Advertising

Smart TV

- Check any/all privacy settings
- Disable voice control?
- Free Apps & Channels?

Smart TV

- Amazon Fire On TV App
Settings > Preferences > Right to Privacy
Collect App and Over-the-Air Usage Data
Internet-based ads
- Roku
Settings > Privacy > Smart TV Experience
Use Information for TV Inputs
Settings > Privacy > Advertising
Limit ad tracking
Still collects data of Roku channels

Streamers

- Many and many more to add Samba TV
 - Knows what is viewed regardless of source
 - Can communicate with other devices
 - Tag web site – view after viewing TV ad
 - Samba “Interact with your favorite shows. Get recommendations based on the content you love. Connect your devices for exclusive content and special offers,”

Samba



Real



NVIDIA Broadcast

AI Eye Contact



Red Key



License Plate Flipper

- Android app

Attempt to connect to Wi-Fi network
it is connected to
with a list of Wi-Fi admin credentials
when successful – change DNS server
settings

Can now steer real sites to fake sites

Roaming Mantis

- Transaction Record Analysis Center
150 million money transfers
between US and 20 other countries
non-profit
hundreds of U.S. law enforcement agencies
Arizona attorney general's office
settlement with Western Union 2014
knowledge due to Senate investigation
ACLU
"one of the largest government surveillance
programs in recent history."

TRAC

- U.S. airline *CommuteAir*
Left exposed U.S. No Fly List
1.5 million names
And company data employees, etc.
- T-Mobile data stolen by API?
30+ million
name, email, address, DoB, phone number,
account number, ...
Australian Optus breach follow on
- Google Fi Customer data breach
Mobile Virtual Network Operator MVNO

Current Events

- SweepWizard ODIN Intelligence
Hacked, data exfiltrated, backups deleted
Data provided to DDoSecrets
Facial recognition scans, ALPR license plate tracking
- Data Ukraine cyber tactics & kinetic actions what we can learn
- UK Royal mail – lack of detail Why?
- Greek Watergate
Nation state level spyware Predator
EU & Greek data protection agency
Fined Intellexa for investigation delay

Current Events

- Israeli spyware sold to Myanmar
Hack telco
Listen in on calls, view text, read email, etc.
Supreme court ruling “Stop” with gag order
Then a military coup
- iOS 16.3 iCloud Advanced Data Protection
worldwide
HomePod issues?
Got Old?
- Yum Brands
KFC, Pizza Hut, Taco Bell
Ransomware 300 restaurants closed
- Guacamaya hackers exposing data
to counter corruption
- <https://www.cnet.com/personal-finance/paypal-breach-what-do-i-do-if-someone-stole-my-social-security-number/>

Current Events

- Moving toward more ads
- More ads – more targeting - more data
- Privacy policy - adjust
- Privacy policies per product 80 or so
- Required data - account
- Data to improve crash data, resource use
- Data processed on device
- Data to improve
 - Health & fitness – more accurate
- Game center – from your device

Apple

- Apple Maps
 - Limited to an identifier that rotates multiple times per hour
 - Identifier Not linked to Apple ID
 - Precise locations -> less-exact data 24 hrs
- Ads expanded for News, Stocks & Apple TV
- First Party
- Apple App Store Locked in Suits
- Siri Generated transcripts sent to Apple
 - Not associated with Apple ID
 - Used to improve
- Apple Search? \$8-12B/year Alphabet
- Apple layoffs - No CEO salary cut 40%

Apple

- iOS

Settings > Privacy & Security > Apple Advertising > Personalized Ads

- macOS

Settings > Privacy & Security > Apple Advertising > Personalized Ads

- OR

View Ad Targeting Information

Privacy & Security

Analytics and Improvements

Apple Opt Out or In

OP

Explain an SSL certificate chain like a stoned surfer bro



Dude, an SSL certificate chain is like this gnarly wave of trust, bro. You got your main certificate, that's like the big Kahuna, the main dude. And then you got all these other little certificates, like tributaries, that all flow together to create this one big wave of trust. And it's all verified by this dude called a certificate authority, he's like the lifeguard of the internet, making sure everything is kosher and legit. And when you surf a website, it's like you're catching that wave, and it's like you know you're in a safe spot, no sharks or anything, just pure shredding.

- Office disables macros by default
- SO increased use of LNK files
- Metadata about target file
 - Application, system, target attributes
- Security bypass

Increased use of LNK

- GoTo is a commercial service that allows collaboration via remote desktop app.
- Like its affiliate LastPass, the company disclosed by an email to current customers that it too had been breached and customer information had been breached.
- Customers may find their passwords reset.

GoTo (LogMeIn)

Our investigation to date has determined that a threat actor exfiltrated encrypted backups from a third-party cloud storage service related to the following products: Central, Pro, join.me, Hamachi, and RemotelyAnywhere.

We also have evidence that a threat actor exfiltrated an encryption key for a portion of the encrypted backups.

The affected information, which varies by product, may include account usernames, salted and hashed passwords, a portion of Multi-Factor Authentication (MFA) settings, as well as some product settings and licensing information. In addition, while Rescue and GoToMyPC encrypted databases were not exfiltrated, MFA settings of a small subset of their customers were impacted.

GoTo

Security Incident Update and Actions to Take

PS

To: [REDACTED]

Reply

Reply All

Forward

Mon 23/01/2023

You forwarded this message on 23/01/2023 22:28.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Customer,

I am writing to update you on our ongoing investigation about the security incident we told you about in [November 2022](#).

Our investigation to date has determined that a threat actor exfiltrated encrypted backups related to Central and Pro from a third-party cloud storage facility. In addition, we have evidence that a threat actor also exfiltrated an encryption key for a portion of the encrypted data. However, as part of our security protocols, we salt and hash Central and Pro account passwords. This provides an additional layer of security within the encrypted backups.

Recommended Actions

Out of an abundance of caution, we are resetting your Central or Pro password. If you use Multi-Factor Authentication to sign into your account, you may be prompted to update your Multi-Factor Authentication settings during this process.

As an additional step to protect you, your account will automatically be migrated to GoTo's enhanced Identity Management Platform as part of your password reset. This platform provides additional security for your users with more robust authentication and login-based security options, including enhanced controls, stronger password requirements, and a Single Sign-On option to access multiple GoTo (formerly LogMeIn) products. Note: all users who have reset their password since December 12 have already migrated to the new platform and do not need to take this action. Additional guidance can be found here for [Central](#) and [Pro](#).

What information was affected

The information in the affected backups include your Central and Pro account usernames and salted and hashed passwords. It also includes your deployment and provisioning information, One-To-Many scripts (Central only), some Multi-Factor Authentication information, licensing and purchasing data such as user emails, phone numbers, billing addresses, and the last four digits of credit card numbers (we do not store full credit card or bank details).

Based on our investigation to date, we continue to believe that the threat actor did not have access to GoTo's production systems. Furthermore, Central and Pro's peer-to-peer technology and end-to-end encryption provide security against interception and eavesdropping of data transferred during remote sessions. Your session data in transit is always protected by Transport Layer Security (TLS) 1.2.

While the investigation is ongoing, we wanted to provide this important update to you, and recommend clear and actionable steps in response to what we have learned. We are committed to protecting you, your information, and the security of our products and will continue to update you. If you have any additional questions, please contact [customer support](#).

Paddy Srinivasan
CEO, GoTo (formerly LogMeIn)

- Williamson County Property Fraud Alert
<https://www.wilco.org/Elected-Officials/Clerks/County-Clerk/Fraud-Alert-System-Sign-Up>
- ChatGPT in the news again and again
Varied ways around safeguards
Criminal use – no surprise
Using ChatGPT less skilled actors
Encryptors, File harvesters, Marketplace
- Fox ad for NFL plays Emergency Alert System
tone \$504,000
- Google removes 50,000 accounts pushing
Chinese disinformation

Current Issues

- Sandworm attack Ukraine Windows Wiper
- 4chan members used ElevenLabs to make deepfake voices of Emma Watson, Joe Rogan, and others saying racist, transphobic, and violent things.
- Madison Square Garden blocking ticket holders
Based on facial recognition
- Microsoft to block downloaded XLL files
Mark of the WEB MOTW
Malware increased use of zip or encrypted archive

Current Issues

- iOS 16.3 iPadOS 16.3 Ventura 13.2
Third Party FIDO keys for AppleID
- Yet another scan the citizenry Poland
- FBI hacked Hive ransomware gang
Distributed decryption keys
Seized ransomware payments
- Russia blocks internal addresses to:
FBI, CIA, US State Department's Reward for
Justice program \$10M reward
- Meta (Facebook, Instagram, etc.)
Disable users MFA if phone number known

Current Issues



Social Security

Date : 06th January, 2023

Case ID : [REDACTED]

Attention :-

This is to inform you that, due to fraudulent activities of your Social Security Number (SSN) will be suspended in the next 24 hours.

We are writing to you to inform that your social security number is being suspended because FTC has found some criminal activities going on in the state of TEXAS by your name.

Your case is referred to the Department of Justice TX & Office of Court Administration to consider for prosecution under the Criminal Code Act 1956, and other criminal offence in the state of TX, including the Proceeds of Crime Act 2002 for:

1. Count 1 (Drug Trafficking Act 258 Section D)
2. Count 2 (Money Laundering) "" Act of 1998
3. Count 3 (Theft by deception) Texas Supreme Court Code conduct 1988

As of now we have received a legal allegation against your name for Identity Theft because - As per our standard procedures, law enforcement agencies have found 5 stolen bank accounts opened using your Social Security number to commit a fraud of approximately \$14 million. These accounts were used in numerous criminal activities like Money laundering, Drug trafficking and Internal Revenue Service (IRS) scams all over the state of New Mexico.

To plead yourself, you can contact the Department of Office General (Social Security Administration) at 1 (800) 591 9425.



- European date format
- No Name

Attention:-

SSN Scam

From: Todd Ednie <bhfdghff7555@gmail.com>

Sent: Tuesday, January 31, 2023 6:18 AM

To: [REDACTED]

Subject: #charges deducted update_22

Dear [REDACTED]

We are happy to inform you that your service plan has been renewed.
Your plan has been paid via using your credit card.

If you have any question about this service or the product details.

Please find your billing details mention below:-

Product: #Norton_360

Product Type: Advance

Invoice No: DHS4234979-845/943K

Invoice Date: Jan 31, 2023

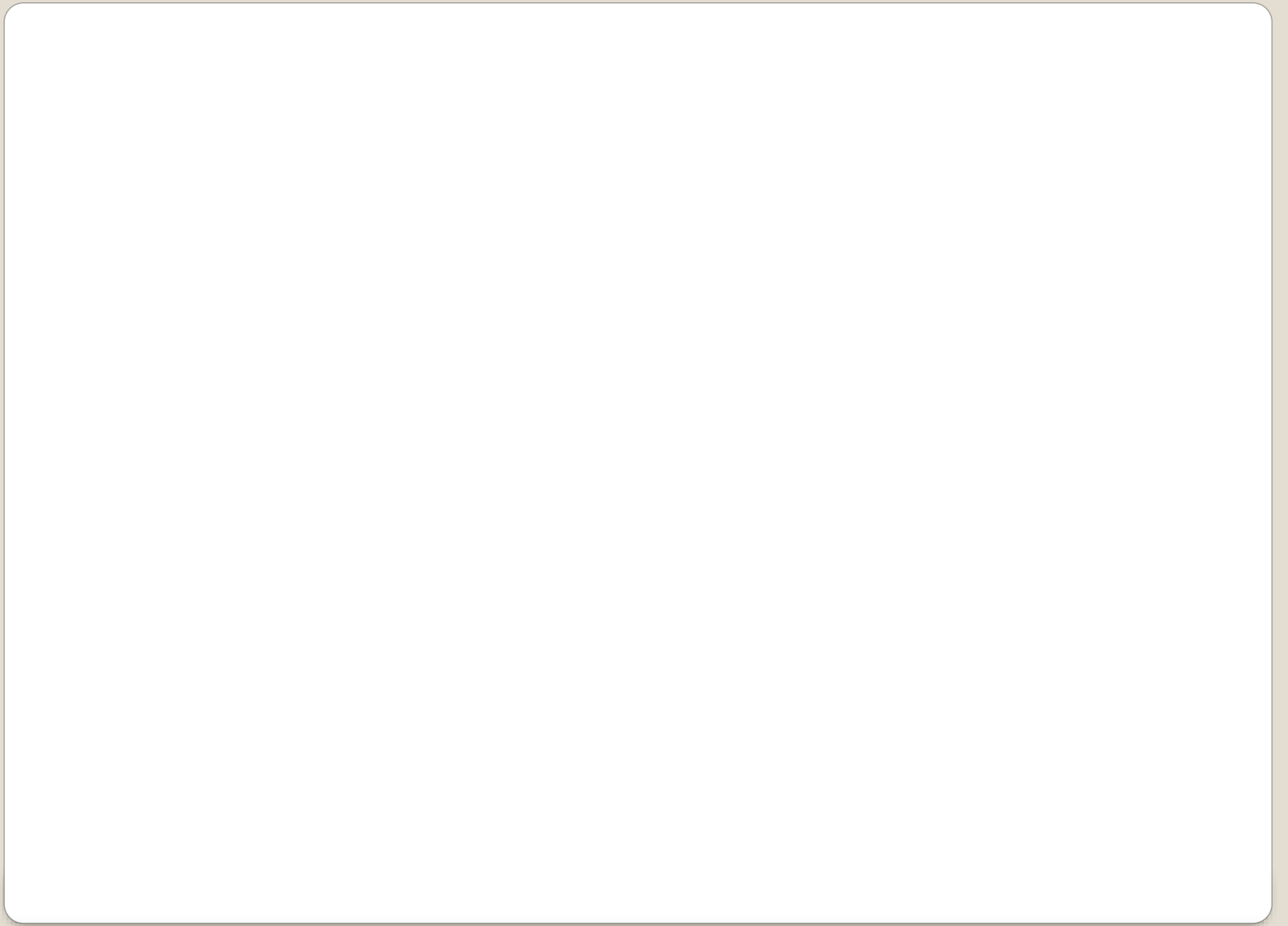
Amount: USD \$356.69

Payment method: Auto-Debit

**If you have any issues with this purchase or have any queries related to the product, then please get in touch with us,
Support Team @ +1 (866) 306-6643... Toll Free**

Regards

Billing_Team.



- What, me worry?
- Vast effort to collect, build profile, sell
- Get caught? Pay fine Fine

- Privacy MANAGEMENT
Settings, settings, settings
Audit and remove old apps
Just say "no"
clicking thru permissions

Privacy

- Used to be Madison Avenue
- Now Facebook & social media engines
- Signal attempt to warn

You got this ad because you're a newlywed pilates instructor and you're cartoon crazy.

This ad used your location to see you're in La Jolla.

You're into parenting blogs and thinking about LGBTQ adoption.



You got this ad because you're a certified public accountant in an open relationship.

This ad used your location to see you're in South Atlanta.

You're into natural skin care and you've supported Cardi B since day one.



You got this ad because you're a Goth barista and you're single.

This ad used your location to see you're in Clinton Hill.

And you're either vegan or lactose intolerant and you're really feeling that yoga lately.



Privacy

- Ad blockers
- No third-party cookies
- Less tracking Less resources

165,140

Trackers & ads blocked

4.20 GB

Bandwidth saved

2.3 hours

Time saved

- Phone number collections
1-800, application for credit, ...
- Oversharing on social media
- Online quiz and/or survey
- Impersonating business you work with

Privacy

- Taken over while you sleep, DND, offline
- You have MFA via SMS
- Attacker attempts WhatsApp
WhatsApp sends PIN to via SMS
You sleep
Attacker tells WhatsApp “didn’t get it”
WhatsApp calls your number
You sleep, call goes to voice mail
Attacker calls you
You sleep
Attacker uses last 4 digits as voice mail
access
Attacker changes MFA

WhatsApp

- Change default PIN for voicemail
- Enable MFA
- Enable 6 digit PIN at WhatsApp
- Provide one of your emails for reclaiming your WhatsApp account

WhatsApp defenses

- Bitwarden acquires Passwordless.dev
<https://bitwarden.com/password-strength/>

- Credential stuffing
Collection #1-5 22 billion credentials
Bot fleets

Detection <<<<< attempts

- Samsung Galaxy system shell access
- US agencies get RMM not just us
- Lexmark Printers security firmware update
Severe RCE bug 100 models
- Bitwarden Hash Iteration counts
LastPass
- Cyber crime third largest economy \$8 Trillion 2023

Current Issues

- Bitwarden Hash Iteration counts
LastPass
Cloud based password managers
Recent increase of password managers to
battle credential stuffing
Bitward – Password Manager
Google search Ad

Bitwarden

- Place Wi-Fi router in central location
- Create strong Wi-Fi network password & change often
- Change default router login credentials
- Turn on firewall and Wi-Fi encryption
- Create/use Guest network
- Use VPN
- Keep router & devices up to date
- Disable remote router access
- Verify connected devices
- Upgrade to WPA3 router

CNET 10 ways to avoid home network hackers

Gallons



- Avoid prolonged breathing of vapors.
 - Keep face, eyes and skin away from nozzle while refueling.
 - Never siphon by mouth.
 - For use as a motor fuel only.
- Self Serve**
- Don't overfill or "top-off" tank.
 - Personnel using dispensers with hold-open latches must remain at the fueling point (outside and next to the vehicle) during refueling.
 - Never jam open the hold-open latch.
- In Case of Fire**
- **DO NOT REMOVE NOZZLE FROM THE VEHICLE.**
 - Evacuate all passengers from the vehicle and refueling area.
 - Activate Emergency Shutoff Switch.
 - Notify attendant.
 - Call 911, if no attendant is on site.

 Vehicle refueling services will be provided upon request to motorists with disabilities if the vehicle displays an official state or locally issued disabled motorist plate or placard.

Refueling service **CANNOT** be provided when there is only one employee on duty or if it is not safe to do so.

To obtain refueling service, back your car here three times. We may use the intercom, if available, for this purpose.

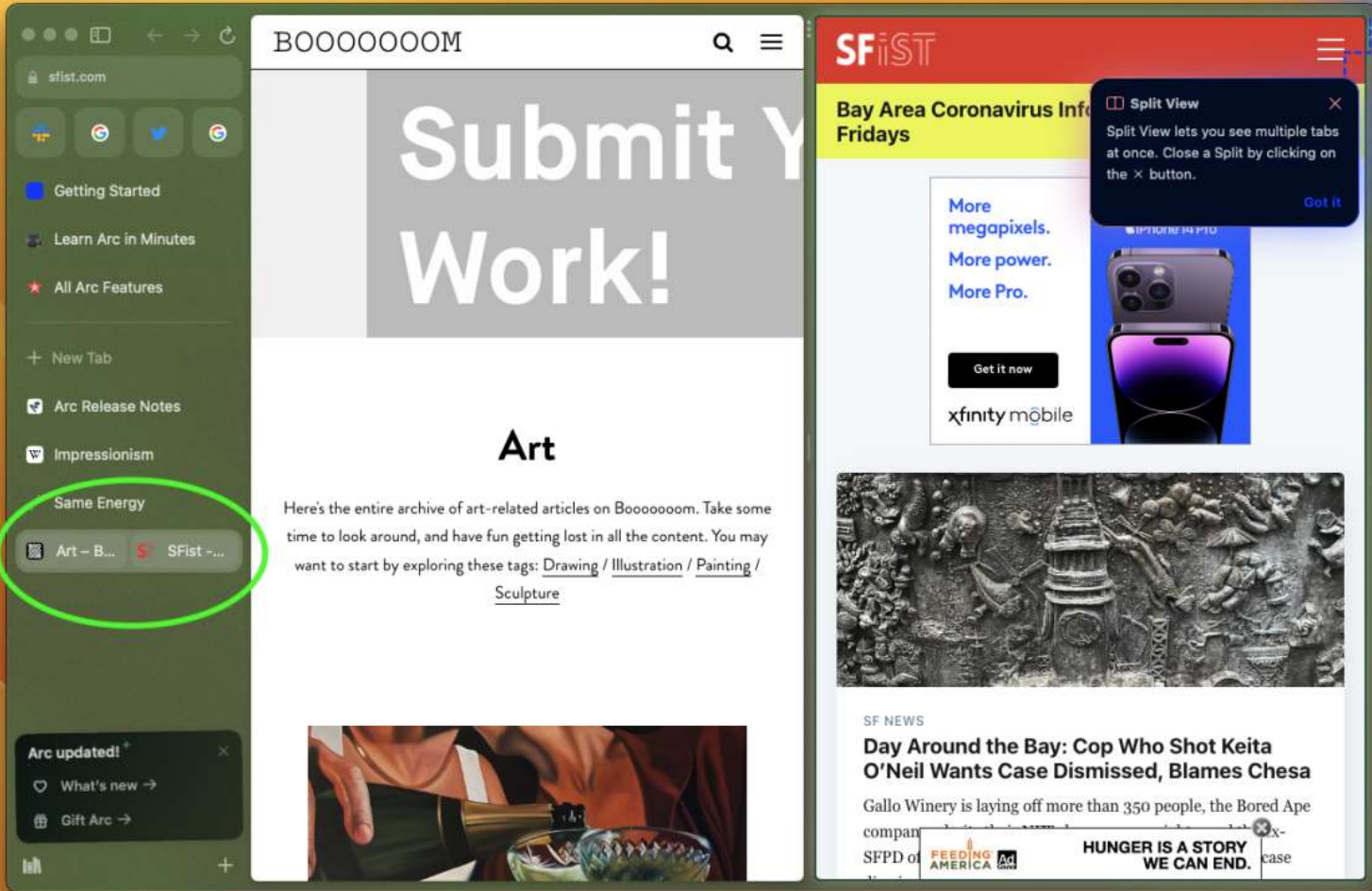


Mute

- Yet another “Save as” format
- Chrome default format



Chrome WebP format




Arc browser

The staff member was unable to open the attachment and asked for help from a Baltimore County Schools tech liaison, according to the report. The school system's tech liaison thought the email was suspicious, according to the report, and sent the email to the school system's security contractor.

According to the report, the security contractor opened the email attachment on their unsecured county school system email account instead of their secure email system. That act delivered the malware into the school system's computer network, according to the report.

And so IT goes

8:11 PM

he died in an accident I think
you know him I'm so sorry... 

<https://> 


ChromeOS Chromebook

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs,
Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com