Sun City Computer Club

Cyber Security SIG

June 2, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

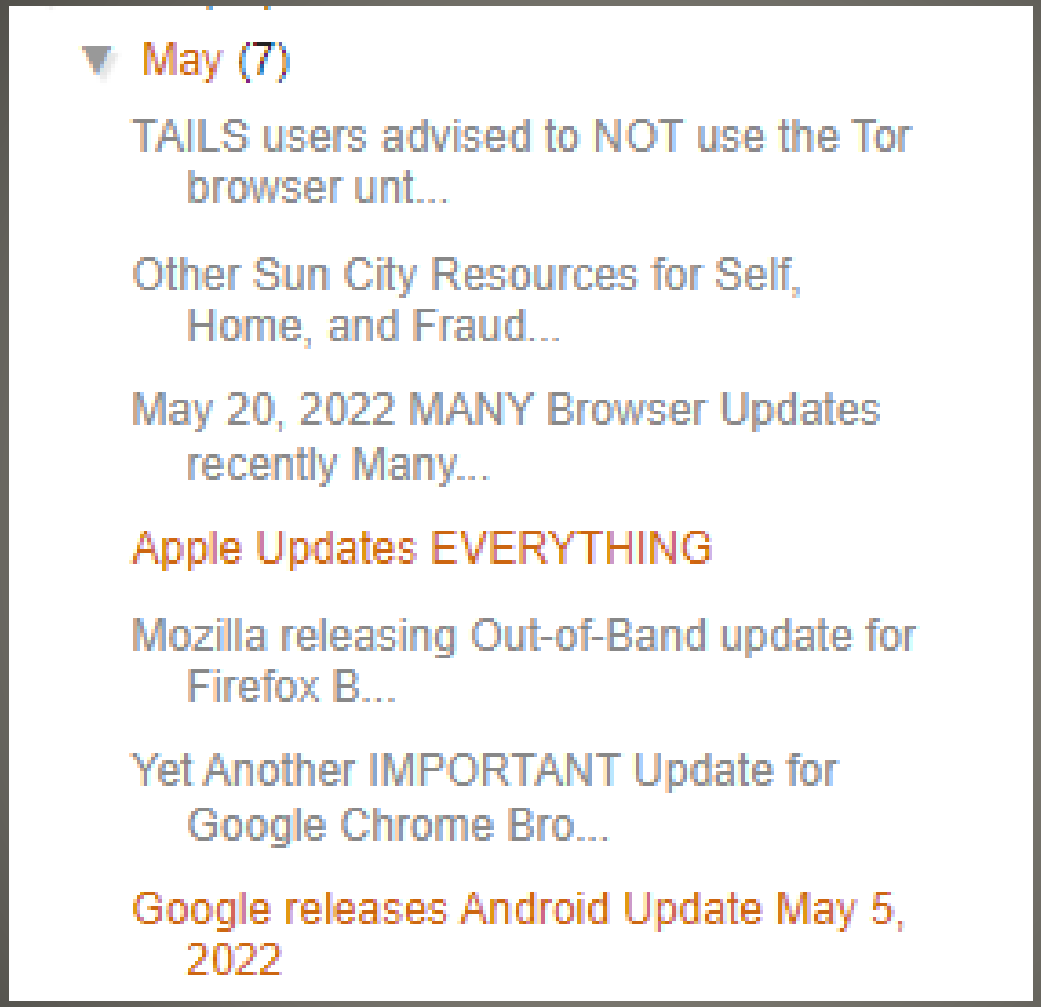
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

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

- Ever want to be a presenter??

Presenter???



News Blog May entries

Securing Android Devices
Big Sur
Sun City Computer Club WEB site navigation and information
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
Sun City MAC Users Group MUG Securing your MAC

No New Seminars Brave

Current Issues

- Texas AG sues Google - Incognito mode
- Streaming services Authentication sites
- Bluetooth Low Energy protocol vulnerability
  - Bluetooth developer board
  - Exploit code
- Tesla, smart locks, laptop w/ proximity


HOME TITLE FRAUD
IS THE IDENTITY THEFT YOU
NEED TO BE WORRIED ABOUT
AND IT'S GROWING
2.5X
FASTER
THAN
CREDIT CARD FRAUD
- BASED ON 2017-2021 FBI INTERNET CRIME REPORTS,
WHICH INCLUDE OTHER REAL ESTATE RELATED CRIMES.

- Digital real estate transactions
- Attack the trust (sic)
- Monitor is one thing, block is yet another
- Deed & titles are legally protected

- NSA & FBI please don’t list

- Multifactor authentication (MFA) is not enforced.
- Incorrectly applied privileges or permissions and errors within access control lists.
- Software is not up to date.
- Use of vendor-supplied default configurations or default login usernames and passwords.
- Remote services, such as VPNs, lack sufficient controls to prevent unauthorized access.
- Strong password policies are not implemented.
- Cloud services are unprotected.
- Open ports and misconfigured services are exposed to the internet.
- Failure to detect or block phishing attempts.
- Poor endpoint detection and response.

BILL DETAILS - #VAA1654106945N OM Inbox ×

Dreinkolp Mrrejinot <dreinkolpmrrejinot28jss@gmail.com>
to nortoncc1.2022, bcc: me

Thank you for your order, Here is your details

INVOICE NUMBER

VAA1654106945NOM

Product Details

NORTON PROTECTION

Order Summary

INVOICE NUMBER: VAA1654106945NOM
START DATE: 2022.06.01
End Date: 1 year from START DATE
Payment Mode: Auto debit from account
Status: Completed

ITEM NAME	Quantity	Total
NORTON PROTECTION (VAA1654106945NOM)	1	$598.00 USD
	Sub-total	$598.00 USD
	Discount	00.00
	Total	$598.00 USD

- We want to help protect you from scammers that attempt to impersonate Amazon. Remember these important clues so that you can identify scams and keep your account and information safe:

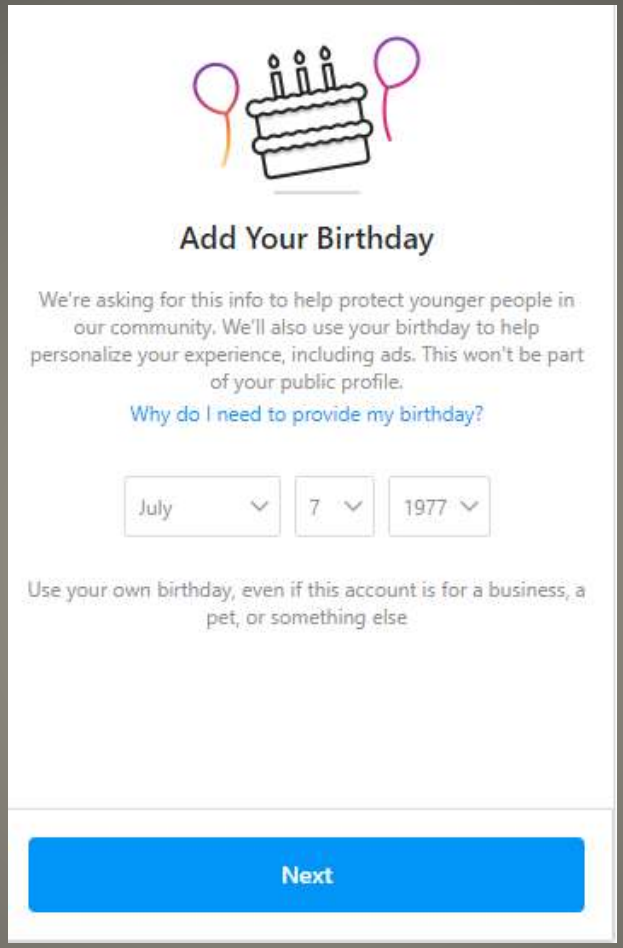
- Never feel pressured to give information (such as your credit card number or account password) over the phone, especially if the call was unexpected. Scammers may try to use calls, texts, and emails to impersonate Amazon customer service. If you're ever unsure, it's safest to end the call/chat and reach out directly to customer support through the Amazon app or website.
- Never pay over the phone. Amazon will never ask you to provide payment information, including gift cards (or “verification cards”, as some scammers call them) for products or services over the phone.
- Trust Amazon-owned channels. Always go through the Amazon mobile app or website when seeking customer support or when looking to make changes to your account.
- Be wary of false urgency. Scammers may try to create a sense of urgency to persuade you to do what they're asking. Be wary any time someone tries to convince you that you must act now.
- For more information on how to stay safe online, or to report suspicious communications, visit the Amazon Customer Service page, which can be found in the Help section at the bottom of the Amazon home page.

- Sincerely,
- Amazon

Amazon

Been there...


FRIDAY EVENING
PERFECT! I'LL FINISH THIS ON MONDAY
MONDAY MORNING...
WHAT DOES THIS MEAN!?!?


Add Your Birthday
We're asking for this info to help protect younger people in our community. We'll also use your birthday to help personalize your experience, including ads. This won't be part of your public profile.
Why do I need to provide my birthday?
July
7
1977
Use your own birthday, even if this account is for a business, a pet, or something else
Next

Instagram

Current Issues

- Supreme Court Justice Department
  No longer charge security researchers
  good-faith testing, investigating, correction
  Computer Fraud and Abuse Act
  Yeahbut state laws, civil suits
- Australian Drivers Licenses
  encryption with 4-digit PIN
  no backend validation
  Easy Identity theft - Underage
  Decrypted data available in device backup
- Web sites collect data AS IT IS TYPED IN
- GM discloses data breach
  names, addresses, phone numbers, locations, car milage, maintenance history
  California attorney general
  Customer reward points

- MS Office remote template feature
  HTML file from remote server
  ms-msdt://URI scheme
  load code & PowerShell
  EVEN tho macros disabled!!
  bypass Protected view using RTF extension

Current workaround:
CMD prompt as Administrator
"reg delete HKEY_CLASSES_ROOT\ms-msdt /f"
NOT detected by Windows Defender

MSDT Follina

Current Issues

- Enquiring Minds audio
  QR codes
  QR codes on borrowed phones
  Transfers on borrowed phones
  Financial transfers via smart watch
  Apple watch with Apple Pay
- DuckDuckGo browser
  block Facebook & Google trackers
  Microsoft not so much
  Browser on iOS, Android, Mac (beta)
  Bing & LinkedIn
  Microsoft NDA
- ProtonMail rebranded Proton
  Proton.me
  Password reset? ReActivate keys

Current Issues

- Warning:
  Gmail credentials to login to Facebook
  Open Authentication hack
  Oauth id_token/code
  Bug bounty $44,625
- What's Up WhatsApp?
  Settings > Account > Request account info > Request report
  Settings > Account > Privacy
- GhostTouch 1.5"

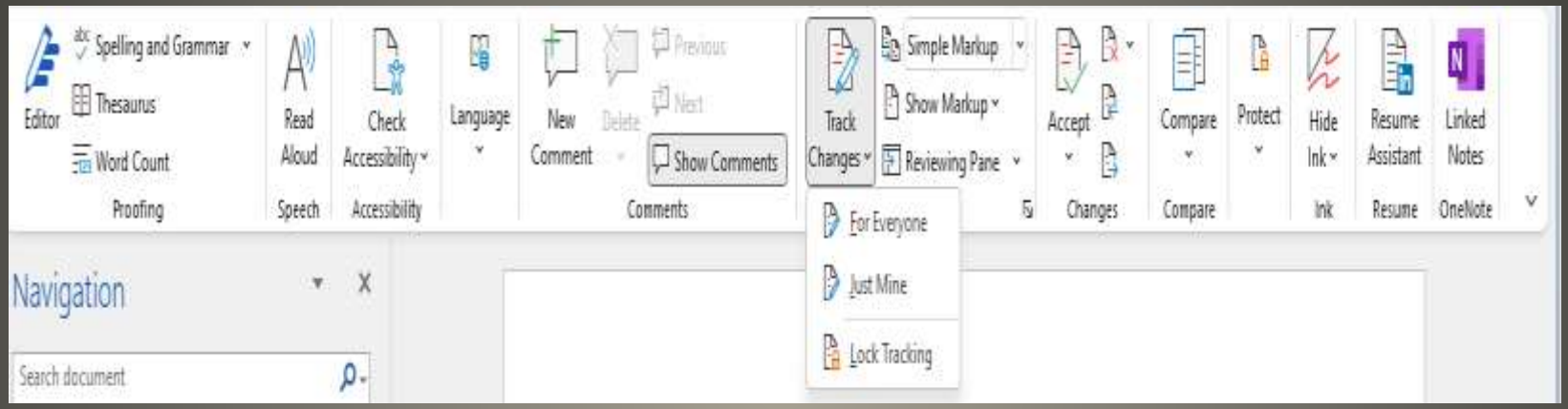
Password Managers – Helpful

- 256-bit AES
- Zero trust Master password encrypted on device
- MFA Multi-factor authentication(s)
- Beats the alternative
- Select which passwords are stored
- Multi password managers

Password managers - cautions

- EVERYTHING in one place
  Decrease chance of hack
  Increase harm of hack
- Keyloggers
  Decreases risk for protected sites
  Increases risk for password manager access
- Managed accounts easy access if logged on
- Fees explicit & implicit
- BACKUP
- Password managers have and will be hacked
- Position of trust
- Locality of company - Privacy laws
- Forget your master password?

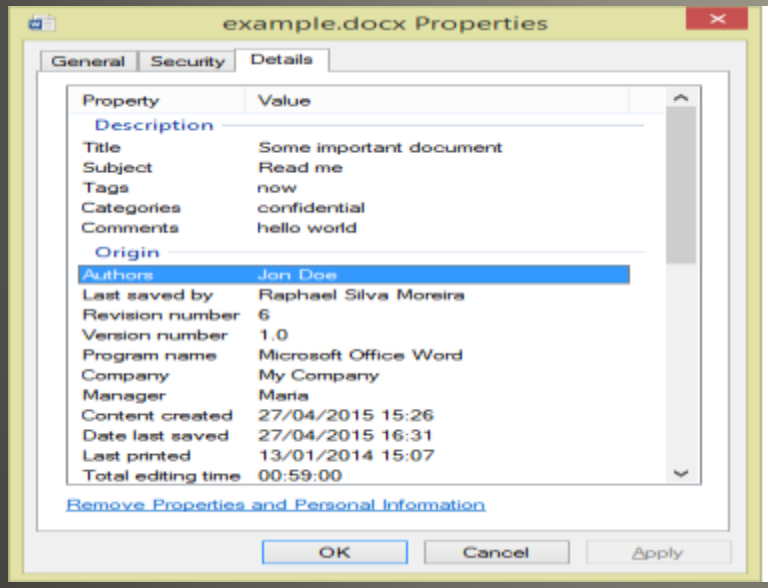
- Office files with Track Changes

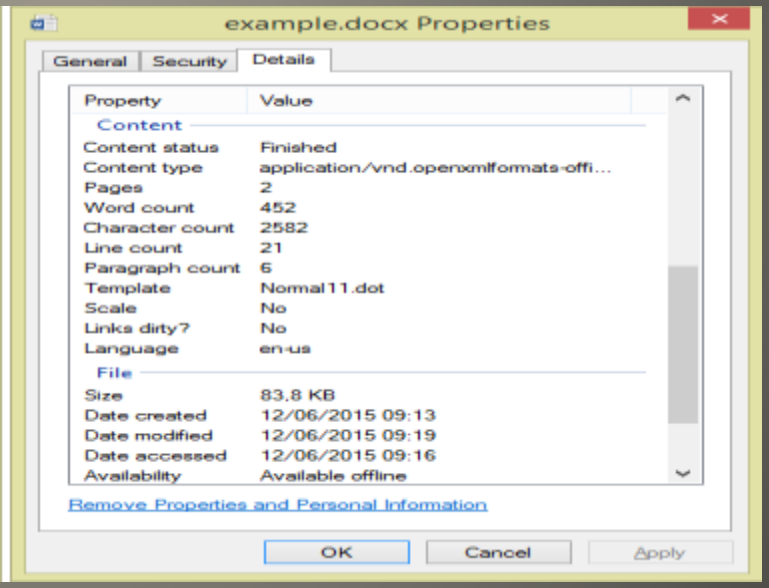


Windows Metadata

- File Metadata

  Right click > Properties > Details > Remove Properties and Personal Information





Windows Metadata

- Create a copy with all possible properties removed
- Remove the following properties from this file
- Helpful <> Harmful
- Backup / archive

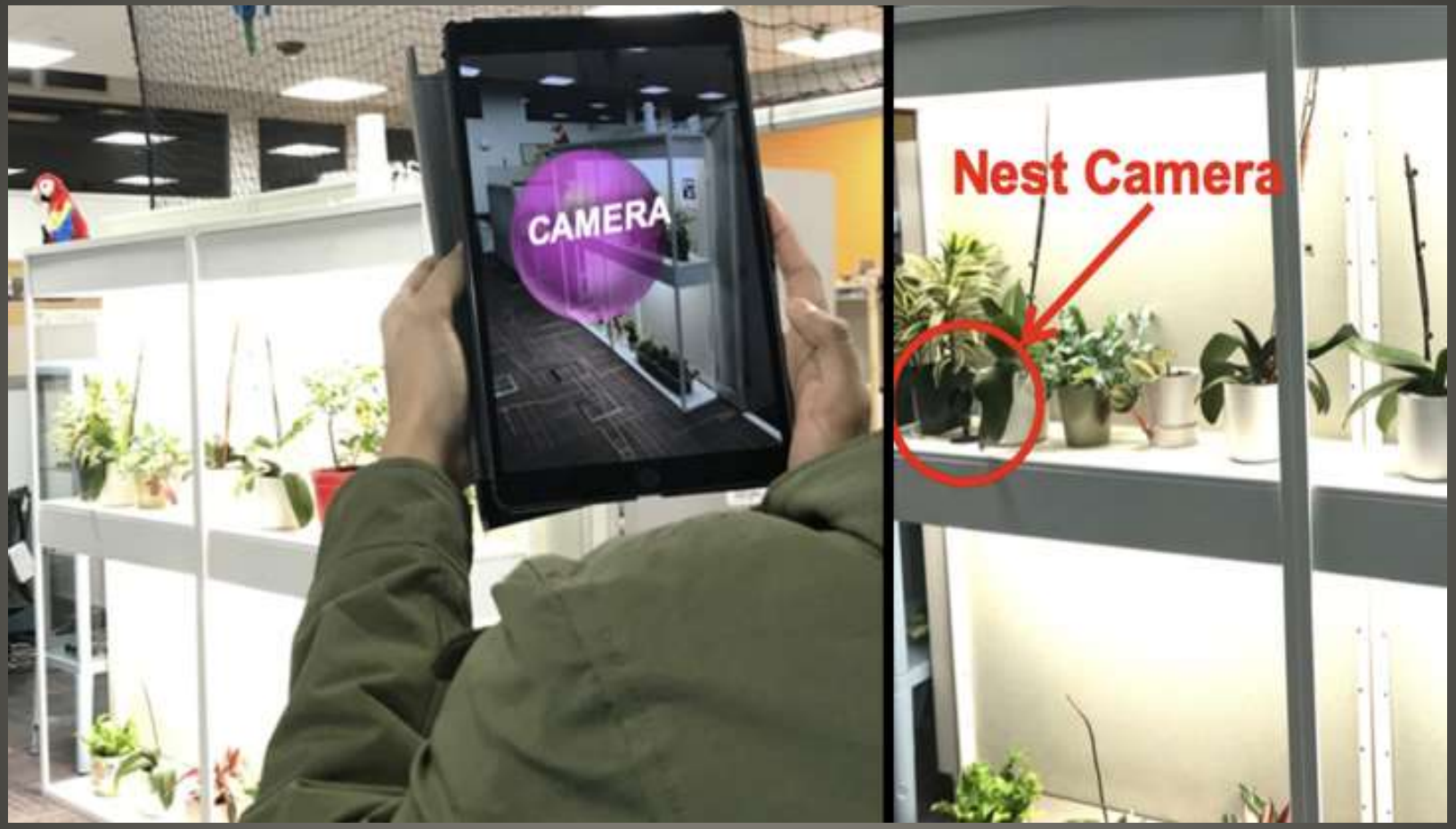
Windows Metadata

ProtonMail gives its users numerous benefits:

- Based in Switzerland, i.e. not one of the "Five Eyes," "Nine Eyes," and "14 Eyes" networks.
- Using zero-access end-to-end encryption. This means that ProtonMail cannot read or decrypt your emails either.
- No logs of IP addresses are kept that can be linked to an anonymous email account.
- It's an open-source, easy-to-use email with a modern inbox design.
- Self-destructing messages.
- Secure communication with other email providers.

- An encrypted transmission (TLS).
- End-to-end encrypted email storage.
- End-to-end encryption of all internal emails.
- Two-factor authentication.
- Apps for Android, iOS, and desktop.
- An encrypted calendar function to keep your activities private.
- Data processing in accordance with the EU's General Data Protection Regulation (RGPD).

Proton Mail vs. Tutanota ?

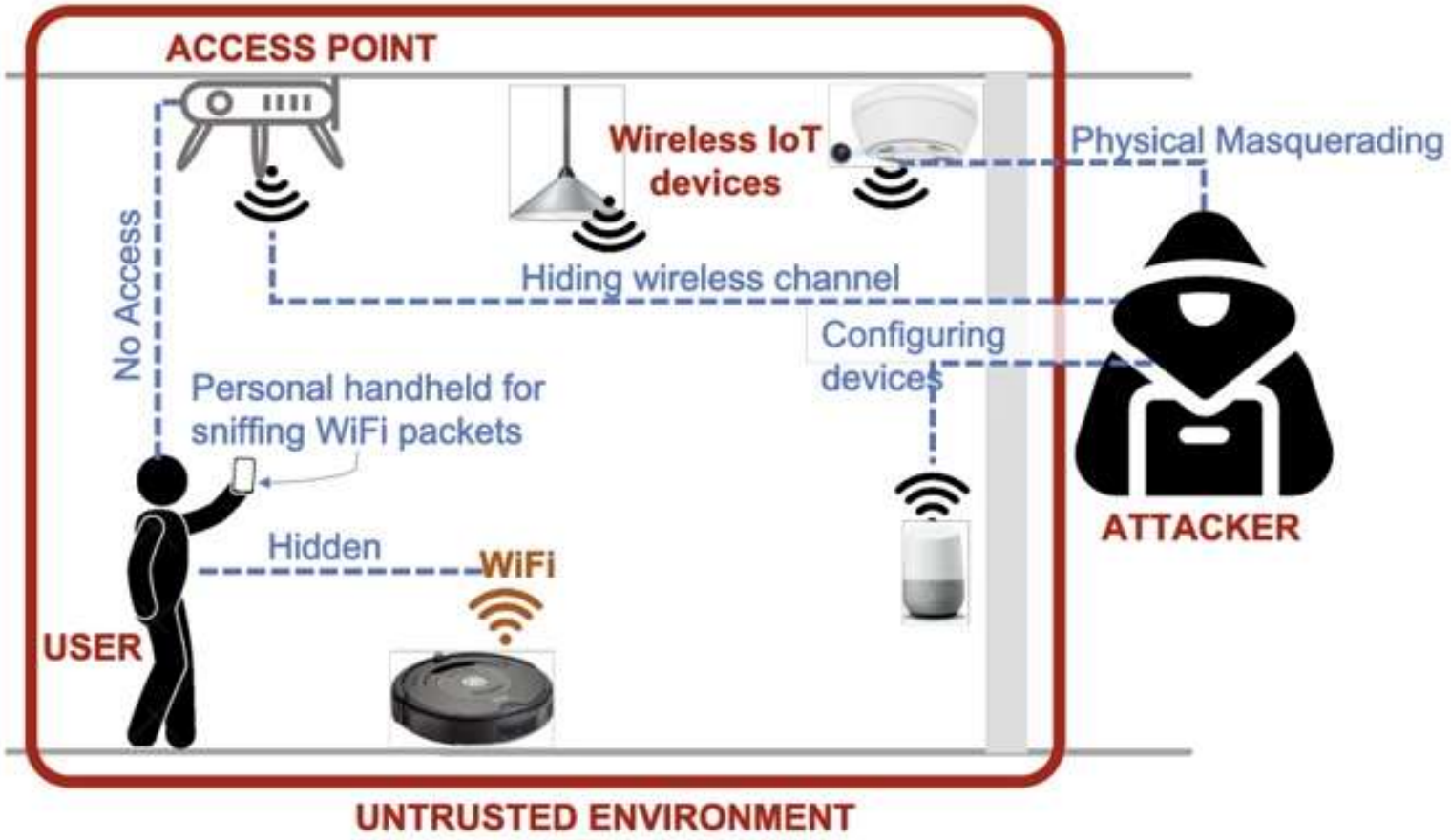


Lumos Wi-Fi IoT detection

Lumos Wi-Fi IoT Detection

- Augmented Reality
- Walk around
- Wi-Fi signal strength (Received Signal Strength) RSSI
- Visual Inertial Odometry (VIO)
- MAC Address
- Alter signal strength & MAC ?

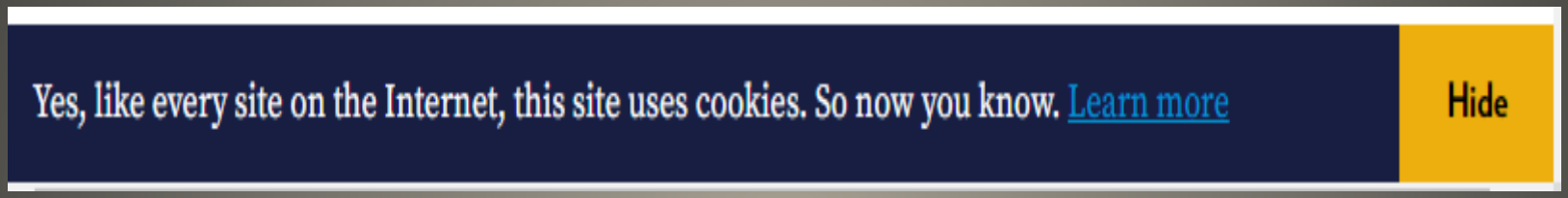
- Local storage instead of Wi-Fi


ACCESS POINT
Wireless IoT devices
Physical Masquerading
No Access
Hiding wireless channel
Configuring devices
Personal handheld for sniffing WiFi packets
ATTACKER
Hidden
WiFi
USER
UNTRUSTED ENVIRONMENT

Current Issues

- Windows Subsystem for Linux (WSL)
  malware steals browser auth cookies
- WSL malware increasing
  Using telegraph to communicate
  standard RAT capabilities
- Free & low costs VPN revenue
  Ads
  Cookies
  Tracking pixels
  Freemium
  VPN logs
  Sell the data

- Lotus-1-2-3 on Linux

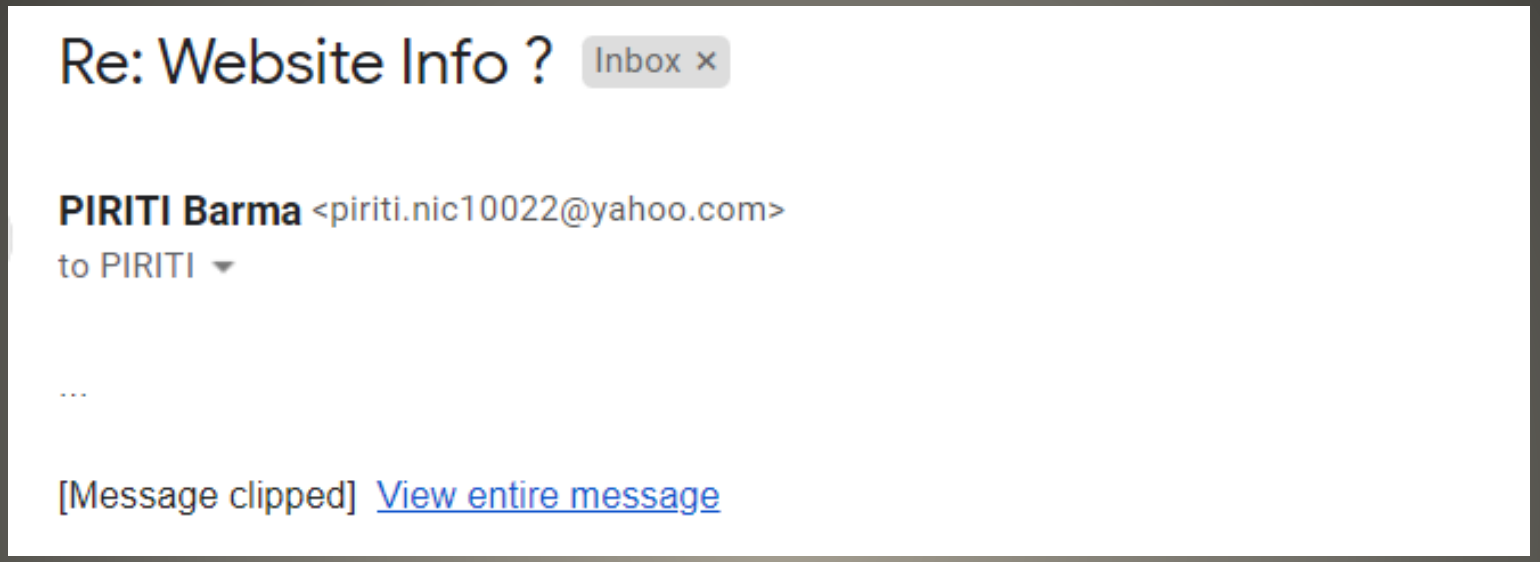


Clearview AI

- Facial recognition services
- Cameras, connectivity, bandwidth, storage, processing, etc. Lowered costs
- 100 Billion images by end of this year
- Illinois Biometric Information Privacy Act 2008 requires consent for any biometric data for Illinois citizen
- ACLU suit settlement – No LE in Illinois
- Helpful <> Harmful
- Ukraine

Facial Recognition

- Expectation of privacy
  Public display of face
  Private display, but given to public
    family celebration to social media
- Right to forget

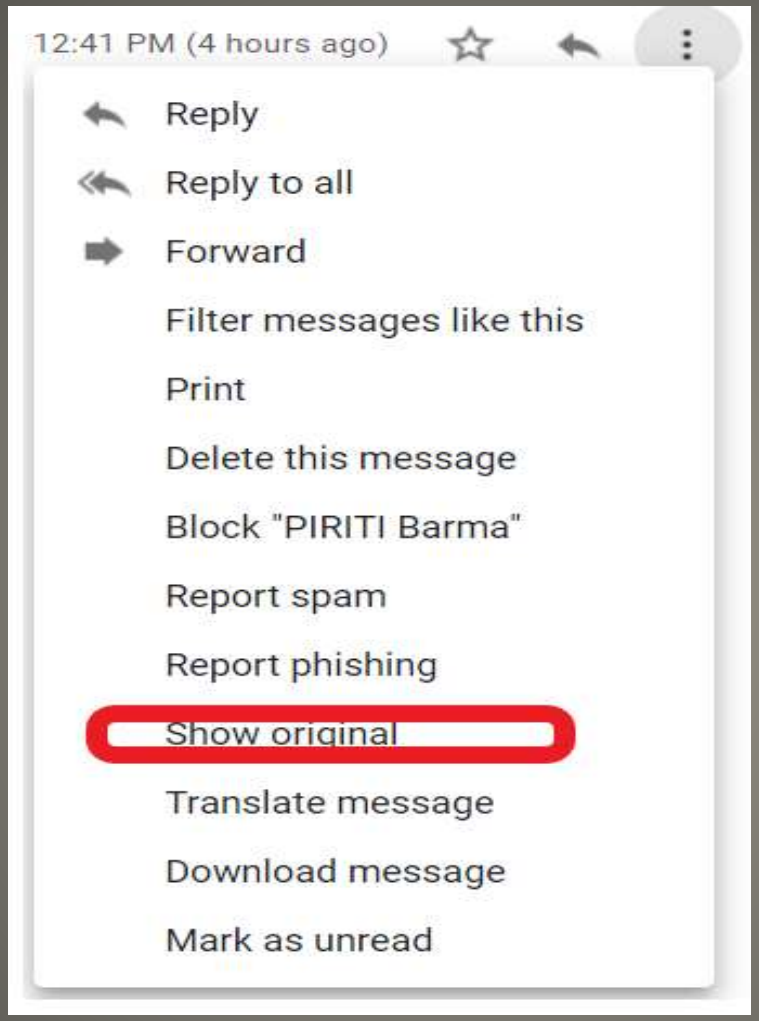


eMail Message clipped

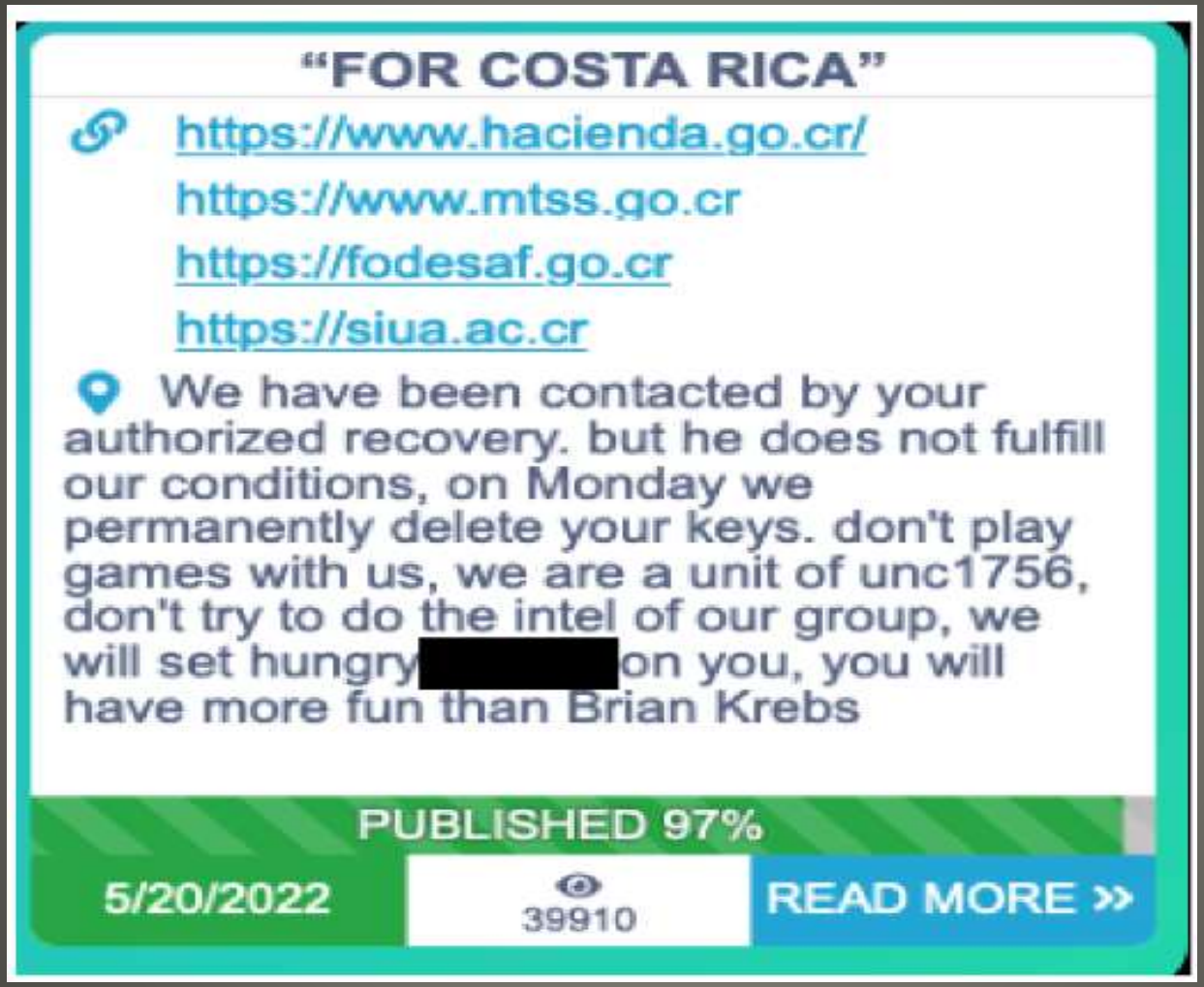
Original Message

Message ID	<1735302473.3852785.1653932453828@mail.yahoo.com>
Created at:	Mon, May 30, 2022 at 12:40 PM (Delivered after 17 seconds)
From:	PIRITI Barma <piriti.nic10022@yahoo.com> Using WebService/1.1.20225 YMailNorrin
To:	PIRITI Barma <piriti.nic10022@yahoo.com>
Subject:	Re: Website Info ?
SPF:	PASS with IP 106.10.244.38 Learn more
DKIM:	'PASS' with domain yahoo.com Learn more
DMARC:	'PASS' Learn more

eMail message clipped



eMail message clipped



Geopolitical Ransomware

Vodafone

- New method of user tracking
- TrustPid
- Fixed ID for every customer at ISP level
- No current bypass method
- Free Internet => users are product

- 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