Sun City Computer Club

Cyber Security SIG

January 5, 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

LastPass Customer Data Stolen

- Insider Threat Known & UnKnown
- Backup(s) of customer data
- Encrypted Vaults & Other customer data
- Customers can expect increased attacks
  Due to the volume & sensitivity of data
- Weak or use of Master password elsewhere
- USE MFA
- Use password managers for NON financial
- Be AWARE Prepare understand
- https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/
- 3rd security incident at LastPass this year
- https://www.tomsguide.com/how-to/how-to-delete-your-lastpass-account

- Passwordstate highly vulnerable
- Associated Press Investigation

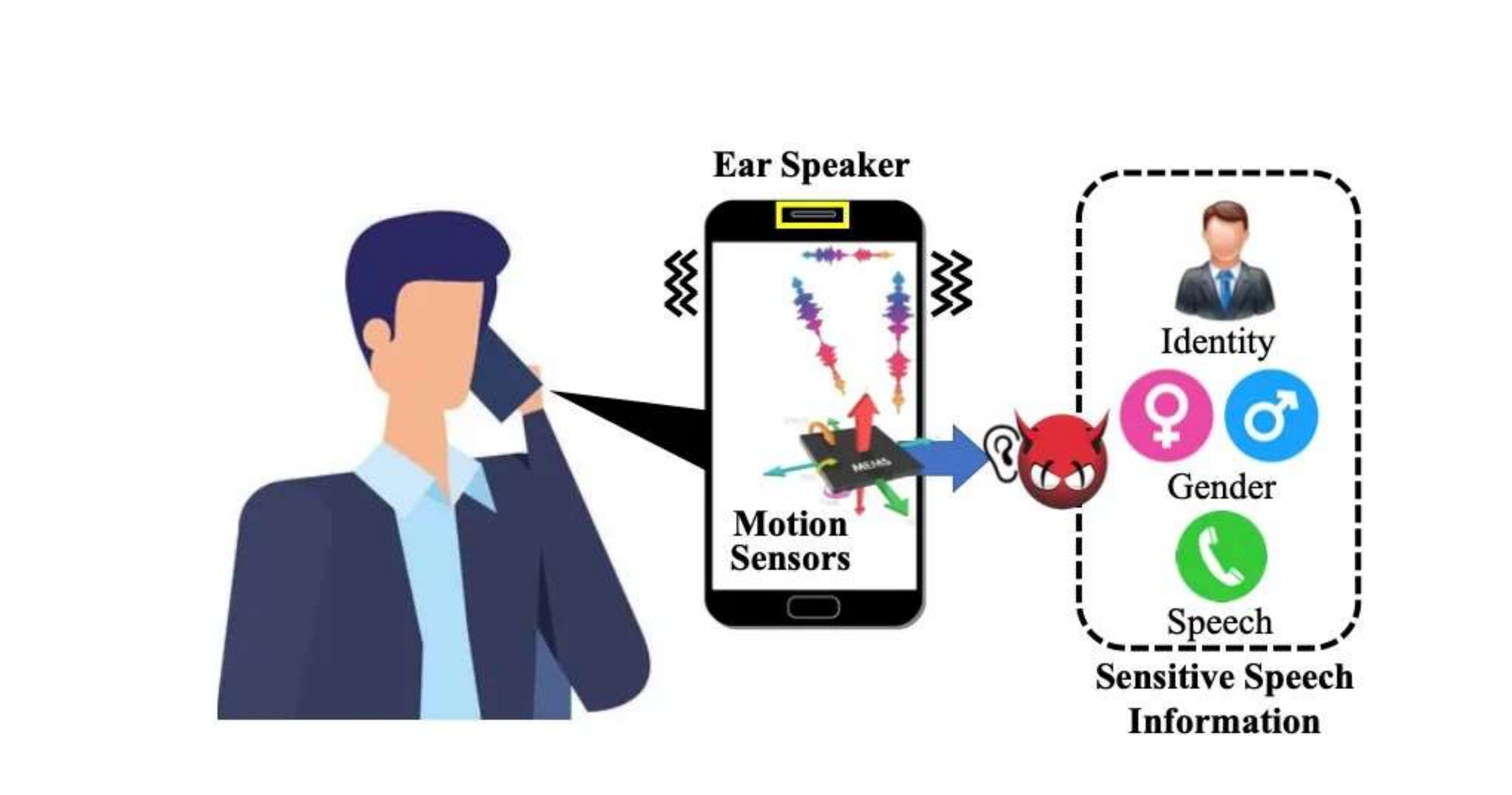
  Covid-19 tech to expand surveillance
- Apple AirTags firmware update

  Version 2.0.36 FindMy Items

  Unknown AirTag moving with you
- Apple Home App upgrade pulled
- TikTok

  Hardware info, installed apps, memory usage, IP Address, recently used Wi-Fi points
- IPVanish VPN selling customer data
- Twitter user data dump offered for sale
- Deezer data breach

Current Issues


Ear Speaker
Motion Sensors
MEMS
Identity
Gender
Speech
Sensitive Speech Information

EarSpy

Todo: Day manager

- Android App
- Banking trojan Xenomorph
- Permissions please
- Yes? Add device administrator

  Difficult to remove   Hide

  Backup Data

  Factory reset

  Monitor bank, broker, shopping, credit card
- No

  Remove app

- Comcast Hacked Xfinity bypass 2FA

  Why would I care?

  Emails from hacked contacts
- Every breach/hack

  They get a portion of *our* money
- Godfather Android banking trojan

  400 banking & cryptocurrency apps

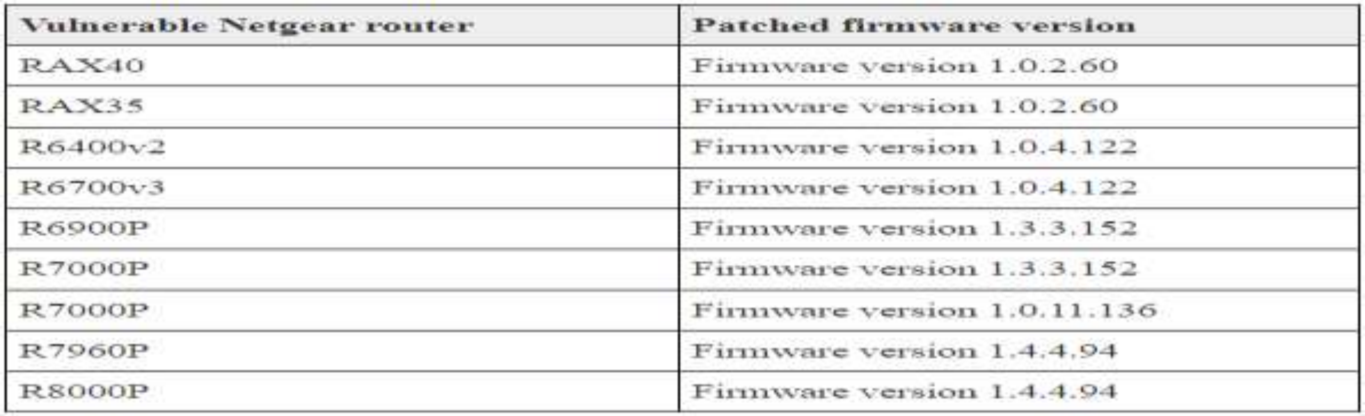
  16 countries 49 US companies

  Fake overlay Fake Google Protect
- Apple Crash Detection feature false positives

Current Issues

Current Issues

- ChatGPT
  - Generate phishing email campaign
  - Closely match to real company
  - Generate infection chain
  - Create VBA code for Excel document
- NetGear Wi-Fi routers



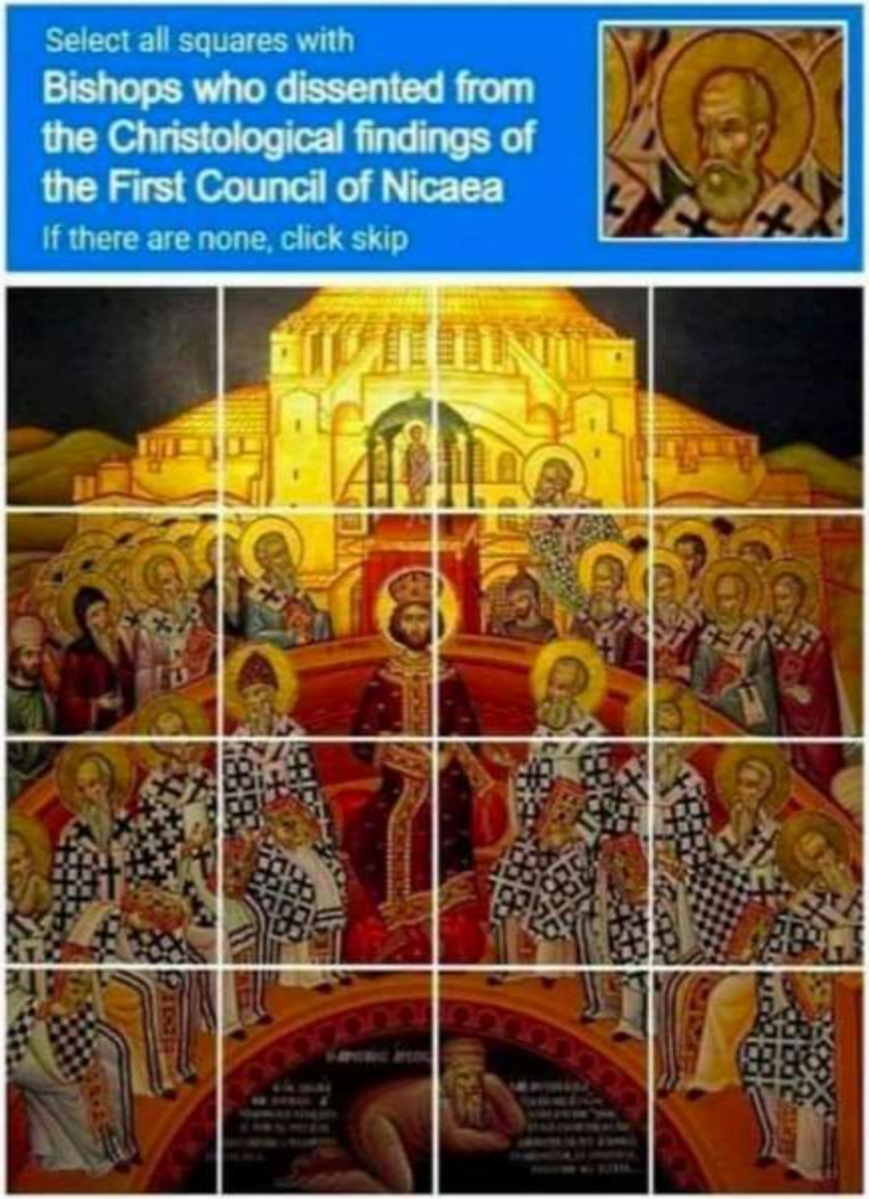
Vulnerable Netgear router	Patched firmware version
RAX40	Firmware version 1.0.2.60
RAX35	Firmware version 1.0.2.60
R6400v2	Firmware version 1.0.4.122
R6700v3	Firmware version 1.0.4.122
R6900P	Firmware version 1.3.3.152
R7000P	Firmware version 1.3.3.152
R7000P	Firmware version 1.0.11.136
R7960P	Firmware version 1.4.4.94
R8000P	Firmware version 1.4.4.94

FBI recommends using Ad blocker

- Phishing   Fake websites   Ads
- Alter search results
- More real than real
- Please remove your ad blocker pleas

Cyber Threat Intelligence Sharing

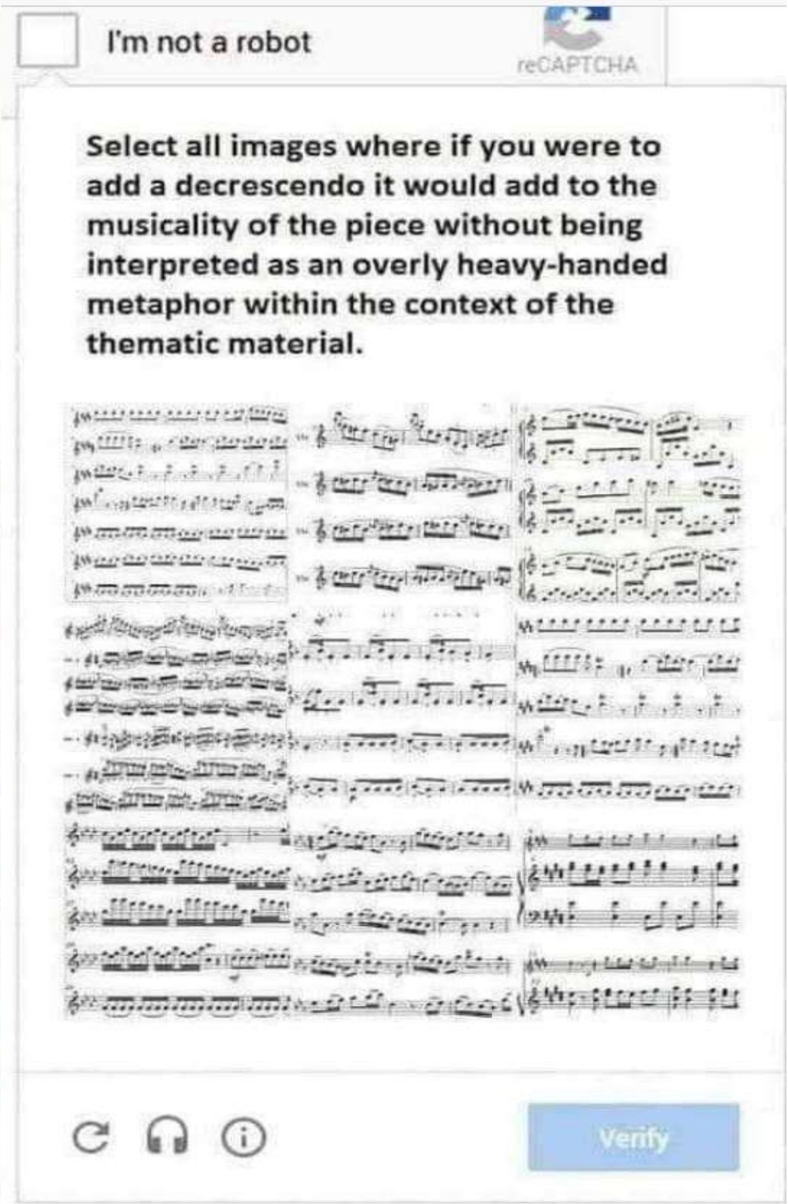
- Awareness, Preparedness, Understanding
- They use sharing playbooks scripts
  Help centers
- Why us as individuals not security vendors?
  They want to sell that information/help
- FBI InfraGard - hacked
- CrowdSec



Select all squares with

Bishops who dissented from the Christological findings of the First Council of Nicaea

If there are none, click skip



Select all images where if you were to add a decrescendo it would add to the musicality of the piece without being interpreted as an overly heavy-handed metaphor within the context of the thematic material.

- Why not both?
- Privacy & Security

Tutanota AES-128 & RSA 2048
encrypts subject line, calendar, address book
Perfect forward secrecy
2FA & U2F

Proton
RSA 2048 between Proton users
AES 256 between users & non-users
No Perfect Forward Secrecy
2FA

Proton Mail vs Tutanota

Proton Mail vs Tutanota

- Privacy & Anonymity

  Tutanota HQ Germany 14-Eyes member
  Not much private info to enroll
  No logs
  IP Address stripped

  Proton HQ Switzerland
  Not much private info to enroll
  No Logs
  IP Address stripped
  Data has been given

- Ease of Use

  Tutanota

  Other users pre-agreed password

  full search capability

  Proton

  External encryption

  Limited search capability

  Senders, subject lines, recipients, time

Proton Mail vs Tutanota

- Compatibility
  Tutanota
  WEB based
  macOS, Windows, Linux, iOS, Android
  No third-party integrations

  Proton
  WEB based
  iOS and Android
  ProtonMail Bridge   IMAP & SMTP

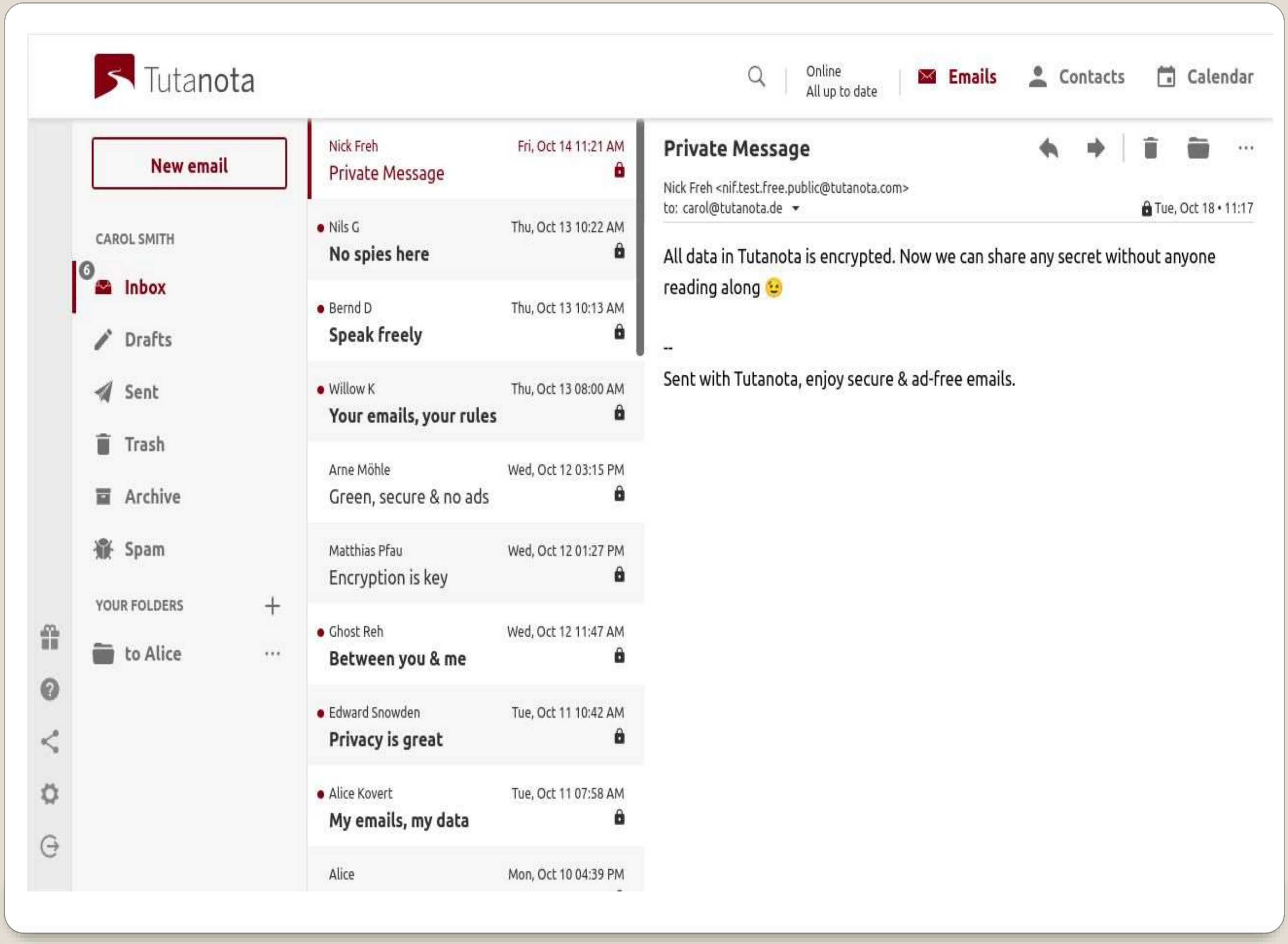
Proton Mail vs Tutanota

Proton Mail vs Tutanota

- Why Not Both?

  Fit for Purpose

  Segment



Nick Freh Fri, Oct 14 11:21 AM
Private Message

Nils G Thu, Oct 13 10:22 AM
No spies here

Bernd D Thu, Oct 13 10:13 AM
Speak freely

Willow K Thu, Oct 13 08:00 AM
Your emails, your rules

Arne Möhle Wed, Oct 12 03:15 PM
Green, secure & no ads

Matthias Pfau Wed, Oct 12 01:27 PM
Encryption is key

Ghost Reh Wed, Oct 12 11:47 AM
Between you & me

Edward Snowden Tue, Oct 11 10:42 AM
Privacy is great

Alice Kovert Tue, Oct 11 07:58 AM
My emails, my data

Alice Mon, Oct 10 04:39 PM

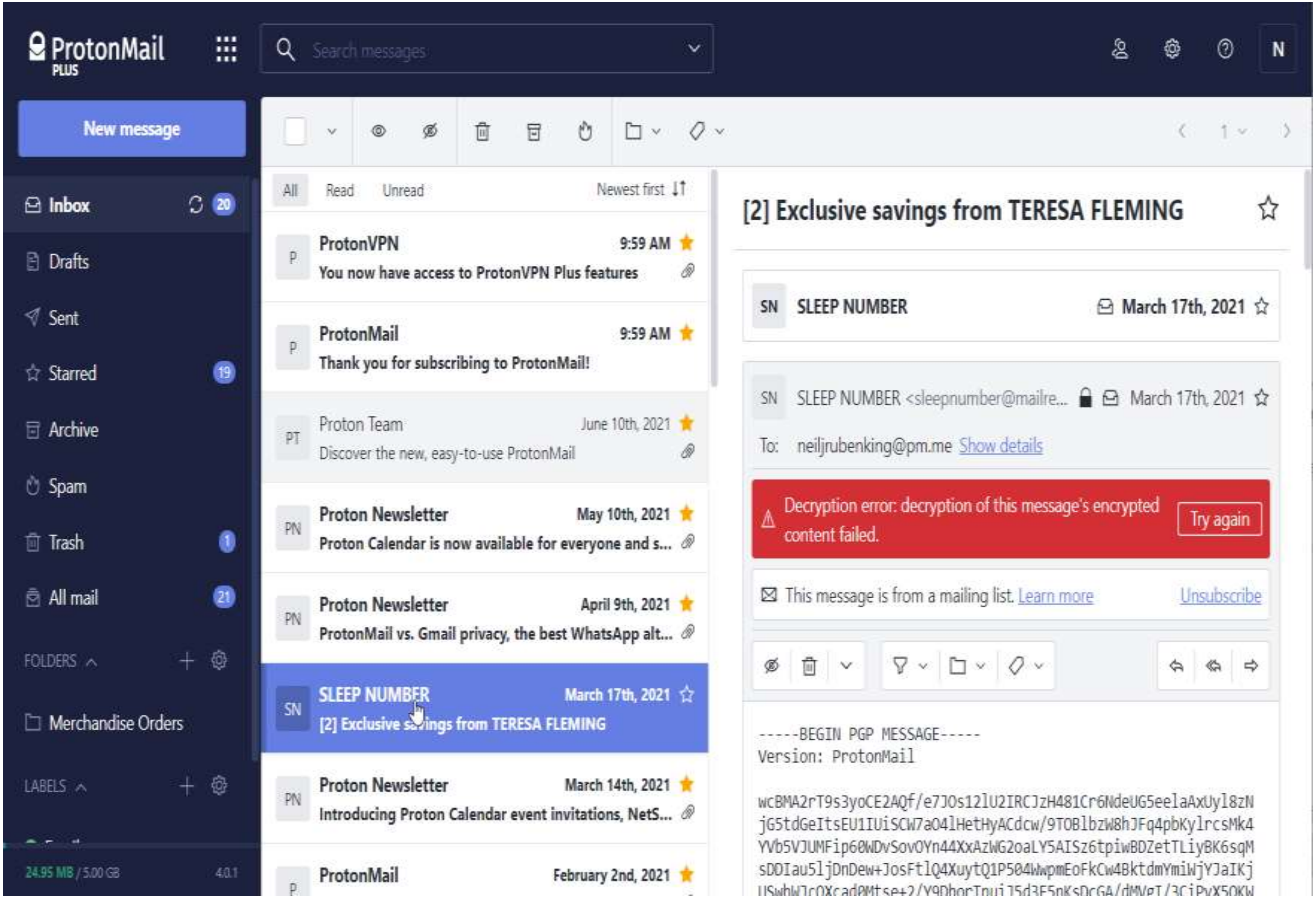
Private Message

Nick Freh <nif.test.free.public@tutanota.com>
to: carol@tutanota.de
Tue, Oct 18 • 11:17

All data in Tutanota is encrypted. Now we can share any secret without anyone reading along 😉

--

Sent with Tutanota, enjoy secure & ad-free emails.



P	ProtonVPN You now have access to ProtonVPN Plus features	9:59 AM
P	ProtonMail Thank you for subscribing to ProtonMail!	9:59 AM
PT	Proton Team Discover the new, easy-to-use ProtonMail	June 10th, 2021
PN	Proton Newsletter Proton Calendar is now available for everyone and s...	May 10th, 2021
PN	Proton Newsletter ProtonMail vs. Gmail privacy, the best WhatsApp alt...	April 9th, 2021
SN	SLEEP NUMBER [2] Exclusive savings from TERESA FLEMING	March 17th, 2021
PN	Proton Newsletter Introducing Proton Calendar event invitations, NetS...	March 14th, 2021
P	ProtonMail	February 2nd, 2021

[2] Exclusive savings from TERESA FLEMING

SN SLEEP NUMBER March 17th, 2021

SN SLEEP NUMBER <sleepnumber@mailre... March 17th, 2021

To: neiljrubenking@pm.me Show details

Decryption error: decryption of this message's encrypted content failed. Try again

This message is from a mailing list. Learn more Unsubscribe

```
-----BEGIN PGP MESSAGE-----
Version: ProtonMail

wcBMA2rT9s3yoCE2AQf/e7JOs12lU2IRCJzH481Cr6NdeUG5eelaAxUyl8zN
jG5tdGeItsEU1IUiSCW7aO4lHetHyACdcw/9TOBlbzW8hJFq4pbKylrcsMk4
YVb5VJUMFip60WDvSovOYn44XxAzWG2oaLY5AISz6tpiwBDZetTLiyBK6sqM
sDDIau5ljDnDew+JosFtlQ4XuytQ1P504WwpmEoFkCw4BktdmYmiWjYJaIKj
USwhWJcOXcadPMtse+2/Y9DhorTnuiJ5d3F5nKsDcGA/dMVgT/3CiPvX5OKW
```

- Additional Features

  Tutanota

  Secure Connect

  website to create encrypted contact form

  Proton

  ProtonVPN

  Self-Destruct messages

Proton Mail vs Tutanota

- Open tracking disrupts email marketing

Apple eMail Privacy changes

VPN Disadvantages

- Slower
- False sense of security
- Increase of data usage Data caps
- Legal issues
- Some sites will have issues
- VPN Logs availability
- Costs

- Ukraine attack on Russian troops

  Blamed on soldier's use of banned cell phones
- EU Digital Markets Act

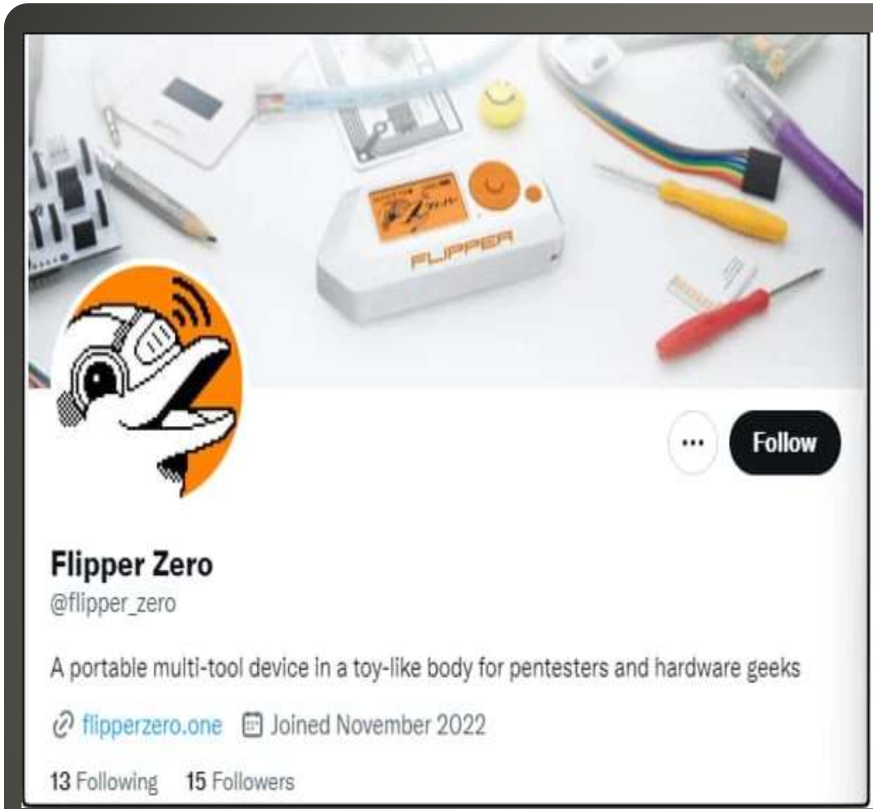
  Choice screens   March 2024

  Proton Switzerland

  UK Online Safety Bill

  EU proposal to fight CSAM
- LockBit ransomware – Toronto Children’s Hospital
- Crypto Currency co2 emissions
- Proof of work -> Proof of stake   or tax

Current Issues

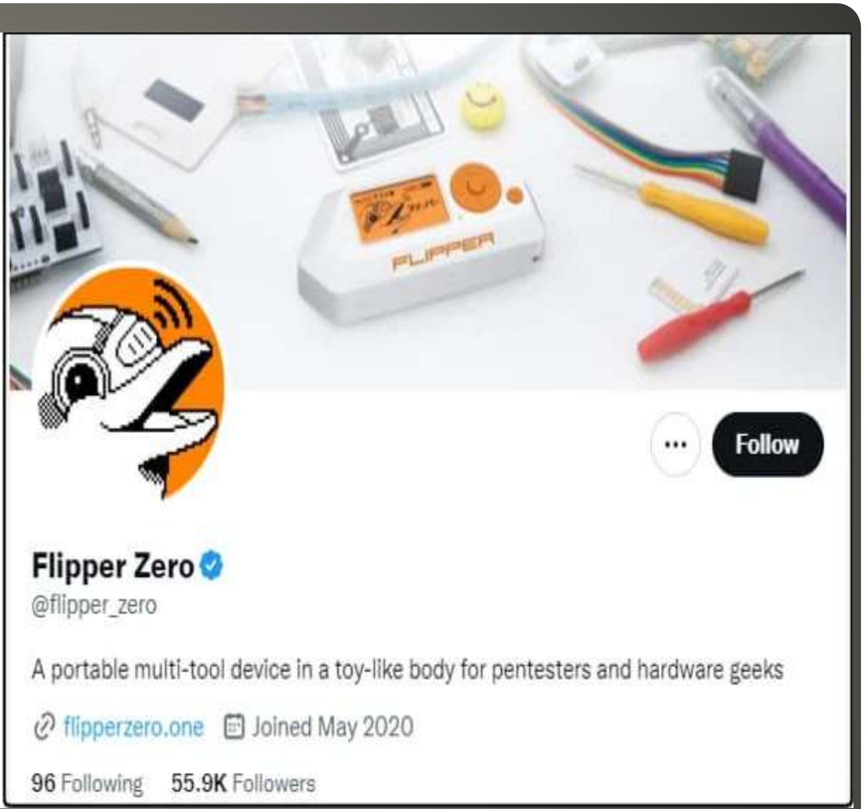


Flipper Zero
@flipper_zero

A portable multi-tool device in a toy-like body for pentesters and hardware geeks

flipperzero.one Joined November 2022

13 Following 15 Followers



Flipper Zero
@flipper_zero

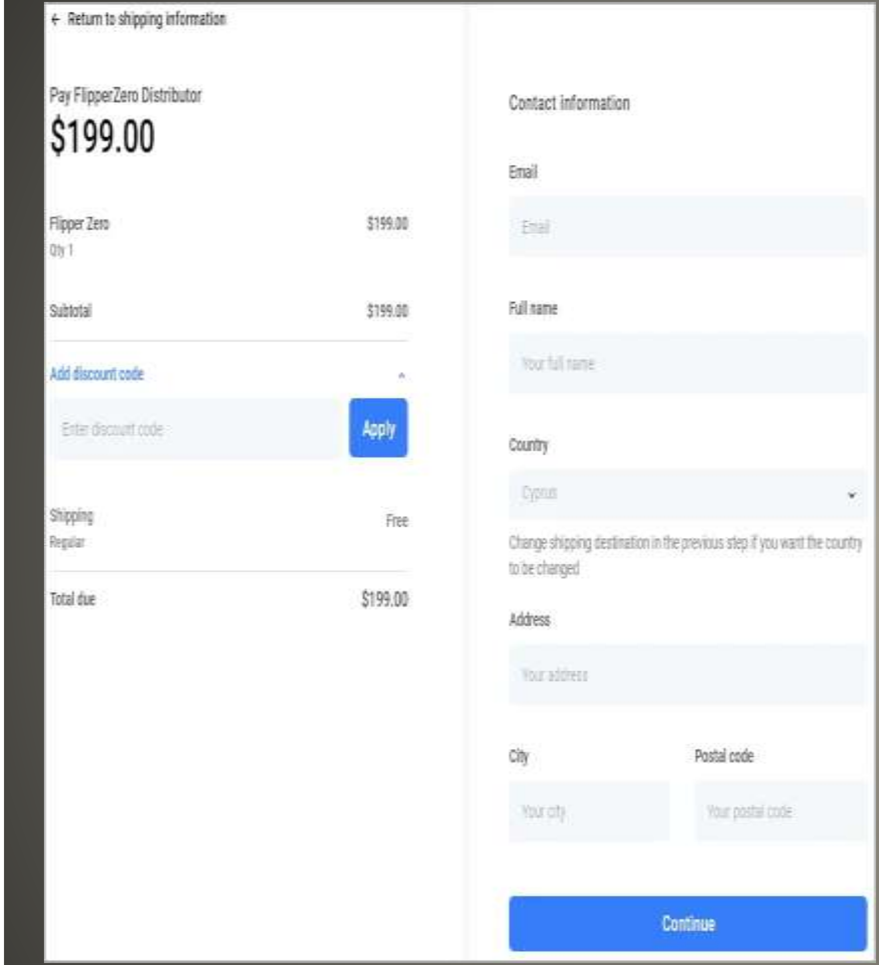
A portable multi-tool device in a toy-like body for pentesters and hardware geeks

flipperzero.one Joined May 2020

96 Following 55.9K Followers

Flipper Zero

Flipper Zero



← Return to shipping information

Pay FlipperZero Distributor

$199.00

Flipper Zero Qty 1	$199.00
Subtotal	$199.00

Add discount code

Enter discount code

Shipping Regular	Free
Total due	$199.00

Contact information

Email: Email

Full name: Your full name

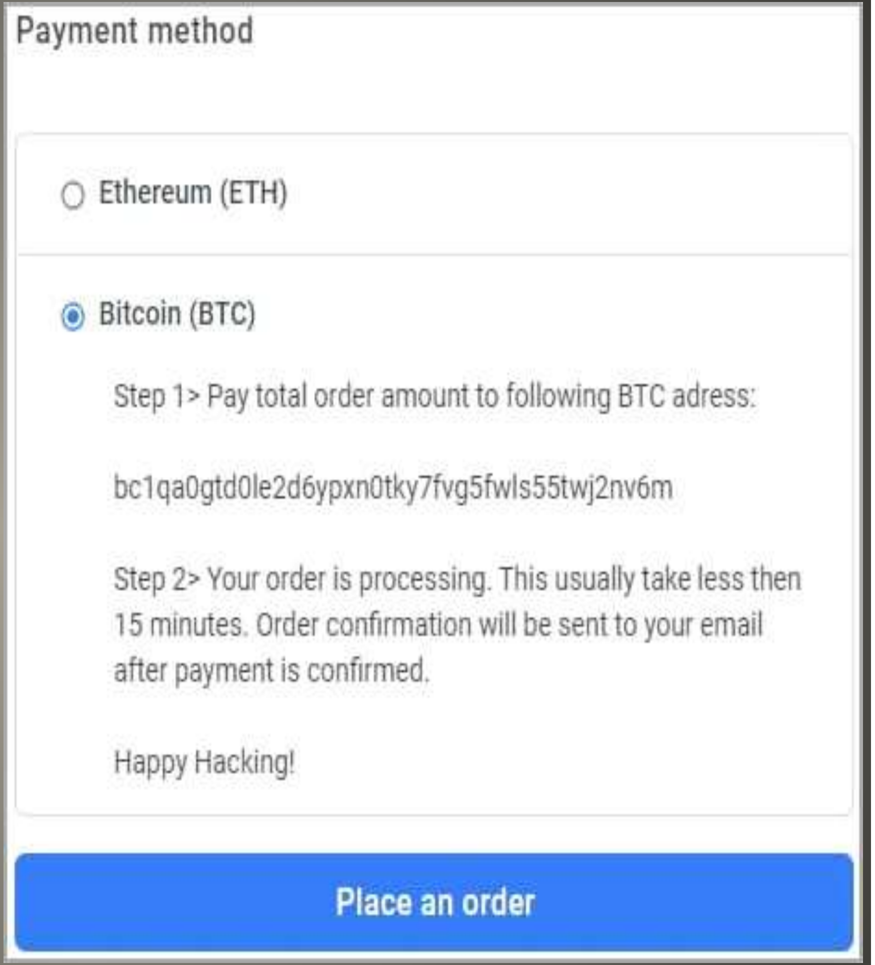
Country: Cyprus

Change shipping destination in the previous step if you want the country to be changed

Address: Your address

City: Your city

Postal code: Your postal code



Payment method

○ Ethereum (ETH)

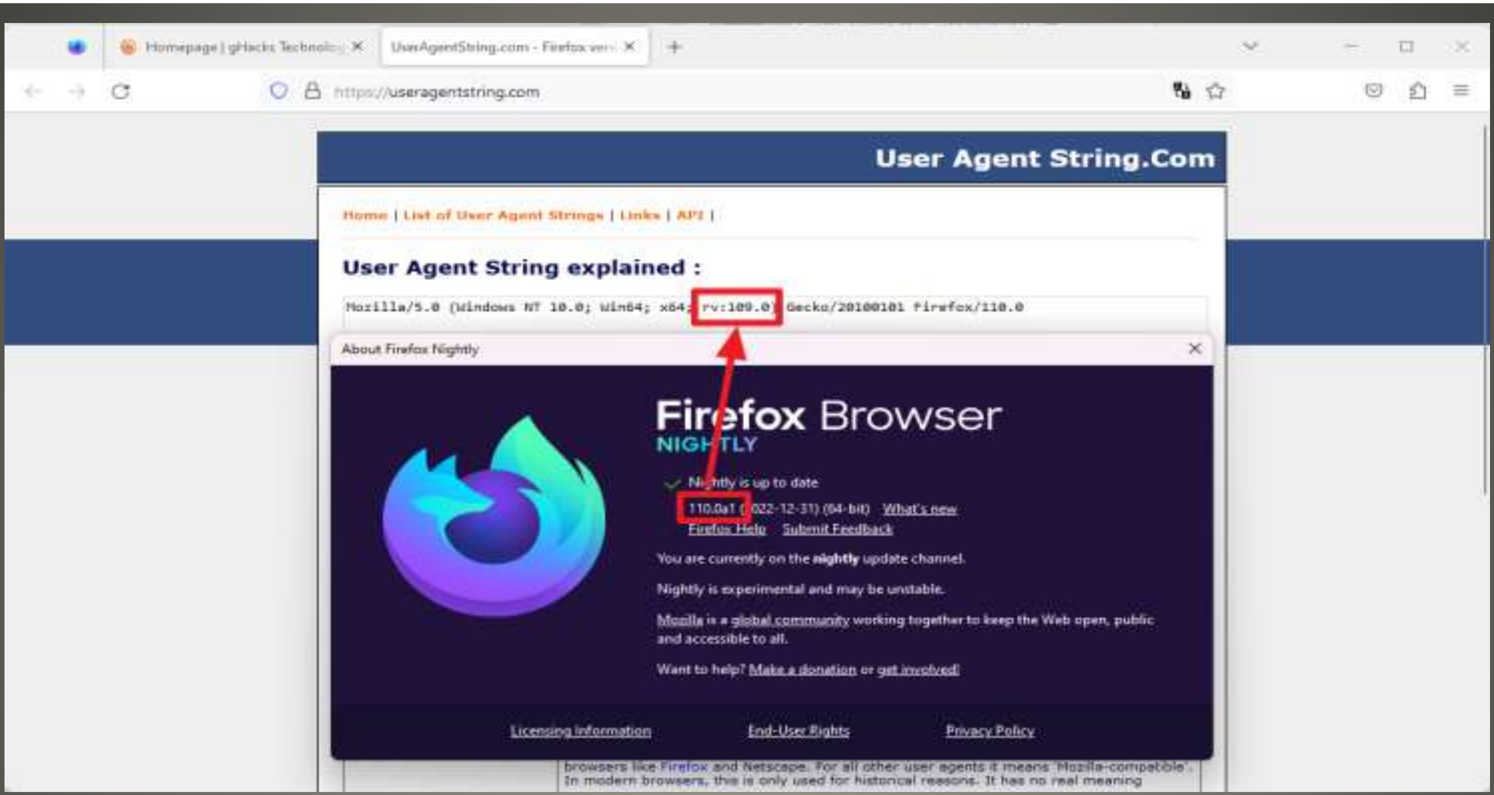
● Bitcoin (BTC)

Step 1> Pay total order amount to following BTC adress:

bc1qa0gtd0le2d6ypxn0tky7fvg5fwls55twj2nv6m

Step 2> Your order is processing. This usually take less then 15 minutes. Order confirmation will be sent to your email after payment is confirmed.

Happy Hacking!


Homepage | gHacks Technolo
UserAgentString.com - Firefox vers
https://useragentstring.com

User Agent String.Com

Home | List of User Agent Strings | Links | API |

User Agent String explained :

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
```

About Firefox Nightly

Firefox Browser
NIGHTLY

✓ Nightly is up to date

110.0a1 (2022-12-31) (64-bit) What's new

Firefox Help Submit Feedback

You are currently on the **nightly** update channel.

Nightly is experimental and may be unstable.

Mozilla is a global community working together to keep the Web open, public and accessible to all.

Want to help? Make a donation or get involved!

browsers like Firefox and Netscape. For all other user agents it means 'Mozilla-compatible'. In modern browsers, this is only used for historical reasons. It has no real meaning

- Internet Explorer 11's user agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko
- Firefox 110's: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:110.0) Gecko/20100101 Firefox/110.0

Firefox changes User Agent String

VPN Obfuscation

- Disguise VPN traffic as normal traffic
- Detect VPN signatures
- Obfsproxy

  ToR project

  HTTP traffic w/ unusual handshake

  Can be blocked
- OpenVPN Scramble

  XOR additive cipher
- OpenVPN over SSL

  SSL encrypted tunnel for VPN tunnel

  Tunnel setup is complex
- Shadowsocks

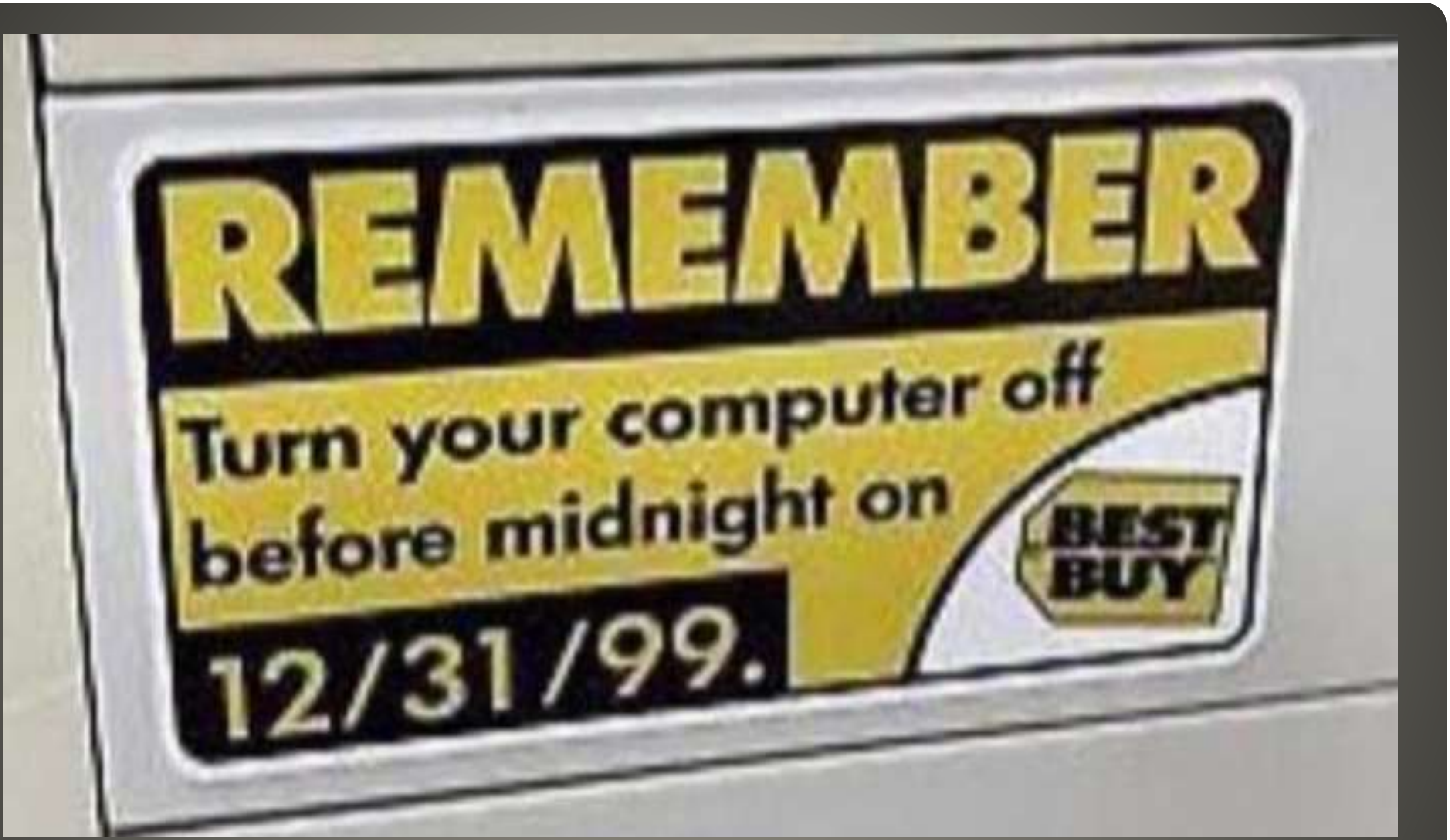
  HTTPS traffic

- Avoid VPN blocks
- Privacy
- Censorship

VPN Obfuscation

- https://support.nordvpn.com/Connectivity/1530940912/How-to-enable-or-disable-Obfuscated-servers.htm

Nord VPN



REMEMBER

Turn your computer off before midnight on 12/31/99.

Y2K

- Hardware

  Very small

  Attach behind PC tower

  Inside keyboard

- Software

  Malicious add-on to OS (Windows, macOS)

  Wrong characters

  Malware indicators

  Unusual account activity

  Watchful, Security Scan, Monitor network activity,

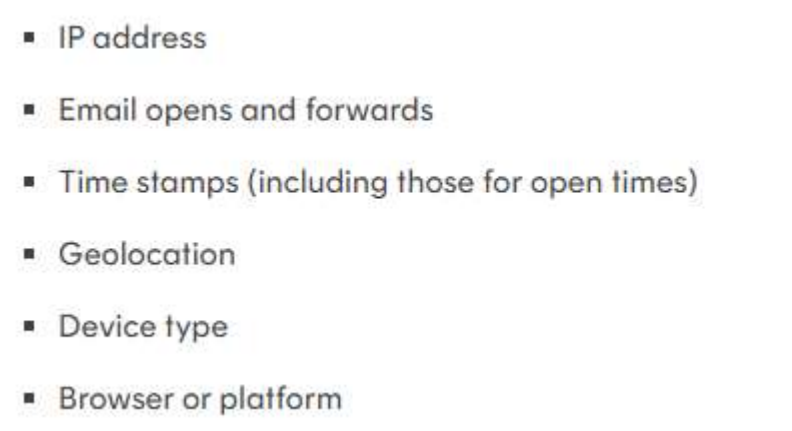
  Reimage – Clean Install

Key Loggers

- Apple Mail Privacy Protection
- Apple Mail 48% market share
- New Features

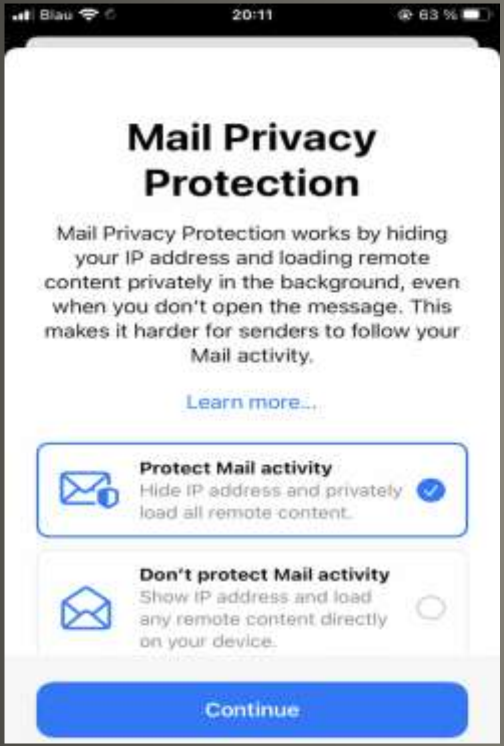
  Allow users to hide information:

  When Where How email is opened
- MPP Mail Privacy Protection



- IP address
- Email opens and forwards
- Time stamps (including those for open times)
- Geolocation
- Device type
- Browser or platform

Apple Mail Privacy change



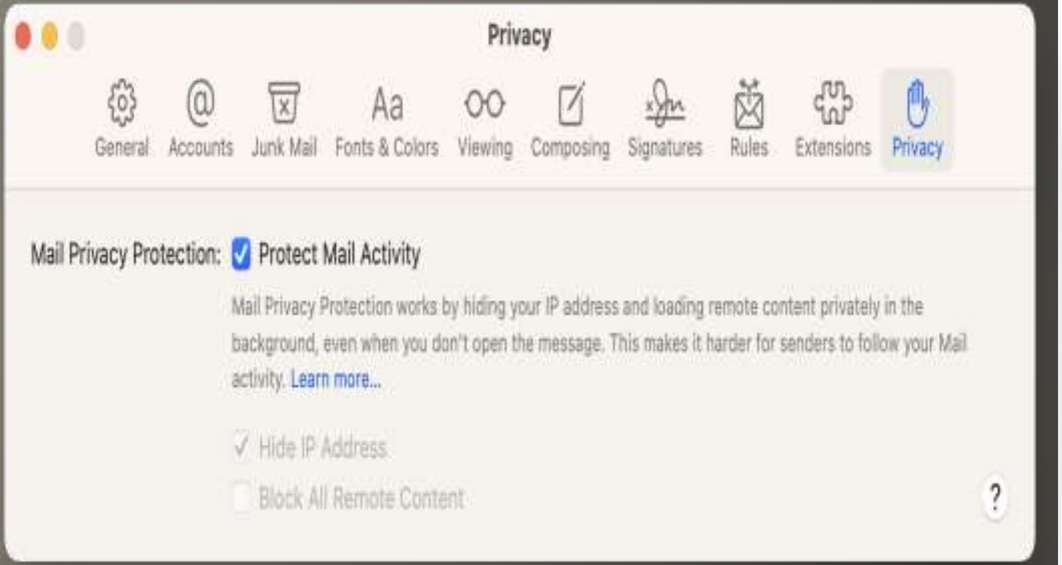
Mail Privacy Protection

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity.

Learn more...

● **Protect Mail activity** Hide IP address and privately load all remote content.

○ **Don't protect Mail activity** Show IP address and load any remote content directly on your device.



Mail Privacy Protection: ☑ Protect Mail Activity

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity. Learn more...

✓ Hide IP Address

□ Block All Remote Content

Apple Mail Protection

Apple Mail Privacy Protection

- Mail content downloaded in background
- Data rendered before user opens
- Multiple proxies
- IP address near recipient’s location

- Mail marketers

  Flawed A/B testing

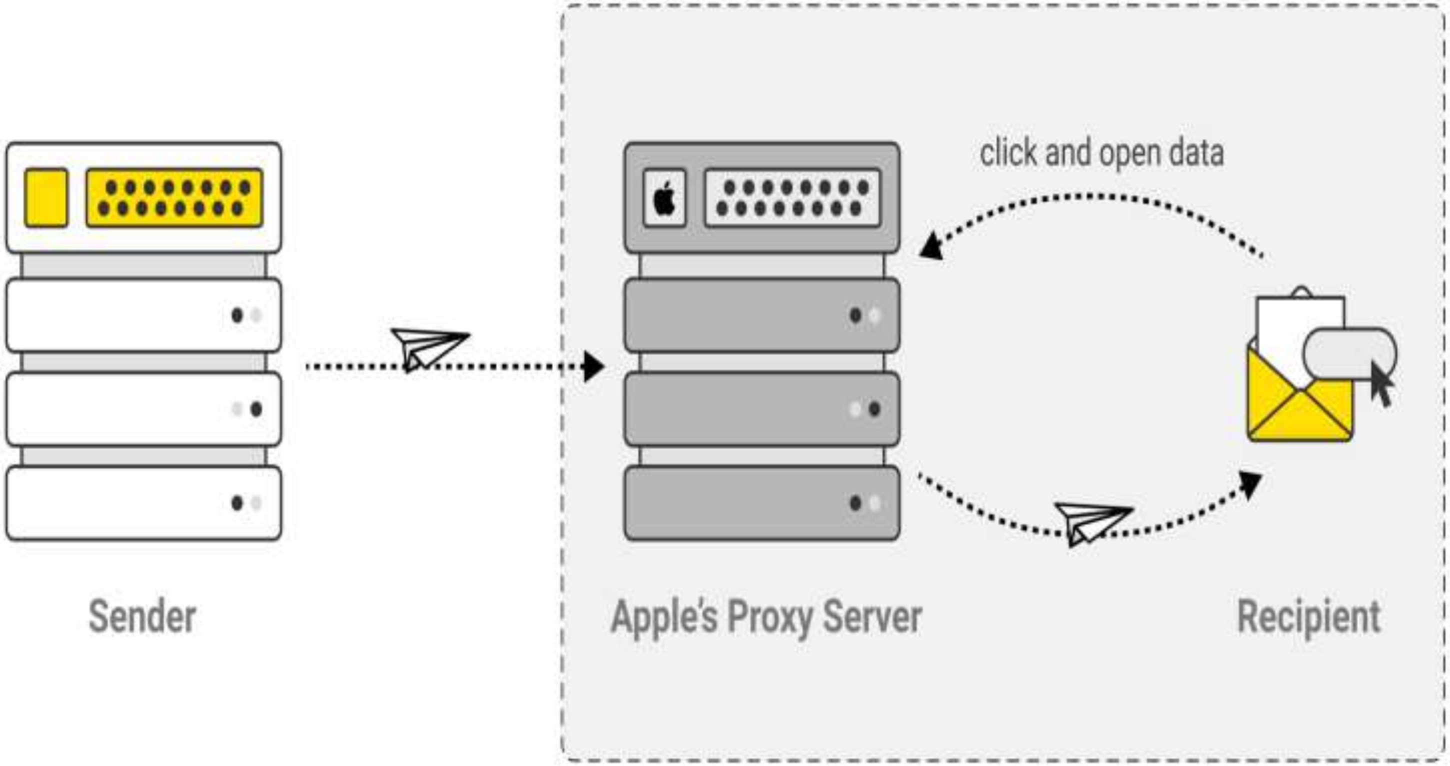
  Flawed send-time optimization

  Difficult track delivery

  Open rate

Postmark

How does Apple Mail Privacy Protection work?



Recipient activity is invisible to the sender

- 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