Sun City Computer Club

Cyber Security SIG

March 17, 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???

- Cyberattack tools
- "*They* will be after anybody"
- Internet – have a plan
- Cellular – have a plan
- ATM – have a plan
- Charging – have a plan
- Medications – stock up
- Enhance home network security
- Translate services
- Update Update Update
- They are after Me Anyone Everyone
- Awareness Preparedness Understanding

Hacktivism Protestware

Current Issues

- Microsoft Patch Tuesday
- Firefox
- Brave

  privacy vs. trackers, data brokers, ad tech vendors
- US executive order on digital assets
- Car salesman fraud
- TorGuard VPN banns BitTorrent
- Russian General tracked and killed

  After using unsecured cellular call
- Crystal City, Va. “Change Your Password”

  Traffic Walk signs
- Russian cybercriminal

  Arrested by Israel – 2015

  Russia fights extradition 4 years

  Arrest Russian woman to force prisoner swap failed

  Extradited – pleads guilty 9 year sentence

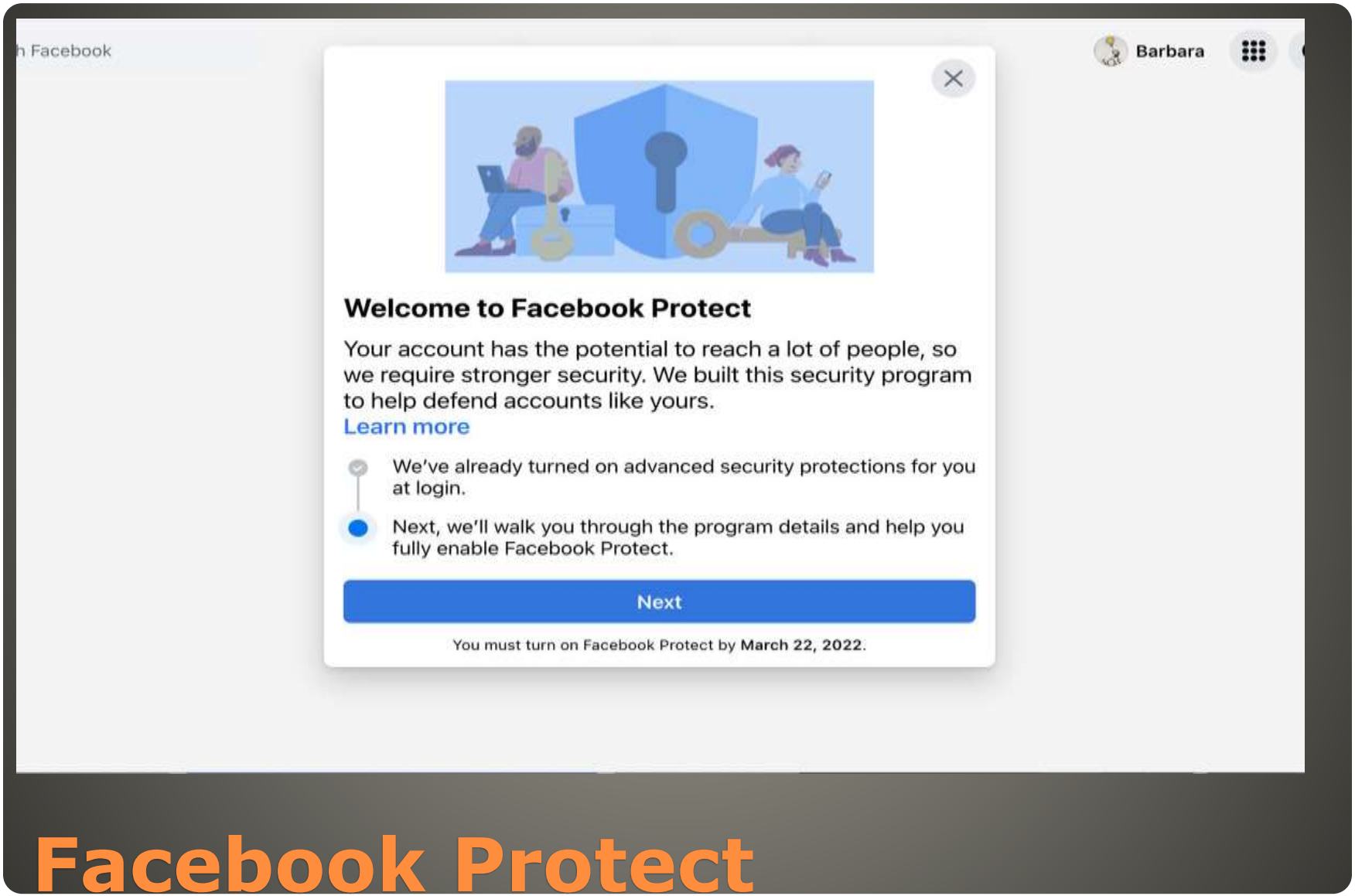
  less than 1 year - released and deported to Russia

  “asset of Great importance”

DON'T START
Finish Crossing
If Started
TIME REMAINING
To Finish Crossing
DON'T CROSS
TO CROSS
PUSH BUTTON

I NOTICED YOU DON'T BACKUP YOUR COMPUTER AT ALL
I TOO LIKE TO LIVE DANGEROUSLY
quickmeme.com

Microsoft
Office 2021
Professional Plus
Office Professionnel Plus 2021
Word
Excel
PowerPoint
Outlook
Teams
OneNote
Publisher
Access
1 PC
Windows
10/11
Transferable License
$559.99
$59.99
LIFETIME
LIMITED OFFER



Facebook Protect

Welcome to Facebook Protect
Your account has the potential to reach a lot of people, so we require stronger security. We built this security program to help defend accounts like yours.
Learn More
We've already turned on advanced security protections for you at login.
Next, we'll walk you through the program details and help you fully enable Facebook Protect.
You have [X] days left to turn on Facebook Protect
[Name], your account has the potential to reach a lot of people, so it requires stronger security. Facebook Protect, an advanced security program, helps defend accounts like yours. Learn more
Turn on Facebook Protect before 3 July 2021. After that, you'll be locked out of your Facebook account until you turn it on.
Advanced security that's always at work
More security at login to make sure that only you can access your account. Learn More
Regular security updates and proactive prompts when we launch something new. Learn More
To finish enabling Facebook Protect, we'll quickly check your account for vulnerabilities.

Facebook <security@facebookmail.com>
Wed 3/9/2022 9:54 AM
To: [redacted]

Facebook

Your account requires advanced security from Facebook Protect

[redacted]

Your account has the potential to reach a lot more people than an average Facebook user. Hackers are often motivated to attack accounts that have a lot of followers, run important Pages, or hold some community significance.

To help defend against these targeted attacks, we require Facebook Protect for your account.

⚠ Turn on Facebook Protect for your account by **17 March 2022**. After that, you will be locked out of your account until you enable it.

- We've already turned on advanced login protections for your account.
- To fully enable Facebook Protect, we'll check your account for vulnerabilities, and help you resolve them.

[redacted]

Turn On Facebook Protect

Ukraine Cyber Warfare

- Mutually Assured Disruption
- Ukrainian IT Army 175,000 subscribed
- Published target list
- NATO CCDCOE
  Cooperative Cyber Defense Centre of Excellence
- Cyber Patriots
- Cyber Hacktivism
- ContiLeaks
- Know and UnKnown
- StarLink
- Content - Control

Cyber Warfare

- Domain registrar to Russian registrants
  Move to another registrar
  yeahbut banks closed, no credit cards, …
- OK, some can

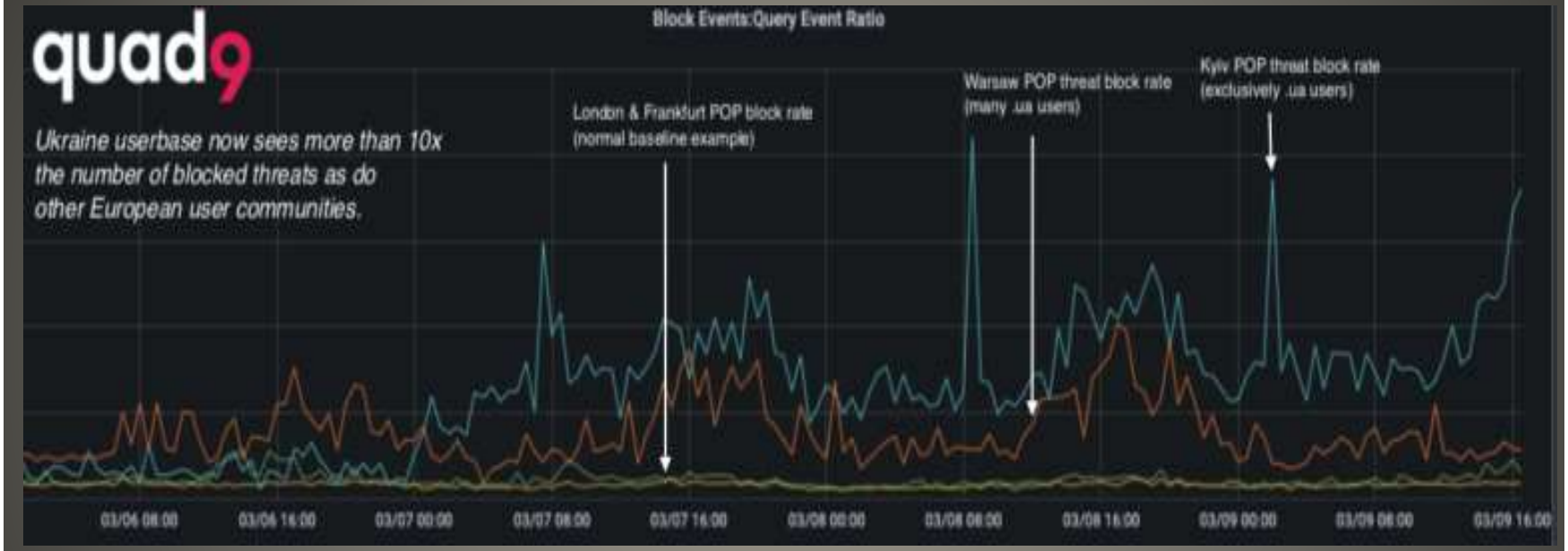
- Telegram six-fold increase
- Crypto currency wallet access

- Permit piracy

- Internet disconnect?

- Escalation in microseconds

- 10 X increase



Cyber Warfare Russia Ukraine

Current Issues

- Zelle
  Immediacy Helpful <-> Harmful
  Fraud recovery
  Regulation E
  recovery of *unauthorized* transactions
- Soli
  Google Nest Hub
  radar privacy friendly?
  vs camera works in dark, temperature
  Hidden

Current Issues

- "Alexa, hack yourself"
  wait … confirm
  Bluetooth thru the window
- USPS master key theft Leander
- Intel Bitcoin mining chip
  BMZ2 Bonanza Mine ASICs
  95% increase
- Drilling for gas - auto gas tank
  Locking gas caps
- Electronic Safety Sign hacked
  Maryland State Police One week
- Indian missile into Pakistan

Current Issues

- US Critical Infrastructure
  Bill passed 3/10/2022
  "substantial cyber incident" 3 days
  ransom paid 24 hours
- Leak of Russian censorship data
  Roskomnadzor
- NVIDIA breach
  Employee data Code signing certificates
- Privacy email providers and Russian users
  Usage and subscription payments
- Russian sites and certificate renewal
- Russian CA added to trust chain
- Chinese state-sponsored actors breached 6 US stage governments
  using US Animal Health Emergency Reporting Diagnostic System vulnerability

- Free movies
- Images not in public domain
- Bypassing paywalls
- Sharing credentials
- Downloading YouTube videos

Legal NoNos

- Covid vaccine record card
- Driver’s License & ID
- Auto License Plate, VIN, Auto Insurance
- Medical & Dental card
- Medicare Cards
- Rent car Before & After
- Vacation Rental Before & After

Photos on Smart Device Camera

- Apple Updates EVERYTHING

SCCCCyber

Monday, March 14, 2022

Apple Updates

iOS15.4

iPadOS 15.4

macOS 12.3

watchOS 8.5

tvOS 15.4

XCode 13.3

Logic Pro X

GarageBand 10.4.6

HomePod 15.4

Cyber Security News Archive

Cyber Security News Archive

- Safari 15.4 (17613.1.17.1.6)
- Edge 99.0.1150.39
- Edge 100.0.1193.0
- Chrome 99.0.4844.74
- Brave 1.36.116
- Opera 84.0.4316.42
- Tor 11.0.7
- Vivaldi 5.1.2567.66
- Firefox 98.0.1

Browser Updates

Updates

- Chrome OS 99.0.4844.57
- Linux Dirty Pipe
  - Worst since Dirty Cow
  - CVE-2022-0847
  - Any User (even nobody)
  - Add root SSH key
  - Hijack SUID binary
  - Write to read-only files
  - root cron job
  - and more …
  - yeahbut I don’t run Linux

UMMMM Android and Android based

- Windows Update Tuesday
  71 flaws 29 Remote Code Execution
  25 elevation of privilege
  6 Information disclosure
  4 denial of service
  3 security feature bypass
  3 spoofing vulnerabilities
  Edge browser 21 issues fixed
- Android a “no user interaction” vulnerability
- Firefox Chrome Chrome OS
- BIOS UEFI CVSS 9.8

Patch

- Intel & AMD
- Inadequate
- And 54% performance hit
- Linux 5.17 delayed

Spectre V2

QR codes

- QR codes easy TOO Easy?
  Send Money, Open website, Open App
  Trusted source
  Check Site's URL, Certificate, Reputation, etc.
  Check for sticker, look-a-like duplicate,
- Parking meters
- Stealing bicycles
- TREAT LIKE UNKNOWN LINKS

Microsoft Family Safety

Microsoft Corp. • Kids & family

Microsoft Family Safety – now available to Windows Insiders!

The Microsoft Family Safety app helps empower you and your family to create healthy habits and protect the ones you love with digital and physical

More

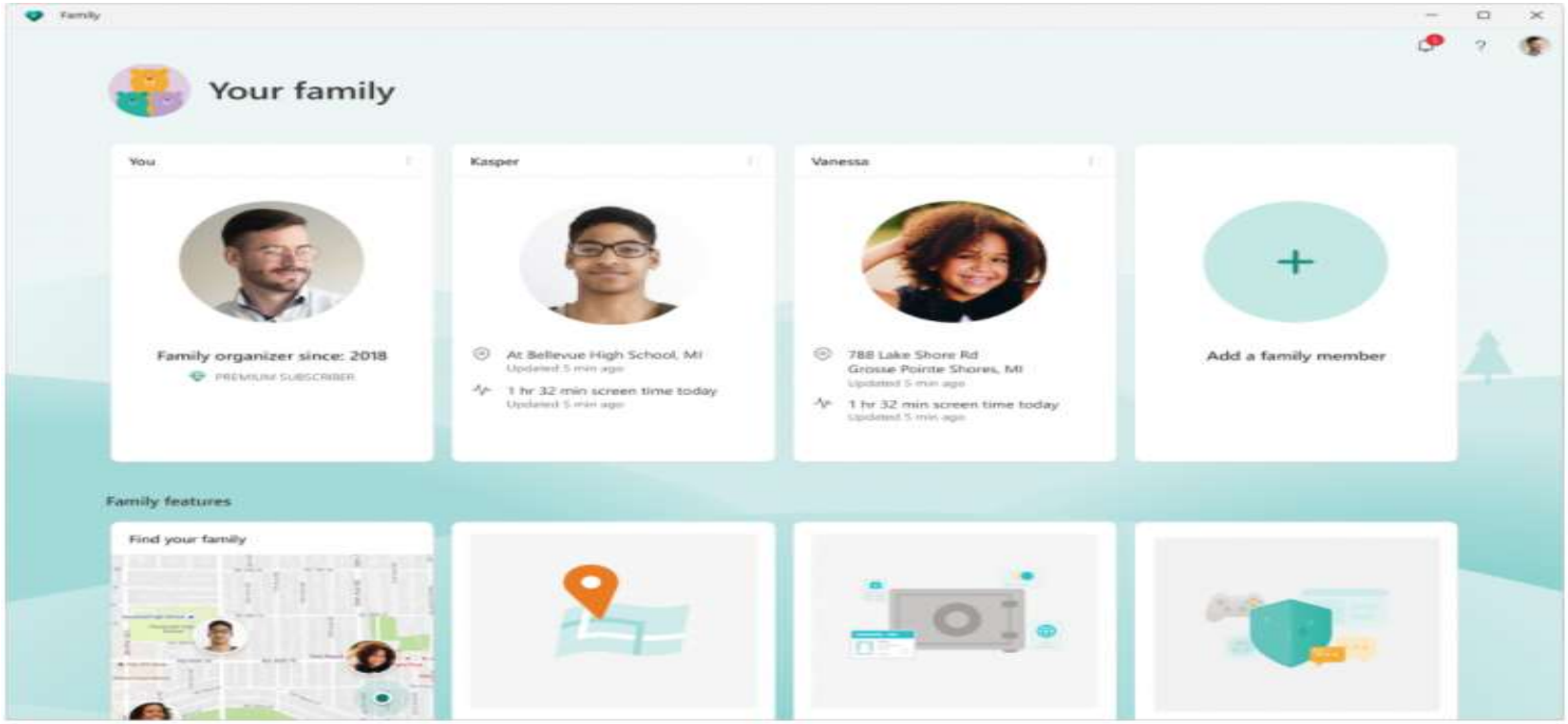
EVERYONE
In-App Purchases

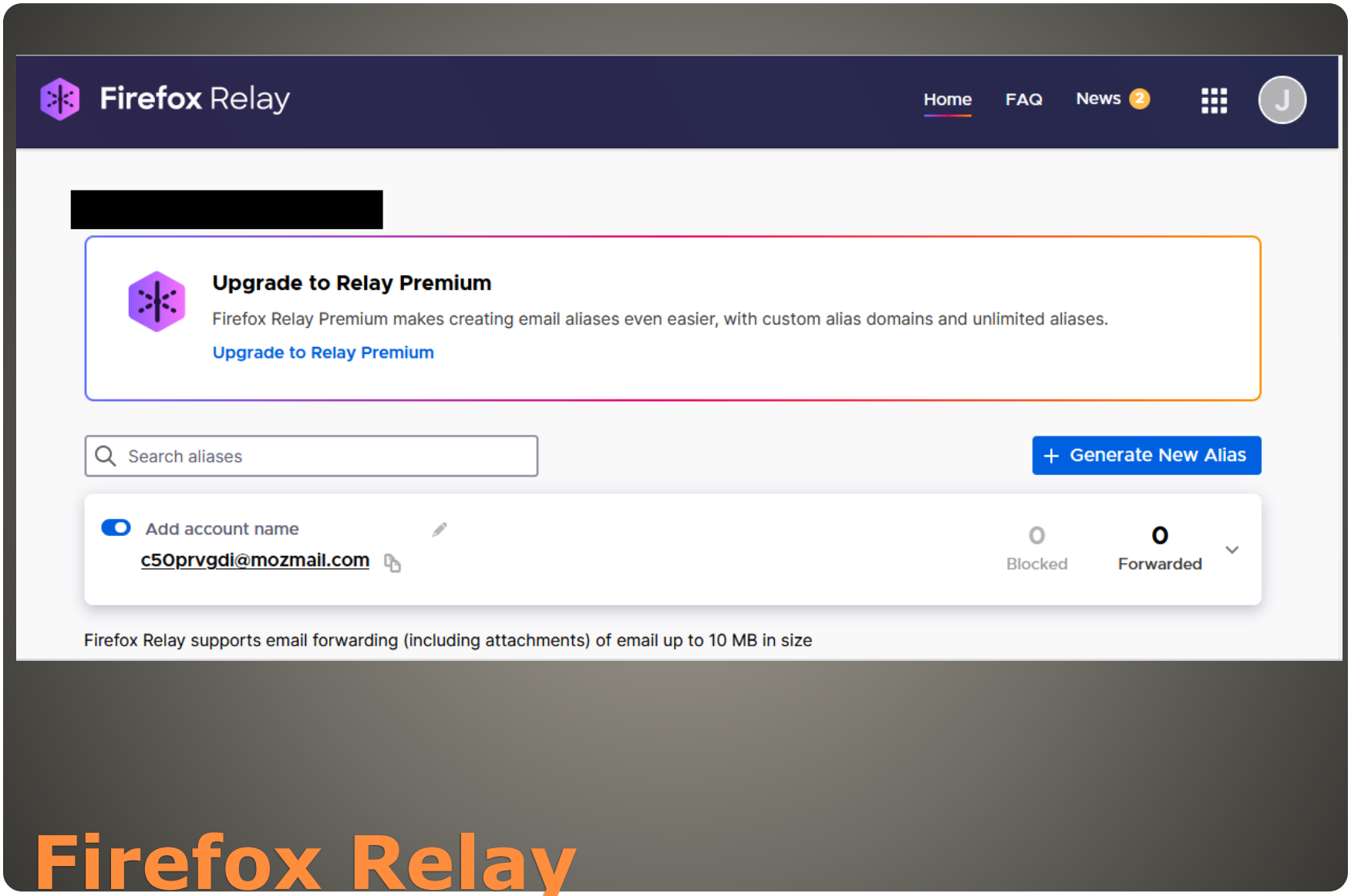
Free

Get

+ Offers in-app purchases

See System Requirements





Firefox Relay

ORDER HERE
Order Here
Safety
32

- 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