Sun City Computer Club

Cyber Security SIG

May 19, 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???

Who is this guy?

- John Jenkinson
- 1962 first computing job first hack
- 1964 ARPA contracts
- 1966 US Army
- 1971 BS Physics 1975 BS Math 1978 MS Computer Science
- 1974 Mostek
- 1983 -> 2016 Big oil
- Cyber security focus, training, certifications, consulting
- FBI InfraGard DHS Critical Infrastructure US-CERT
- Mensa

- Safer not Safe
- E-Postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio Not wireless
- Internet is vital Internet is vulnerable

Vocabulary

Current Issues

- Blast from Past
  - Alaska telecom provider
  - 7+ years later
  - Un paid bill
  - New billing system mistake
  - 7+ years later
- Microsoft Security Experts
  - Billions blocked
  - “We’re Microsoft, we are here to help”
- Spain’s spy chief fired
  - Pegasus fall out

Current Issues

- https://americandragnet.org/
  Immigration and Customs Enforcement
  50 miles from border
  seize electronic equipment
  Fifth amendment protections
  Passwords NOT biometrics
  passkey

Passkey

- The major players
  Apple, Microsoft, Google
  May 5 Password Day
  passphrase, please
  committed to build passwordless authentication
  Phones or smart devices
  PIN, drawing pattern, fingerprint, facial ID, etc.
  Simplicity & security
  Password capture

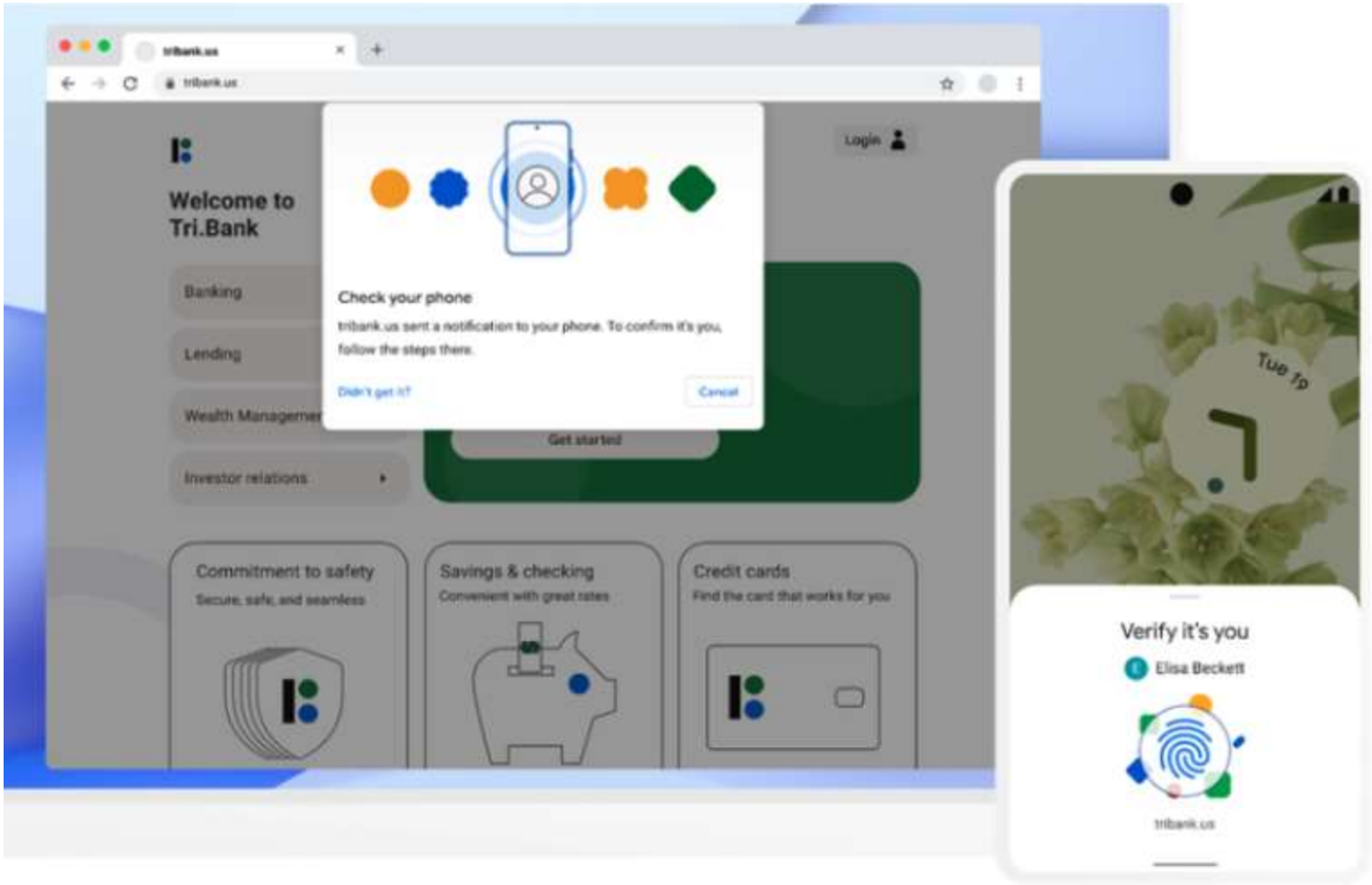
Yeahbut lose THE device …

User Experiences with Multi-device FIDO Credentials

Allow users to automatically access their FIDO sign-in credentials (referred to by some as a "passkey") on many of their devices, even new ones, without having to re-enroll every account.

Enable users to use FIDO authentication on their mobile device to sign-in to an app or website on a nearby device, regardless of the OS platform or browser they are running.

AT&T Wi-Fi
1:52 PM
76%
Authenticator
GUN
[redacted]
Approve sign-in?
GUN
[redacted]
Deny
Approve
Authenticator
Passwords
Addresses


tribank.us
Login
Welcome to Tri.Bank
Banking
Lending
Investor relations
Get started
Check your phone
tribank.us sent a notification to your phone. To confirm it's you, follow the steps there.
Didn't get it?
Cancel
Commitment to safety
Secure, safe, and seamless
Savings & checking
Convenient with great rates
Credit cards
Find the card that works for you
Verify it's you
Elisa Beckett
tribank.us

- Easily forgotten
- Frequently stolen by malware & phishing
- Leaked
- Stolen
- Data breaches

passwords

- FIDO W3C
- Sign-in with Google | Facebook
- Secure enclave

Wait

- Lost phone
- Recovery from cloud backup

passkey

Current Issues

- DCRat $5.00
- Suggested Actions Windows Dev channel
- Chrome
  Topics -> Federated Learning of Cohorts
  FLEDGE
  First Locally-Executed Decisions Group Experiment
  Chrome not Chromium
  DuckDuckGo Privacy Essentials
- PayPal scam $3000+ loss
  create PayPal account using stolen Identity
- Car key fob metal tray

- San Francisco police using autonomous vehicles for surveillance

Current Issues

- Self Defense Club Self & Home Security
  Cybersecurity Risks and Scams
  Outdoor Surveillance Cameras
  Williamson County Sheriff
  CA Community Standards Director
    Safety Procedures
  GPD Security, safety & Protection Devices
  Safety on the Sun City Trails

Other Sun City Resources

Sun City Texas Community Association

NRO Anti-Fraud Group

How to identify and stop fraud in transactions and communications

« ALL CLUBS
« NRO
GROUP MEMBERS
CALENDAR
PHOTO ALBUMS
MEETING AGENDAS AND MINUTES
ALERTS
ANTI-FRAUD HANDBOOK
SCAMS AND FRAUDS
REQUEST A FRAUD PRESENTATION
PRESENTATIONS

POWERPOINT SHOWS

Get Involved – Stay Safe	View | Download
Common Scams	View | Download
How to use the Anti-Fraud Webpages	View | Download

To view, you will need Adobe Acrobat Reader.

RESIDENT HOME | LIFESTYLE & ACTIVITIES | CLUBS & NEIGHBORHOODS | FITNESS

Sun City Texas Community Association

NRO Anti-Fraud Group

How to identify and stop fraud in transactions and communications

My Profile | Account Statements | Resident Directory | My Neighborhood | My Memberships

« ALL CLUBS
« NRO
GROUP MEMBERS
CALENDAR
PHOTO ALBUMS
MEETING AGENDAS AND MINUTES
ALERTS
ANTI-FRAUD HANDBOOK
SCAMS AND FRAUDS
REQUEST A FRAUD PRESENTATION
PRESENTATIONS

ALERTS

20220412HOWDOYOUSPOTASCAM	View | Download
CON-GAMES-FRAUD-SCAMS-1.PDF	View | Download
CREDIT CARD INTEREST RATE REDUCTION	View | Download
FRAUD ALERTS	View | Download
FRAUD AND OLDER ADULTS	View | Download
GIVING TO CHARITY	View | Download
HOW TO AVOID A SCAM FTC CONSUMER INFORMATION	View | Download
IDENTITY THEFT	View | Download
INTERNET FRAUD FBI	View | Download
TOP FRAUDS OF 2021	View | Download

RESIDENT HOME | LIFESTYLE & ACTIVITIES | CLUBS & NEIGHBORHOODS | FITNESS

Sun City Texas Community Association

NRO Anti-Fraud Group

How to identify and stop fraud in transactions and communications

My Profile | Account Statements | Resident Directory | My Neighborhood | My Memberships

« ALL CLUBS

« NRO

GROUP MEMBERS

CALENDAR

PHOTO ALBUMS

MEETING AGENDAS AND MINUTES

ALERTS

ANTI-FRAUD HANDBOOK

SCAMS AND FRAUDS

REQUEST A FRAUD PRESENTATION

PRESENTATIONS

HANDBOOK

Anti-Fraud Handbook — View | Download

To view, you will need Adobe Acrobat Reader.

NRO Anti-Fraud Handbook

Version 2.0
May 2022

"Sun City does not vet or endorse any resource or service provider in this handbook. Each resident should perform their own due diligence before choosing any service provider. This handbook is solely a compilation of resources and information to help residents deal with life challenges and maintain or improve their ability to recognize fraud and prevent becoming a victim.

Financial exploitation has been called "the crime of the 21st century" with one study suggesting that older Americans lost at least $2.9 billion to financial exploitation by a broad spectrum of perpetrators, including persons they know and trust, as well as strangers. Cognitive impairment diminishes the ability of some older adults to make financial decisions and to detect frauds and scams.

This epidemic is under the radar. The cases tend to be very complex and can be difficult to investigate and prosecute. Elders who lose their life savings usually have little or no opportunity to regain what they have lost. Elder financial exploitation can result in the loss of the ability to live independently. It can also result in a decline in health, broken trust, and fractured families.

Awareness is the first step. Planning ahead for financial wellbeing and the possibility of diminished financial capacity is critical. Reporting and early intervention are vital to preventing loss and recovering loss when possible."

Residents may refer to the numerous internet links in the PDF version of this document (NRO ANTI-FRAUD HANDBOOK) for additional resources.

Community Association, Sun City Texas

Sun City Texas Community Association

NRO Anti-Fraud Group

How to identify and stop fraud in transactions and communications

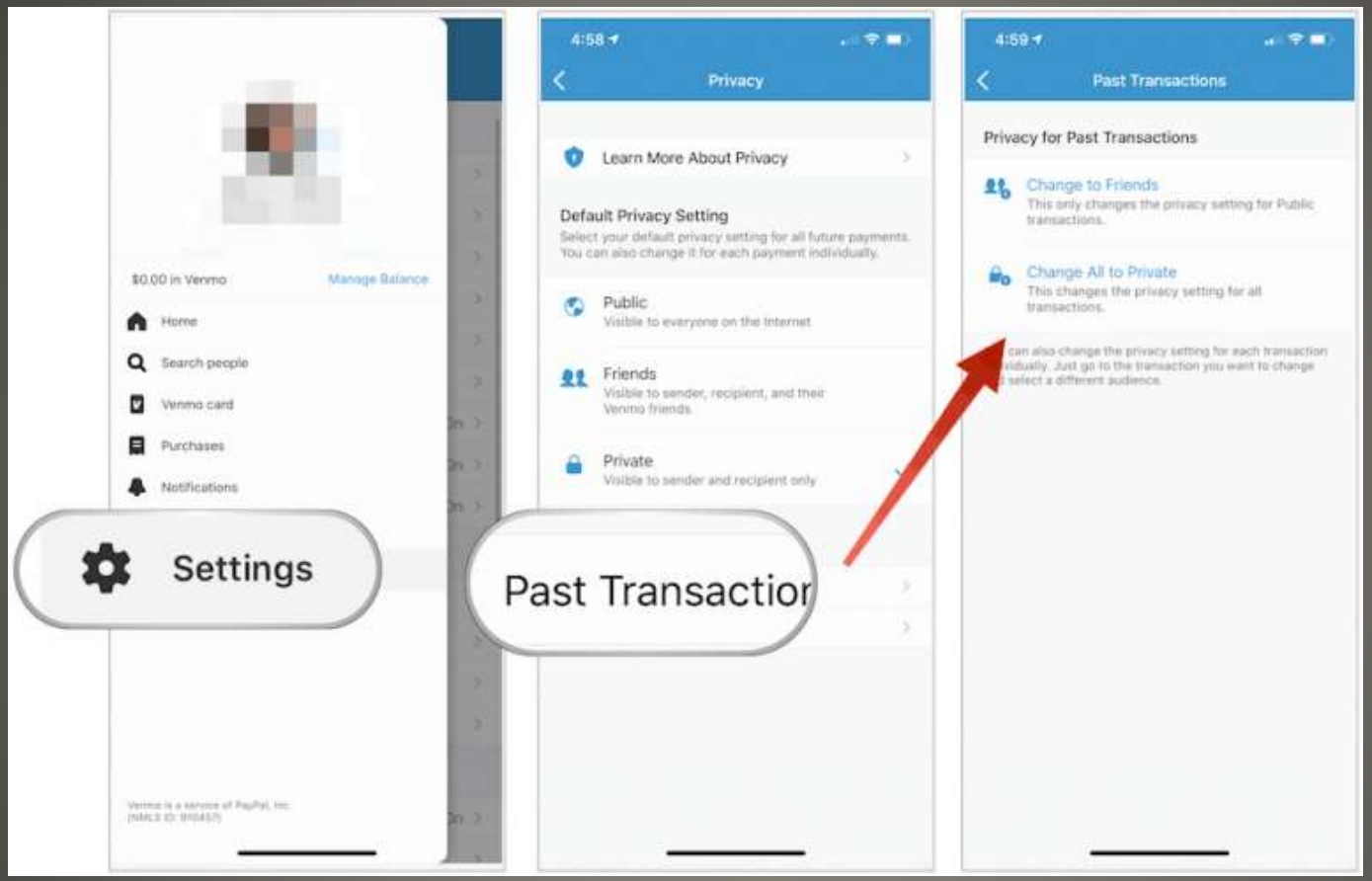
« ALL CLUBS
« NRO
GROUP MEMBERS
CALENDAR
PHOTO ALBUMS
MEETING AGENDAS AND MINUTES
ALERTS
ANTI-FRAUD HANDBOOK
SCAMS AND FRAUDS
Grandparent Scams
Investment/Securities Scams
ID Theft
Credit Card Scams
Romance Scams
REQUEST A FRAUD PRESENTATION
PRESENTATIONS

SCAMS AND FRAUDS

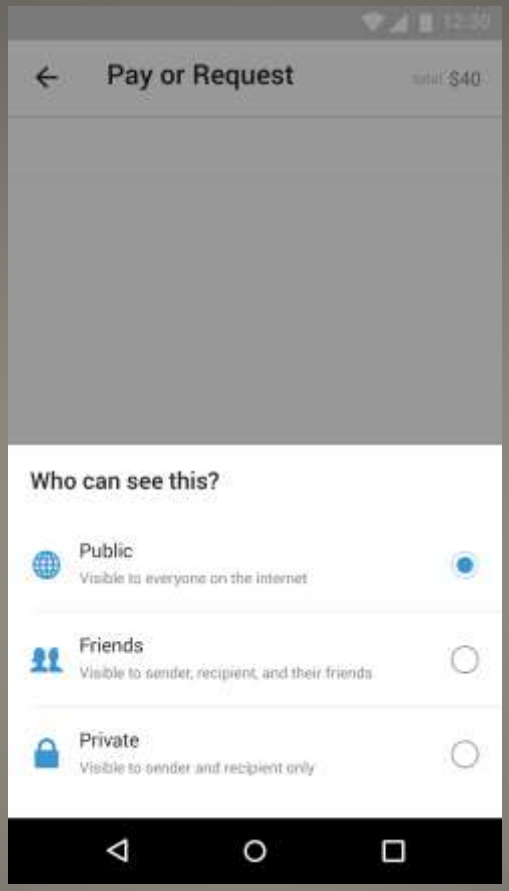
- Zelle
  Bank Account – Bank Account
  Routing and Account Numbers !
  Payment limits
  lack of fraud protection
  No bank card
  No middleman
  No requirement for recipient to use Zelle
  No Fees

- Venmo
  - Social
  - Smart Phone oriented
  - Social by default
- PayPal
  - Secure International payment
  - Online Shopping
  - Buyer protection

- Google Pay
  Quick contactless merchant payments
  Loyalty cards
  Transit tickets
- Wise
  Real exchange rates
  SWIFT/BIC and IBAN
- Cash App
  Stocks & Bitcoin
- Apple Pay


$0.00 in Venmo
Manage Balance
Home
Search people
Venmo card
Purchases
Notifications
Settings
4:58
Privacy
Learn More About Privacy
Default Privacy Setting
Select your default privacy setting for all future payments. You can also change it for each payment individually.
Public
Visible to everyone on the Internet
Friends
Visible to sender, recipient, and their Venmo friends
Private
Visible to sender and recipient only
Past Transactio
4:59
Past Transactions
Privacy for Past Transactions
Change to Friends
This only changes the privacy setting for Public transactions.
Change All to Private
This changes the privacy setting for all transactions.

Venmo


Pay or Request
$40
Who can see this?
Public
Visible to everyone on the internet
Friends
Visible to sender, recipient, and their friends
Private
Visible to sender and recipient only

Venmo

Current Issues

- NIST “No known flaws”
  Quantum-Resistant Algorithms
- DEA investigating data breach
  Law Enforcement Portal
- Reminder – even before you enter Enter
  or similar action
- Sysrv-K botnet
- Getting back at SPAM callers

https://www.komando.com/video/komando-picks/getting-back-at-scam-callers/837688/

WARNING!! Do NOT ATTEMPT

Old and forgotten

- You've dis-remembered
- Attacker finds, gets password reset or info from data breach
- MySpace
- Old but verifiable information
  - Postal mail addresses, old phone numbers, etc.
- Old providers ISP, dentists, Kmart, …

iDevice Low Power Mode

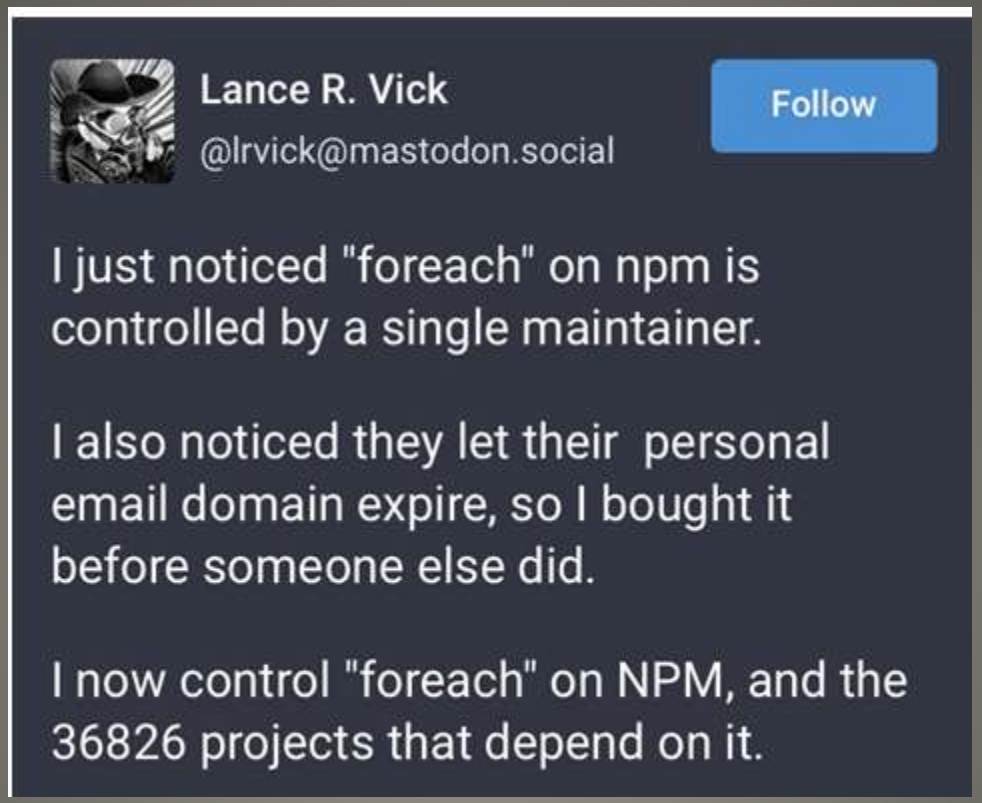
- No OFF - battery not easily removed
- Find My – needs power
- Bluetooth, NFC, UWB chips
  Power for Find My
  Power for Express Card transactions
  Thus wired to Secure Enclave
- Bluetooth, NFC, UWB firmware not signed

Current Issues

- Amazon shopping with Edge?
  Discount coupon
- Apple employees “tap-to-pay”
- Scan / photo sensitive documents into Secure note - Not camera roll / photos
- Photos GPS Helpful<->Harmful
- Smart ID Card reader
  Personal Identity Verification
  USB Common Access Card
  Update VirusTotal

United States Government
FEB2013
SAMPLE
Uniformed Services
Marine Corps
2013FEB01
DOE, JOHN Q.
E6
SSGT
Geneva Conventions Identification Card
EXPIRATION DATE
FEDERAL IDENTIFIER
AFFILIATION
SERVICE/AGENCY
COLOR INDICATION
PAY GRADE
RANK
INTEGRATED CIRCUIT CHIP (ICC)
SAMPLE
1961FEB01
1401770611
BLOOD TYPE
DoD BENEFITS NUMBER
GHOST IMAGE
DATE OF BIRTH
GENEVA CONVENTION CATEGORY
DoD IDENTIFICATION NUMBER (ALSO USED AS THE GENEVA CONVENTIONS NUMBER)

This Slide intentionally blank



npm repository Node.js projects

A

Apple Updates EVERYTHING

Published • May 16

M

Mozilla releasing Out-of-Band update for Firefox Browser

Published • May 16

Yet Another IMPORTANT Update for Google Chrome Browser 11-May-2022

Published • May 11

G

Google releases Android Update May 5, 2022

Published • May 8

N

New Ability to request removal of Personally Identifiable Information from Googl...

Published • Apr 28

M

MUST UPDATES for Java

Published • Apr 27

A

Apple Beta

Published • Apr 26

M

Microsoft Windows Cumulative Update Previews available today April 26

Published • Apr 26

A

Android Remote Execution Flaw

Published • Apr 25

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

Current Issues

- Google Android update 37 flaws
- US offering $10M for information Conti
  Costa Rica government
  customs & taxes - new administration
  Ireland Health Service
- APT 41 "CuckooBees" 60 minutes
  FBI Director well hidden long persistence

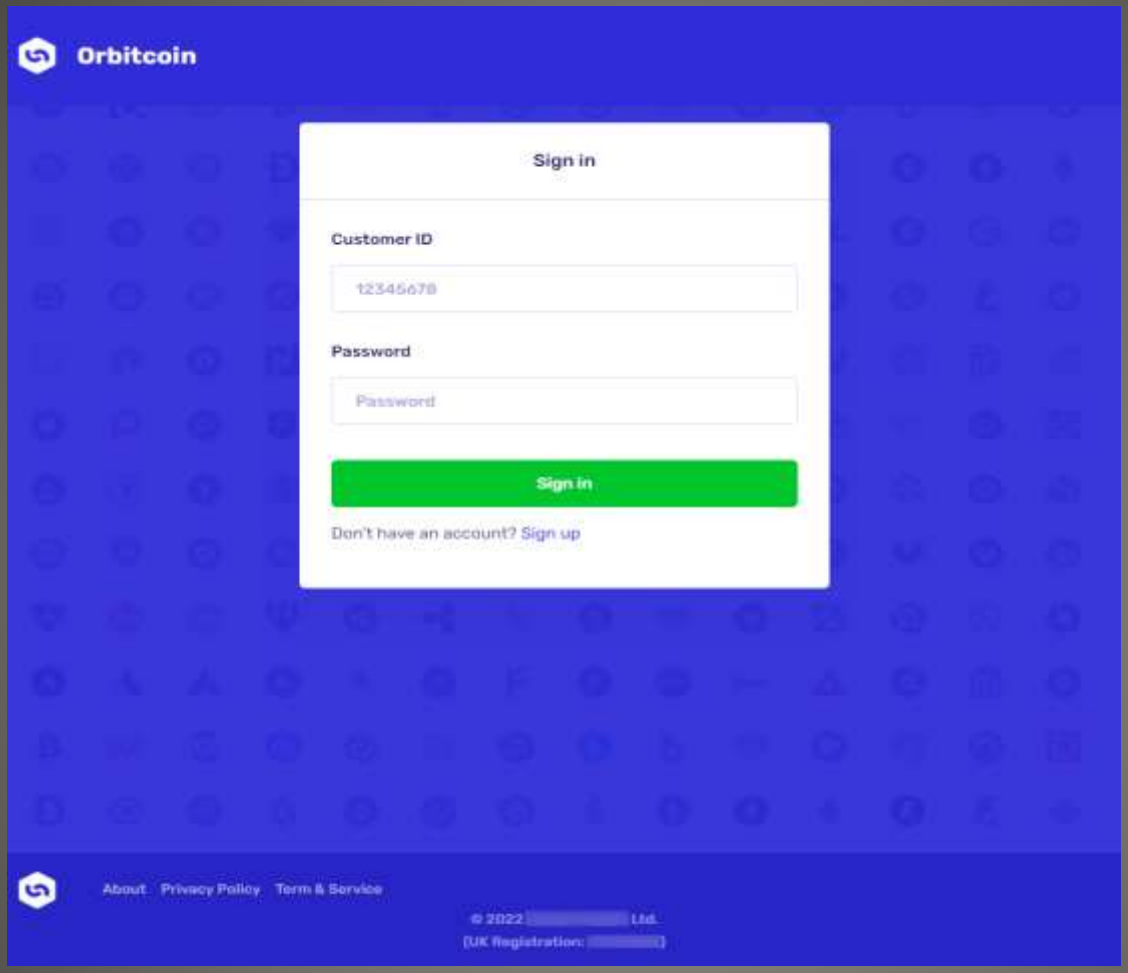
Passkey

- FIDO W3C WebAuthn
- Smartphones roaming authenticator
  BUT subject to phishing
  switch web sites
  cloud synched passkeys
  TBD

From: BTC <info@yahoo.com>
Sent: Thursday, May 12, 2022 8:33 AM
To: Recipients <info@yahoo.com>
Subject: BTC Payment

Hi Rob Hoffman, As requested, we have now deposited 30 BTC which amount to ($919,914.30 USD) into your bitcoin portfolio at https://www.orbitcoin.net/signin Customer Id: 71452874, Password: EF978peb

YAN Scam - Bitcoin style



YAN Scam – Bitcoin style

- AH Got in - to another individual's account
- I see the 50 bitcoin
- Site forces password change, SMS MFA
- Then transfer attempts get

YAN Scam – Bitcoin style

YAN Scam – Bitcoin style

- OK, I'll transfer to my wallet
- "Sorry first transfer can be no more than 0.00001BTC, security reasons"
- Transfer appears to be done, confirmed
- Now transfer the 50BTC, please
- "Sorry 30BTC is minimum transfer limit."
- For a minimum transfer in I can get a good bit if bitcoin from a stranger's wallet

- SCAM

Passwords

- Passphrases
- Password theft
- Password guessing
- Password hash theft & cracking
- Unauthorized password reset / bypass

- Password manager
- Strong & Unique passwords
- Guard & Monitor those passwords

- 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