# RANSOMWARE & OTHER CYBER THREATS PLAGUING KŪPUNA

Al Ogata
President & CEO
September 22 & 23, 2023

CYBER HAWAII

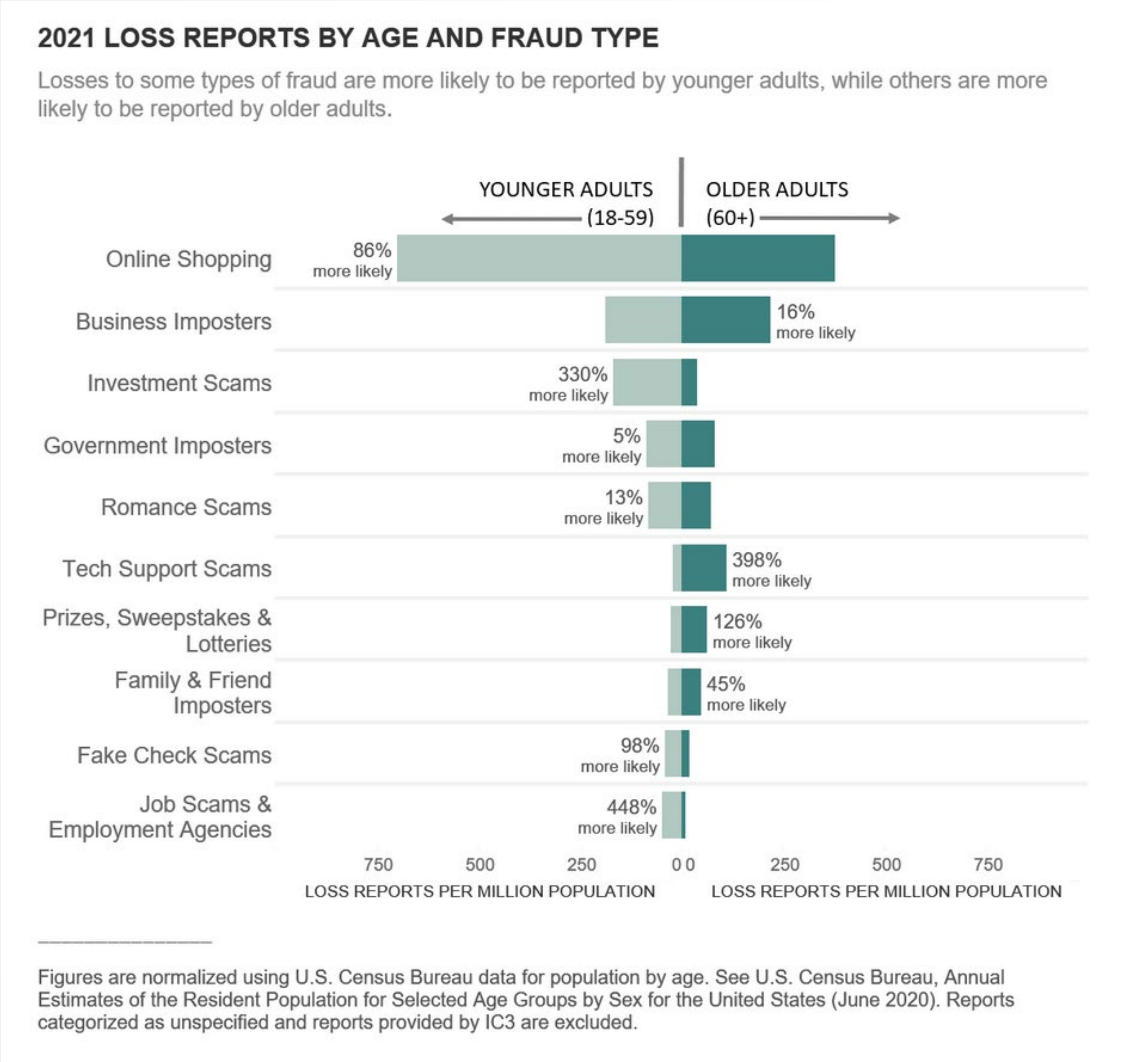
# ABOUT CYBERHAWAII

CyberHawaii is an information sharing and analysis non-profit organization committed to developing and enhancing Hawaii's cybersecurity capabilities

- CyberHawaii is committed to a whole community approach that will help to:
  - Mitigate cyber risks for all community members
  - Develop educational and workforce pathways for students
  - Augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations
  - Inform local decision makers about cyber security risks and solutions
- Founded 2016
- Part of CyberUSA network
- www.cyberhawaii.org

CYBER HAWAII

# EFFECTIVE SCAMS VARY BY AGE



**2021 LOSS REPORTS BY AGE AND FRAUD TYPE**

Losses to some types of fraud are more likely to be reported by younger adults, while others are more likely to be reported by older adults.

Figures are normalized using U.S. Census Bureau data for population by age. See U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020). Reports categorized as unspecified and reports provided by IC3 are excluded.

- Gen Xers, Millennials, and Gen Z young adults were 34% more likely than older adults to report losing money to fraud
- Median loss much higher for older adults
  - $1,500 for those 80 and over
  - $800 for people 70-79
  - $500 for people 18-59
- Kūpuna more likely to report failed scams

Source: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages

# RANSOMWARE

## Characteristics

- Encrypts data files
  - Unbreakable (256 AES)
- Reusable
- May rename files
- Organization notified when open encrypted file
- Payment is in crypto currency
  - Receive encryption key
  - Receive promise not to disclose data
- Business decision whether to pay or not (except if national security involved)
- Payment may be to sanctioned organizations

## Prevention

- Do not click on suspicious links or download files from unknown sources
  - Email, text, website as sources
- Perform regular backups of critical data
  - Keep backup devices offline when not in use
  - Do not enable automatic backups to the cloud

## Mitigation

- Isolate infected systems from the internet
- Remove malware
- Notify affected friends, family clients, staff and regulatory agencies
- Notify FBI
- Restore from backups or decide if going to pay ransom

*Image source: BleepingComputing*

CYBER HAWAII

# TECH SUPPORT SCAMS

## Characteristics

- You receive a notice that something is wrong with account or device
  - Phone call, email, text message
  - Pretend to be from known company
- Immediate action required
  - Don’t talk to anyone else
  - Only they can help you
- Request to access computer
  - Download “clean up” software
  - Establish remote access
- Request for initial funds
  - Clean up of files
  - Bait to trap hackers
  - Administrative/regulatory fees
  - Pay to monitor computer
- Request for Additional funds

## Prevention

- Do not respond to notices that there’s something wrong with your computer
  - Third party vendors do not have any way of legitimately knowing this
- If your computer or phone is acting unusual, check directly with the manufacturer, the organization you bought it from, or a recovery organization you trust
  - Do not trust a person or organization you don’t know or can’t independently verify

## Mitigation

- Stop paying any requested fees; check with bank or credit card company to see if payments can be stopped
- Isolate infected systems from the internet
- Remove malware; or
- Reinstall operating system and/or applications (i.e., restore to a clean version); or
- Buy a new computer or device

# PRIZES, SWEEPSTAKES, LOTTERIES

## Characteristics

- Receive a notice that have won global sweepstakes
  - Phone call, email message
  - Prize only redeemable if the "winners" send money to cover insurance and other fees
  - Forged documents involved
- Calls masked to appear to be from local area code
- Money must be wire transferred
  - Very short period of time to recover funds
- Additional call that their prize has increased so need to send more for taxes and other fees

## Prevention

- Do not respond to unknown prize notifications
  - Keep track of legitimate contests you enter; follow up directly with organizers
- Don't  get talked into forgetting you entered or that someone else entered on your behalf

## Mitigation

- Contact your bank immediately to try and stop payment
- Contact the FBI
- Talk to family about how to prevent in future
- Be honest with yourself

# SOCIAL/FAMILY SCAMS

## Characteristics

- Romance scams target loneliness
  - Build trust, then request $'s
  - Fake backgrounds
  - Recurring threat
- Ransom of family members
  - Typically uses social media data
  - Kidnapping, arrest, threat of harm
  - Family member not in danger
- Voice impersonation using AI
- Invokes sense of urgency & panic
  - Don't call others
  - Get immediate payment (cash cards or wire transfers)

**Prevention**

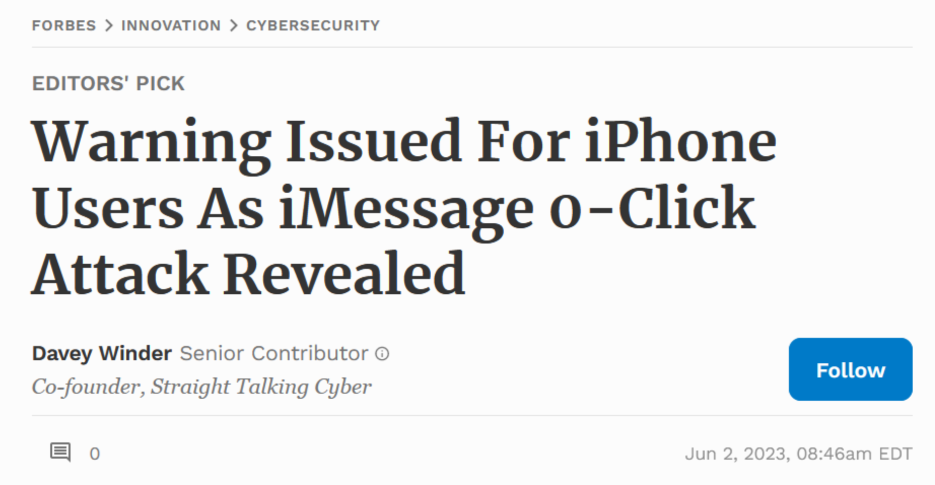
- Maintain strong social network you can trust
  - Refrain from fully trusting online only friends
  - It's normal to need someone you can talk to
- Anyone can be scammed; nothing to be ashamed of
- Go out of band to validate threats
- Have "secret" word to validate identity
- Avoid putting current travel info on social media

**Mitigation**

- Pause initial contact & and connect with someone you trust
- Do not give direct access to bank accounts
- Delay paying
- Contact police or FBI

# APPLE ATTACKS

- Apple mobile devices being attacked more frequently
  - Out of band patches becoming more common
- Common threats
  - Spyware
  - Hijack device
  - Modify/extract files
- 0-click Malware
- Good practices
  - Reboot mobile device periodically
  - Keep up to date on patches
  - Apple optional Lockdown Mode



FORBES > INNOVATION > CYBERSECURITY

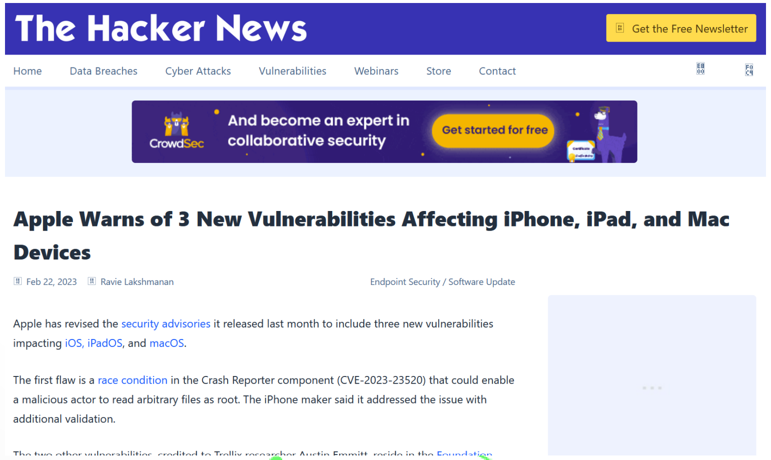
EDITORS' PICK

## Warning Issued For iPhone Users As iMessage 0-Click Attack Revealed

**Davey Winder** Senior Contributor

*Co-founder, Straight Talking Cyber*

Jun 2, 2023, 08:46am EDT



## Apple Warns of 3 New Vulnerabilities Affecting iPhone, iPad, and Mac Devices

Feb 22, 2023 Ravie Lakshmanan Endpoint Security / Software Update

Apple has revised the security advisories it released last month to include three new vulnerabilities impacting iOS, iPadOS, and macOS.

The first flaw is a race condition in the Crash Reporter component (CVE-2023-23520) that could enable a malicious actor to read arbitrary files as root. The iPhone maker said it addressed the issue with additional validation.

The two other vulnerabilities, credited to Trellix researcher Austin Emmitt, reside in the Foundation

# SECURITY FOR SMALL BUSINESSES

- Understand assets & value if lost
  - Customer information
  - Family information
  - Trade secrets
  - Physical inventory
  - Business reputation
- Focus on Key Controls
  - Security Leadership
  - Password Management
  - Access Control
  - Data Management (including mobile & removable access)
  - Patch Management
  - Regular training (and Testing)
- Develop action plan for responding to & surviving an attack

CYBER HAWAII

# PHYSICAL INDICATORS OF COMPROMISE

- Change in Computer Performance
  - Slow performance
  - High CPU usage
  - Unusual hard drive activity
  - Unexpected crashes
  - Unusual network activity
- Change in Settings
  - Browser settings
  - Disabled security software
  - Firewall settings
- Change in Behaviors or Software
  - Unexpected computer activity
  - Unexpected email behavior
  - Unwanted pop-ups
  - New or unfamiliar programs
  - Unauthorized access or account activity
  - Disappearing files

CYBER HAWAII

# SUMMARY

- Everyone can be a victim of a scam – but Kūpuna can be especially vulnerable
- Specific scams are effective against specific generations
- Do not click on links or open attachments without confirming sender
- Back up your data regularly
- Do not give money based on a phone call, email or text message
- Give Aloha to everyone – Only give Trust to people you know well
- Report scams to the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/
    - All federal law enforcement agencies share information

# QUESTIONS?

*Mahalo*

TRUST ALOHA