STOP. VERIFY. PROTECT.

A practical Molokaʻi community guide to avoiding scams

For families, kūpuna, young adults, and small businesses

Scams can happen to anyone.

No shame. Slow down, ask for help, and act quickly when something feels wrong.

"I was a victim of a scam years ago, too. Scammers are skilled at creating fear, urgency, confusion, and trust. This guide is here to help our community pause, verify, and protect one another."

— John "Honu" Puaoi, Owner / Lead Technician, JP Tech

Prepared by JP Tech ● Molokaʻi, Hawaiʻi ● September 2026

jptech.llc • kokua@jptech.llc

QUICK REFERENCE

The one-page scam safety card

Print it, place it near the phone, and review it with your ‘ohana.

1	2	3
STOP	**VERIFY**	**PROTECT**
Pause. Do not click, pay, share a code, install an app, or stay on a pressured call.	End the contact. Use a number, app, bookmark, card, bill, or person you already trust.	Tell someone. Secure exposed accounts, contact the bank, save evidence, and report.

Seven signs that should make you stop

Unexpected contact The call, text, email, social message, QR code, or pop-up arrived out of the blue.	**Urgency or fear** “Act now,” “you will be arrested,” “your account closes today,” or a countdown timer.
Secrecy They tell you not to call family, your bank, your employer, the police, or another technician.	**Unusual payment** Gift cards, wires, crypto, cash, gold, or payment apps are demanded.
Codes or credentials They want a password, PIN, recovery code, one-time code, or approval of a login prompt.	**Remote control** They want you to install software and let an unexpected stranger view or control your screen.
Too good to be true Guaranteed returns, easy money, a prize, grant, job, refund, or recovery service.	**They resist verification** They keep you on the phone, rush you, or become angry when you say you will call back.

THE SAFEST SENTENCE TO SAY

A real bill, fraud alert, or account issue can have a deadline. The key test is this: a legitimate organization should allow you to stop and verify the matter through an official channel. Do not use the link, phone number, or payment instructions supplied by the suspicious contact.

“I do not make security or payment decisions during unexpected calls. I will contact the organization myself.”

UNDERSTAND THE TACTIC

Scammers use pressure, not magic

The story changes, but the emotional pattern is often the same.

Scammers succeed by making a person feel afraid, excited, responsible, embarrassed, or isolated. Their goal is to shorten the time between the message and your action. They may know your name, address, relatives, workplace, or recent purchases because personal information can be collected from public records, social media, old data breaches, and previous messages.

NO SHAME
Anyone can be caught at the wrong moment — tired, worried about a loved one, distracted at work, or eager to solve a problem. Shame helps the scammer. Calm conversation and early action help the victim.

The common pressure cycle

1. Hook A bank alert, virus warning, family emergency, package problem, prize, job, refund, or investment.	**2. Pressure** A deadline, threat, emotional story, countdown, repeated calls, or "stay on the line."
3. Isolation "Do not tell anyone." "Your bank is involved." "Only I can help."	**4. Action** Click, sign in, share a code, install remote access, move money, or buy a gift card.
5. Escalation Once you comply, the scammer asks for more and invents new fees or problems.	**6. Recovery scam** Another person later promises to recover the loss for an upfront payment.

Stories you may see

- **Bank or credit-union impersonation:** "There is fraud; move your money to a safe account."
- **Family emergency or voice clone:** "I am in trouble; do not tell Mom or Dad."
- **Fake tech support:** "Your computer is infected; call now and let us connect."
- **Package, toll, utility, tax, or subscription:** a small urgent payment leads to stolen card or login details.
- **Job, rental, marketplace, or fake check:** money is sent or shown, then you are told to pay part back.
- **Investment, romance, prize, grant, or refund:** trust is built before the request for money.
- **Business impersonation:** a fake owner, vendor, or employee requests a changed bank account or urgent payment.

BREAK THE CYCLE
Pause the story and test the request. Independently call the person or organization. Verify account changes using a second channel. For a family emergency, call the loved one's saved number or another relative. For a business payment, confirm with a known contact before changing banking instructions.

EMAIL

Look past the sender name and logo

A polished message can still be fake. Check, then verify independently.

A scam email can copy a company logo, colors, footer, receipt, or security notice. The visible display name — such as “Apple Support” or “Bank Security” — can be typed by anyone. Click or tap the sender name to reveal the full email address.

Learn the parts of an address

Example structure

Mailbox: `john.doe`
@ symbol: `@`
Main domain: `microsoft.com`
Complete example: `john.doe@microsoft.com`

The domain is the part after the @ symbol. A subdomain is an extra label placed before the main domain. In support.microsoft.com, “support” is the subdomain and microsoft.com is the main domain. Subdomains can be legitimate because the organization controls what appears before its main domain.

Read the address from right to left near the domain ending

Legitimate structure: `support.apple.com`
Main domain: `apple.com`
Misleading example: `apple.com.security-check.invalid`
Actual main domain: `security-check.invalid`

The word apple.com in the misleading example is only placed before the real main domain. The .invalid ending is reserved for examples and is not a real website. Criminals use real look-alike domains with missing letters, extra letters, hyphens, or a different ending.

What to inspect

- **Full sender address:** Is the domain expected and spelled exactly right?
- **Reply-to address:** Does replying send the message somewhere different?
- **Request and context:** Were you expecting this invoice, password reset, shared file, or payment change?
- **Links and attachments:** Do not open them just because the message looks familiar.
- **Tone and pressure:** Watch for urgency, secrecy, threats, or an unusual procedure.

IMPORTANT LIMIT
Domain checking is useful, but it is not perfect proof. Sender information can be spoofed, legitimate businesses may use documented third-party services, and a real account can be compromised. For an important request, open the official app or website yourself, or call a verified number.

LINKS AND WEBSITES

A convincing page can still steal your information

The safest link is often the one you do not use.

A fake sign-in or payment page may look identical to Apple, Google, Microsoft, Facebook, a bank, a delivery company, or a government site. It can copy logos and layouts in seconds. The page may collect your username, password, card details, and verification code, then display an error so you try again.

Safer ways to reach an account

- **Open the official app** already installed on your device.
- **Use a bookmark** you created when you knew you were on the correct site.
- **Type the known address** yourself instead of following an unexpected link.
- **Use the number printed** on your card, statement, bill, or official paperwork.
- **For work**, use the saved vendor contact and verify payment changes by a second method.

Padlock / HTTPS It means the connection is encrypted. It does not prove the site owner is honest.	**Shortened links** They hide the destination. Do not open an unexpected shortened link to inspect it.
QR codes A QR code is simply a link you cannot read at a glance. Unexpected codes deserve the same caution.	**Sponsored search results** Scammers may buy ads for fake support numbers. Prefer the official app or known address.

Before entering a password or payment

- ☐ Did I navigate here independently, or did a message send me here?
- ☐ Is the main domain exactly correct — not just a familiar word somewhere in the address?
- ☐ Was I expecting this sign-in, renewal, delivery fee, toll, invoice, or security check?
- ☐ Can I confirm the same alert inside the official app or account dashboard?
- ☐ Am I being asked for more information than the task should require?

WHEN IN DOUBT

Hovering over a link on a computer or pressing and holding it on a phone may reveal the destination, but this is only an inspection step. You do not need to solve a confusing address. Close the message and reach the organization independently.

CALLS AND TEXTS

Caller ID is a label, not proof

The number on your screen can be spoofed to look local or official.

A scammer can make caller ID show a bank, police department, government office, utility, business, or local number. A text can appear in the same message thread as a legitimate sender. Treat the content and verification process as more important than the displayed name or number.

The safe callback method

1	2	3
END IT	**FIND IT**	**CONFIRM IT**
Hang up or stop replying. You do not owe an unexpected caller a continued conversation.	Use the number on your card, official app, bill, saved contact, or known local office.	Ask whether the alert, employee, case number, or transaction is real.

Never give an unexpected caller

- A password, PIN, security answer, full card number, Social Security number, or recovery code.
- A one-time sign-in code or approval of a login notification you did not begin.
- Permission to move money to a "safe," "protected," or "government" account.
- Remote access to your phone or computer so they can "verify" or "refund" something.
- Silence — scammers may tell you your family, bank employees, or police are involved.

ABOUT VERIFICATION CODES

Some legitimate organizations use codes during a process you initiated through an official channel. The danger is giving a code to someone who contacted you unexpectedly or using a code to authorize a transaction you do not understand. Read the code message; many explicitly say not to share it.

Family emergency and AI voice-clone scams

A short audio sample from social media can be used to imitate a voice. The caller may claim to be a child, grandchild, partner, police officer, lawyer, or doctor. Emotion is the weapon: an accident, arrest, hospital bill, kidnapping, or urgent travel problem.

- Hang up and call the loved one on the number already saved in your phone.
- Call another relative or trusted person who can verify where the person is.
- Ask a question a stranger is unlikely to know — but do not rely on public facts such as a birthday.
- Choose a private family safe word now and do not post it online.

TEXT-MESSAGE TIP

For unwanted scam texts, use your phone's "Report junk" option when available. In the United States, many carriers also accept forwarded spam texts at 7726 (SPAM). Do not reply "STOP" to a clearly fraudulent message unless your carrier specifically instructs you to do so.

FAKE VIRUS ALERTS

When the browser screams, do not call

Full-screen warnings, alarms, and countdowns are common tech-support scams.

A website can imitate a system warning, enter full-screen mode, play an alarm, repeat pop-ups, or show a phone number. It may say your device is infected, your files are being deleted, your bank account is at risk, or your computer will be locked. The goal is to make you call the scammer or install remote-access software.

DO NOT CALL THE NUMBER
Legitimate Microsoft, Apple, browser, and antivirus warnings do not need you to call a random phone number displayed by a web page. A website cannot be trusted to perform a complete diagnosis of your device.

Exit the page safely

STEP	ACTION
First	Do not click inside the warning — including "Cancel," "Scan," "Close," or "Allow."
Try	Press Esc. On many Windows/Linux browsers, F11 exits full screen. Some laptops require Fn+F11.
Close	Windows: Alt+F4. Mac: Command+W closes the tab; Command+Q quits the browser.
If stuck	Use Task Manager / Force Quit or restart the device. Reopen the browser without restoring the suspicious tabs.
Afterward	Update the browser and operating system, check downloads, remove suspicious extensions, and run a trusted security scan.

Website notification abuse

A site may ask to "Allow notifications" and later send fake virus warnings even when the original page is closed. Choose Block unless you deliberately want alerts from a trusted site. To remove permission in Chrome: Settings → Privacy and security → Site settings → Notifications, then block or remove the suspicious site. Other browsers have similar notification settings.

WHY IT LOOKS OFFICIAL
A notification may display the Chrome, Edge, Safari, or Firefox icon because the browser delivered it. That does not mean the browser company created the warning. Read which website is named as the sender.

REMOTE ACCESS

The software may be legitimate; the request may not be

Control of your screen can become control of your accounts and money.

Remote-support tools are used every day by legitimate technicians, employers, and family members. The same tools are also abused by scammers. The key questions are who initiated the contact, how the person was verified, what access is being requested, and whether the work matches the support request.

Safer situation	Dangerous situation
You contacted a known provider through its official website, saved number, or existing support ticket, and you understand the task.	An unexpected caller, pop-up, email, or text tells you to install an app and stay on the line.
Safer behavior	**Dangerous behavior**
Close private apps, watch the session, ask what each action does, and end access when the task is finished.	The person hides the screen, opens banking, asks for codes, changes passwords, or tells you to lie or keep secrets.

Before granting access

- ☐ Did I initiate this support request through a channel I already knew was genuine?
- ☐ Can I independently call the provider or confirm the Kōkua Ticket / case number?
- ☐ Do I know what software is being installed and how it will be removed or disabled?
- ☐ Is the person asking for access limited to what is needed for the repair?
- ☐ Can I stop the session at any time without being threatened or pressured?

VERIFY JP TECH TOO

Do not trust a person only because they claim to be JP Tech. Before allowing access, contact JP Tech through jptech.llc, kokua@jptech.llc, or an existing Kōkua Ticket. JP Tech is local to Moloka'i and uses verified support channels, but impersonation is still possible.

If the session becomes suspicious

- Disconnect Wi-Fi or unplug the network cable, then close the remote-access app.
- Do not open your bank, email, password manager, payment app, or cryptocurrency account.
- Do not type passwords while the person can view or record the screen.
- From a different trusted device, contact your bank and change important passwords, starting with email.
- Preserve the app name, caller number, messages, receipts, and approximate times for reporting.

COMMON REFUND TRICK

A scammer may black out your screen or claim a refund was accidentally made for too much money. The "extra balance" can be a visual trick inside a browser or edited page. Never send money back based only on what someone shows during remote access.

MONEY

Unusual payment methods are a warning

Scammers choose payments that are fast, difficult to reverse, or hard to trace.

Gift cards A bank, government office, utility, court, or tech company will not require gift-card numbers as payment.	**Wire transfers** Transfers can move quickly and may be difficult to recover. Call the bank immediately if sent.
Cryptocurrency Transactions are often irreversible. "Guaranteed" crypto profits and recovery services are common scams.	**Cash or gold** Couriers may be sent to a home. Never hand valuables to a stranger claiming to protect them.
Payment apps Treat payments like cash. Confirm the recipient and do not send money to unlock a refund or prize.	**Fake checks** A bank may show funds before the check is finally rejected. You can still be responsible for money sent onward.

Phrases that should stop the payment

- "Move your money to a safe account."
- "The cashier may ask questions — tell them it is a gift."
- "Do not tell your family or bank; they are involved in the investigation."
- "Pay the tax, fee, shipping, bond, or insurance first to receive the prize or refund."
- "Send back the extra amount from this check."
- "The return is guaranteed, risk-free, or available only today."
- "We can recover what you lost, but you must pay us first."

VERIFY THE MONEY
Do not rely on a phone balance, screenshot, email receipt, or what a remote caller displays. Confirm deposits and transfers directly with your bank through its official app or number. A pending transaction can disappear or be reversed.

Before paying or investing

- ☐ Where does the promised money actually come from?
- ☐ Why is this person rushing me or preventing independent advice?
- ☐ Can the business, license, account, and investment be verified outside the message?
- ☐ What happens if I wait 24 hours and discuss it with family, the bank, or a professional?
- ☐ Is the payment method normal for this organization and documented on its official site?

ACT QUICKLY
When money has already been sent, contact the bank, card issuer, wire service, gift-card company, payment app, or cryptocurrency exchange immediately using official contact information. Ask whether the payment can be stopped, recalled, frozen, or disputed. Recovery is not guaranteed, but speed matters.

APPS AND DOWNLOADS

Free, urgent, and “required” can be bait

Use official stores and known vendor sites; avoid solving a pop-up with another download.

Most modern browsers and phones can open PDFs without a separate reader. Free PDF tools, media players, cleaners, drivers, and browser extensions can be legitimate, but ads and imitation download buttons may install something different from what you intended.

Safer download habits

- Use the Apple App Store, Google Play, Microsoft Store, or the software maker’s known website.
- Avoid download links inside warning pop-ups, unsolicited messages, and sponsored “support” ads.
- Read the publisher name, ratings, recent reviews, requested permissions, and subscription terms.
- Remove apps and extensions you do not recognize or no longer use.
- Update the operating system, browser, apps, router, and security software.
- Keep backups of important photos and files in more than one place.

“Cleaner” or “booster” Modern devices have built-in storage and maintenance tools. Be cautious when an app uses fear or asks for broad access.	**Driver updater** Use Windows Update or the computer/component maker’s official support page when a driver is actually needed.
Browser extension An extension may read pages, change search, insert ads, or capture data. Review permissions and remove unknown items.	**Mobile antivirus** Do not install security apps from pop-ups. Keep the phone updated and use the official app store and built-in protections.

Built-in protection still needs you

On a supported Windows version, Windows Security includes Microsoft Defender Antivirus and firewall features. macOS includes built-in protections such as XProtect and Gatekeeper. Phones also use app sandboxing, permissions, and store review. These systems reduce risk, but no tool can safely approve a scammer’s request for you.

YOUR DECISION MATTERS
The first line of defense is the pause: read the screen, ask why the permission is needed, and do not approve an action you do not understand. A few seconds of checking can prevent hours or days of recovery work.

Signs an app or extension deserves review

- Your search engine, home page, or new-tab page changed without permission.
- Pop-ups or notifications continue after the original website is closed.
- The device requests accessibility, device-administrator, screen-recording, or notification access unexpectedly.
- A new remote-control, cleaner, VPN, wallet, or payment app appeared during a support call.

ACCOUNT SECURITY

Protect email first — it opens many other doors

Long unique passwords and strong multi-factor authentication stop many account takeovers.

Most account theft is not a movie-style password-guessing attack. Criminals often use phishing, reused passwords from old breaches, fake password-reset pages, stolen session cookies, social engineering, or one-time codes that the victim is tricked into sharing.

START WITH EMAIL
Your email account is often the "master key" because password resets and security alerts go there. Use a unique password, strong multi-factor authentication, current recovery information, and regular device/session review.

Password rules that are practical

- Use a different password for every important account. One breach should not unlock everything.
- Prefer long passwords or generated passwords. Length matters more than forced symbol tricks.
- Use a reputable password manager so you do not have to memorize every password.
- Change a password when it is exposed, reused, phished, or you see suspicious activity — not simply because a calendar says so.
- Never send passwords or recovery codes by text, email, or chat.

Multi-factor authentication: strongest to basic

METHOD	WHAT TO KNOW
Passkey or security key	Phishing-resistant when properly used. Strongest common option.
Authenticator app	Generates codes on your device. Stronger than SMS for many users.
Push approval	Convenient, but never approve a prompt you did not initiate. Number matching is safer.
Text / SMS code	Better than password-only when stronger options are unavailable, but vulnerable to phishing and phone-number attacks.

Do not lock yourself out

- Keep your recovery phone number and recovery email current.
- Store backup/recovery codes offline or in a secure password manager — never in an exposed note or photo gallery.
- Register more than one sign-in method when the service allows it, such as a passkey plus a backup security key.
- Review signed-in devices, connected apps, forwarding rules, filters, delegates, and app passwords.
- Do not approve repeated prompts. "MFA fatigue" is a tactic used to make someone tap Allow just to stop the notifications.

AFTER AN INCIDENT

What to do if something already happened

Act quickly, work from a trusted device, and do not let embarrassment delay help.

IMMEDIATE PRIORITIES
First: stop communicating with the scammer. Tell a trusted person. Use official contact information. Save evidence before deleting messages or uninstalling software when it is safe to do so.

WHAT HAPPENED	WHAT TO DO NEXT
Clicked only	Close the page. Check downloads and notification permissions. Update the browser/OS and run a trusted scan. Watch the account for alerts.
Entered a password	Go to the real site from a trusted device. Change it immediately, then change every account that reused it. Sign out other sessions and enable MFA.
Shared a code / approved a prompt	Contact the account provider. Change the password, revoke sessions, review MFA methods and recovery information, and check for unauthorized actions.
Shared bank/card details	Call the number on the card or official app. Freeze or replace the card/account as advised, dispute unauthorized charges, and monitor transactions.
Installed remote access	Disconnect the affected device. End the session. From another trusted device, call the bank and secure email/financial accounts. Get a trusted technician to inspect it.
Sent money	Contact the bank, card issuer, wire service, gift-card company, payment app, or exchange immediately and ask about stopping or recalling the payment.
Shared SSN / ID documents	Use IdentityTheft.gov for a recovery plan. Consider a free credit freeze with all three bureaus and monitor for new accounts.
Device locked / ransomware	Disconnect it from networks and storage. Photograph the message. Do not rush to pay. Get professional help and report to law enforcement / IC3.

Email account cleanup checklist

- ☐ Unknown signed-in devices and active sessions
- ☐ Recovery phone numbers and recovery email addresses
- ☐ Forwarding addresses, inbox rules, filters, and delegated access
- ☐ Connected third-party apps, app passwords, and unfamiliar passkeys/security keys
- ☐ Sent mail, deleted mail, payment receipts, and password-reset messages you did not create

WATCH FOR RECOVERY SCAMS
After a known loss, expect a second wave. Recovery scammers may claim to be investigators, lawyers, government agents, cryptocurrency experts, or technicians. They often know details of the original scam and promise results for an upfront fee.

COMMUNITY PROTECTION

Teach without shame and practice before a crisis

A calm family plan is more useful than a lecture after something goes wrong.

Scammers target every age group. Kūpuna may face tech-support, government, romance, investment, and family-emergency stories. Young adults may face fake jobs, rentals, marketplace sales, scholarships, account-verification messages, and cryptocurrency offers. The tactics overlap, and no group is immune.

A simple ʻohana safety plan

- Choose two trusted people who can be called before sending money or granting access.
- Create a private family safe word for real emergencies and keep it off social media.
- Make a rule that unexpected payment or remote-access requests always require a callback.
- Practice locating the official number on a bank card, bill, app, or saved contact.
- Keep a printed copy of the one-page safety card near the phone or computer.
- Agree that no one will be shamed for asking “Is this real?” or admitting a mistake.

THE RIGHT FIRST RESPONSE

A person who expects criticism may hide the call, payment, or account problem. That delay gives the scammer more time. Thank the person for speaking up, stop the contact, and work through the response steps together.

Use AI as a learning assistant — not an authority

AI can explain a suspicious message, identify common red flags, translate technical language, help locate an official security page, or walk you through enabling multi-factor authentication. It can also be wrong, outdated, or fooled by missing context.

Safe to share A redacted screenshot, general wording, a public website address, or a description with names and account details removed.	**Never paste** Passwords, one-time codes, recovery codes, full card or bank numbers, Social Security numbers, private keys, or identity documents.
Good question “What red flags do you see, and what official channel should I use to verify this?”	**Final check** Confirm important steps with the organization’s official app/site, a known professional, or a trusted family member.

Learn from examples without engaging scammers

Educational channels such as Scammer Payback can show common scripts, fake refund techniques, remote-access tricks, and pressure tactics. Use them for awareness, not confrontation. Do not call scammers back, attempt to access their systems, or put yourself at risk.

THE FAMILY RULE

For a child, kūpuna, or anyone who needs extra support, set a default rule: no unexpected payment, code, account change, or remote-access decision is made alone. Taking a pause is not rude — it is safe.

REPORTING AND HELP

Where to report scams and identity theft

Reporting may help protect you and others, even when money cannot be recovered.

URGENT SITUATIONS

For immediate danger or a crime in progress, call 911. For suspected account or payment fraud, contact the bank, card issuer, payment provider, or exchange first using official contact information.

ReportFraud.ftc.gov Report scams to the Federal Trade Commission.	IdentityTheft.gov Create a personal recovery plan for identity theft.	IC3.gov Report internet-enabled crime to the FBI.	Hawai'i OCP File a consumer complaint with the State of Hawai'i.

Phone and local contacts

RESOURCE	CONTACT	PURPOSE
Federal Trade Commission	**1-877-382-4357**	Scam reporting and consumer guidance.
Hawai'i Office of Consumer Protection	**1-844-808-DCCA (3222)**	State consumer complaints and assistance.
Spam text reporting	**7726 (SPAM)**	Forward or report spam through participating U.S. carriers.
Molokai Police Station	**808-553-5355**	110 Ainoa Street, Kaunakakai.
Maui Police non-emergency	**808-244-6400**	Use for non-emergency police assistance.
Emergency	**911**	Immediate danger, crime in progress, or urgent public-safety need.

JP TECH

JP Tech community support: verify us through jptech.llc, kokua@jptech.llc, or an existing Kōkua Ticket. For active financial fraud, identity theft, threats, or crime, contact the bank and appropriate authorities first. No technician can guarantee recovery of money or data.

REFERENCES

Sources and update notes

This guide is educational and was checked against current official guidance in September 2026.

Public scam tactics, software interfaces, reporting systems, and phone numbers can change. Use the official pages below to confirm current instructions. This guide does not replace legal, financial, law-enforcement, or incident-response advice for a specific case.

1. **Federal Trade Commission — Protect yourself from phishing scams**
   https://consumer.ftc.gov/consumer-alerts/2025/04/protect-yourself-phishing-scams
2. **Federal Trade Commission — What To Do if You Were Scammed**
   https://consumer.ftc.gov/articles/what-do-if-you-were-scammed
3. **Federal Trade Commission — How To Avoid Imposter Scams**
   https://consumer.ftc.gov/features/how-avoid-imposter-scams
4. **Federal Trade Commission — Only scammers tell you to buy a gift card to pay them**
   https://consumer.ftc.gov/consumer-alerts/2024/10/only-scammers-tell-you-buy-gift-card-pay-them
5. **Federal Trade Commission — Scammers use AI to enhance family emergency schemes**
   https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
6. **Federal Trade Commission — Scammers hide harmful links in QR codes**
   https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information
7. **Cybersecurity and Infrastructure Security Agency — Secure Our World**
   https://www.cisa.gov/secure-our-world
8. **National Institute of Standards and Technology — Digital Identity Guidelines, SP 800-63B-4**
   https://pages.nist.gov/800-63-4/sp800-63b.html
9. **Microsoft Support — Protect yourself from tech support scams**
   https://support.microsoft.com/en-us/office/protect-yourself-from-tech-support-scams
10. **Microsoft Support — Windows Security**
    https://support.microsoft.com/en-us/windows/windows-security-app-for-windows
11. **Google Account Help — Secure a hacked or compromised Google Account**
    https://support.google.com/accounts/answer/6294825
12. **Apple Support — Recognize and avoid social engineering schemes**
    https://support.apple.com/102568
13. **Apple Platform Security — Protecting against malware in macOS**
    https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
14. **Federal Communications Commission — Unwanted calls and texts**
    https://consumercomplaints.fcc.gov/hc/en-us/articles/11500223420 3-Unwanted-Calls-Texts-Phone
15. **Federal Bureau of Investigation — Internet Crime Complaint Center**
    https://www.ic3.gov/
16. **State of Hawai‘i Office of Consumer Protection**
    https://cca.hawaii.gov/ocp/
17. **State of Hawai‘i Office of Consumer Protection — Complaint portal**
    https://web2.dcca.hawaii.gov/ocpcomplaint/
18. **County of Maui — Molokai Police Station**
    https://www.mauicounty.gov/facilities/facility/details/Molokai-Police-Station-95
19. **Google Chrome Help — Use notifications to get alerts**
    https://support.google.com/chrome/answer/3220216
20. **JP Tech — Official website and support contact**
    https://jptech.llc

COMMUNITY USE

Share this guide freely with your ‘ohana and community. Keep the JP Tech attribution and source page intact so readers can verify and update the information.

Local Tech Support from Molokaʻi — Built with Aloha.

jptech.llc • kokua@jptech.llc