Bank of Hawai'i

Insights & Stories

AI and oversharing: Tips to stay safe on social media

Reading time: 4 minutes

February 11th, 2026





Social media makes it easy to connect, promote your business, and stay informed. But before posting personal details, it's worth pausing to consider how much is too much.

Many people assume their profiles are protected. In reality, it only takes one overshare for someone to learn more than you ever intended. And in 2026, scammers aren't relying on guesses—AI tools allow them to collect, analyze and act on the information we post.

Here are a few types of personal details to avoid sharing if you want to protect your privacy, identity and finances.

Personal information

Most people know not to share their driver's license, passport, Social Security number or account details online. But everyday personal facts can be just as risky.

Posts about your school, graduation year, mother's maiden name, childhood pet or the street you grew up on may feel harmless. In reality, they mirror common security questions used by banks and financial institutions. Criminals collect this information to reset passwords and access accounts.

And today's scams go even further. With AI, fraudsters can now:

- Build detailed profiles from your public posts
- Create messages that sound like someone you know
- Mimic your writing style or your employer's tone
- Combine small personal details into highly targeted scams

What feels like casual sharing can become fuel for AI-driven fraud.

Location data

Sharing photos from a trip is tempting—but it's safer to wait until you're home. Real-time vacation posts can signal that your house is empty. Even publicly asking for a pet sitter can draw unwanted attention. Travel details should only be shared with people or services you trust.

Scammers also use your travel posts to create convincing financial scams. If you mention a destination, they may generate fake charges from that area and contact you pretending to be your bank. With AI, these messages often mirror a bank's tone, timing and design.

More advanced tactics are also emerging. Fraudsters may:

- Use AI-generated messages that adapt in real time
- Send travel-related alerts that look identical to bank or card notices
- Create deepfake audio or video pretending to be a hotel, airline or even a family member

These scams are designed to feel legitimate—and increasingly, they do.

Close relationships

It's natural to share moments with friends, family and coworkers. But those details can also help scammers impersonate the people you trust most.

Criminals scan tagged photos, comments and group posts to learn who you're close to. With that information, they can create fake profiles—or even use AI to clone someone's voice or image—to make a message or call seem real.

Beyond the familiar "I lost my wallet—can you help?" scams, AI now enables:

- Deepfake voice calls that sound like a family member
- Video calls where the person appears real but isn't
- AI chatbots that hold emotional conversations while posing as someone you know

These scams work because they feel personal. And in 2026, impostors can sound, look and write more convincingly than ever.

If you suspect fraud: Do this now

Act quickly. The faster you respond, the more options you'll have to stop losses and recover.

- **Contact your bank right away.** Ask to freeze or lock your debit and credit cards—many banks let you do this in their mobile app. Review recent transactions, add extra verification, and update your online and mobile access. Your bank can guide next steps and issue new cards if needed.
- **Report identity theft.** At the time of this update, the Federal Trade Commission is closed due to lack of funding, but some online resources remain available, including their identity theft checklist and credit freeze instructions.
- **Place a fraud alert or credit freeze.** A freeze blocks new credit in your name. It's free, can be lifted anytime and doesn't affect your score. You only need to contact one bureau—they'll notify the other two.

Equifax: Freeze or manage alerts: equifax.com/personal/credit-report-services/credit-freeze
Experian: Freeze: experian.com/help/credit-freeze, Fraud alert: experian.com/help/fraud-alert
TransUnion: Freeze: transunion.com/credit-freeze, Fraud alert info: transunion.com/fraud-alerts

Helpful reminders

Freezes offer the strongest protection against new accounts. Lift them briefly when applying for credit, then refreeze—online lifts typically process within an hour.

Fraud alerts add an extra check without fully freezing your credit—useful if you're still applying for loans or credit cards.

Keep monitoring. Review statements, set up account alerts and check your credit reports at AnnualCreditReport.com.

When in doubt, go to the source. Don't click links in texts or emails about fraud. Use the phone number on your card or visit your bank's website directly.

We're here to help.

We care about you and your financial wellbeing. If you spot unauthorized transactions or suspect you are a victim of fraud, contact us as soon as possible. For more information on how to protect yourself against fraud, visit our Bank of Hawaii security hub.

FEDERAL TRADE COMMISSION

IdentityTheft.gov

Is someone using your personal information to open new accounts, make purchases, or get a tax refund? **IdentityTheft.gov** can walk you through each step of the recovery process. Here's how to get started.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- ☐ Call the fraud department. Explain that someone stole your identity.
- ☐ Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- ☐ Change logins, passwords and PINS for your accounts.

Step 2: Place a fraud alert and get your credit report.

- ☐ Contact one of the three credit bureaus. That company must tell the other two.

  Equifax.com/CreditReportAssistance
  1-888-766-0008

  Experian.com/fraudalert
  1-888-397-3742

  TransUnion.com/fraud
  1-800-680-7289

A fraud alert is free. It will make it harder for someone to open new accounts in your name.

You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.

- ☐ Get your free credit report right away. Go to **annualcreditreport.com** or call 1-877-322-8228.

  Did you already order your free annual reports this year? If so, you can pay to get your report immediately. Or follow the instructions in each fraud alert confirmation letter to get a free report, but it might take longer.

- ☐ Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 3: Report identity theft to the FTC.

☐ Complete the FTC's online complaint form at **ftc.gov/complaint**. Give as many details as you can. The complaint form is not available on mobile devices, but you can call 1-877-438-4338 to make your report.

Based on the information you enter, the FTC complaint system will create your Identity Theft Affidavit. You'll need this to complete other steps.

☐ Print and save your FTC Identity Theft Affidavit immediately. Once you leave the page, you won't be able to get your affidavit.

Do you need to update your affidavit? Call 1-877-438-4338.

Step 4: File a report with your local police department.

☐ Go to your local police office with:

- a copy of your FTC Identity Theft Affidavit
- a government-issued ID with a photo
- proof of your address (mortgage statement, rental agreement, or utilities bill)
- any other proof you have of the theft (bills, IRS notices, etc.)
- the FTC's Memo to Law Enforcement (available at **IdentityTheft.gov**)

☐ Tell the police someone stole your identity and you need to file a report. If they are reluctant, show them the FTC's Memo to Law Enforcement.

☐ Ask for a copy of the police report. You'll need this to complete other steps.

☐ Create your Identity Theft Report by combining your FTC Identity Theft Affidavit with your police report.



Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.

Go to **IdentityTheft.gov** for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company. **IdentityTheft.gov** can help — no matter what your specific identity theft situation is.