Voice Cloning

Komando.com, The Current, 2/19/26

Three seconds. That's all AI needs to clone your voice with 85% accuracy. Not three minutes. That Instagram story you posted? Voicemail greeting? More than enough.

Researchers say voice cloning has crossed the indistinguishable threshold. Fakes sound so real that 70% of people can't tell the difference. Scammers are having a field day.

Tools are easy to find

ElevenLabs is the biggest name in AI voice cloning. Upload a minute of audio, and it spits back a near-perfect copy of your voice in 29 languages. **Resemble AI** does it from 10 seconds. **Descript** and **PlayHT** offer similar features. These are legitimate tools built for podcasters and filmmakers.

Scammers use them and open-source tools. The dark web has more powerful versions with no identity checks.

The playbook is simple.

Grab a clip of your kid's voice from social media, clone it, call you in a panic: "Mom, I've been in an accident. I need money." One woman lost $15,000 after hearing her "daughter" crying on the phone. 77% of people who received a cloned voice call lost money.

🛡️ **Your bank's voice ID danger**

Banks push voice authentication like it's Fort Knox. When I tried to opt out of my bank's voice ID, they gave me hassles, calling it "increased security." Really?

A BBC reporter used a cloned voice to break into her accounts at two major banks by playing the phrase "my voice is my password." A Business Insider reporter did the same thing with a service costing a few bucks a month.

Even OpenAI CEO Sam Altman said at a Federal Reserve conference that voice authentication is "a crazy thing to still be doing. AI has fully defeated that."

Protect yourself now:

1. **Set a family code word.** If anyone calls in a crisis, ask for it. No code word, no money.
2. **Hang up and call back** on a number you have saved. Not the one they called from.
3. **Lock down social media.** Every clip is raw material for a scammer.
4. **Call your bank and opt out of voice authentication.** Push back if they resist. A onetime access code is safer.

I guess you could say AI has really found its voice. Unfortunately, it's yours.

Fake Fraud Alerts Are a Growing Scam — Here's How To Spot Them

Written by Clark.com Staff | February 18th, 2026

Keeping tabs on your financial accounts has never been easier — thanks to banking apps, real-time alerts, and text notifications. But scammers have learned to exploit those same tools.

Now, criminals are sending **fake fraud alerts** that look like they come from your bank, credit union, or credit card company — all to trick you into handing over sensitive information.

Money expert Clark Howard warns this scam is spreading — and even savvy consumers are getting fooled.

Got a Fraud Alert From Your Bank? Read This First

The Federal Bureau of Investigation (FBI) recently issued a public service announcement, warning of the rise in "cyber criminals impersonating financial institutions to steal money or information in Account Takeover (ATO) fraud schemes." Since January 2025, the FBI has reported more than **$262 million** in losses.

In this type of scam, scammers send **fraudulent alerts** while pretending to be employees of financial institutions.

Their goal? Convince victims to share:

- Online banking credentials.
- One-time passcodes.
- Two-factor authentication (2FA) codes.
- Other personal financial information.

Clark says the scam comes in many forms, but their goal is the same: to get access to your hard-earned money.

Here's How the Fraud Alert Scam Works

Scammers contact you by **text, phone, email, or app notification**, pretending to represent:

- Your bank.
- A credit union.
- A credit card issuer.
- A brokerage or retirement account provider.

"They'll claim there's suspicious activity on your account," Clark says. "And they often sound incredibly legitimate — sometimes because they know banking procedures and industry language."

In some cases, criminals already have partial personal data from breaches or insider leaks. That makes the message feel more real.

"They'll use the right lingo. Even people who never fall for scams can get tricked," Clark warns.

What Scammers Are Really After: Your Login or 2FA Code

Even if criminals already know your account number or password and maybe even your account balance, **they still need your two-factor authentication (2FA) code** to fully access your account.

Clark strongly supports using strong passwords and 2FA — but warns:

A real bank will NEVER ask you for your verification code.

Scammers create urgency, saying things like:

- "Your money is at risk — act now."
- "We need your code to stop fraudulent charges."

- "We're shutting down suspicious activity."

What are they actually trying to do? **Break into your account and drain your money immediately.**

Red Flags That a Fraud Alert Is Fake

Be suspicious if someone:

- Pressures you to act immediately.
- Asks for a password or verification code.
- Requests personal information over phone, text, or email.
- Claims to be "fraud support" but refuses to let you call back.
- Spoofs your bank's phone number or email address.

Urgency is a major warning sign. Scammers want to **rush you before you have time to verify.**

What Banks Will NEVER Ask You

A legitimate financial institution will **never *call you* and request**:

- Your online banking password.
- A one-time authentication or 2FA code.
- Full Social Security number by phone.
- Remote access to your device.
- Login credentials by email or text.

If someone asks, **it's a scam.**

How To Protect Your Financial Accounts

Here are some steps Clark says you need to take if so that you don't fall victim:

1. Talk As Little As Possible or Not At All

If you get a suspicious phone call, say:
"Thank you for the notice. I'll check on it myself." Then **hang up.**
Clark warns against engaging scammers — even to test them.

2. Never Share Your 2FA or Verification Code

"That code is for you — not them," Clark says.
If someone asks for it, assume fraud immediately.

3. Contact Your Financial Institution — Using Official Channels

Do **not** click links or return calls from suspicious messages.
Instead:

- Open your bank's official app.
- Type the bank's real website yourself.
- Call the number printed on your debit or credit card.

Log in and check your account activity firsthand.

4. Avoid Oversharing — Even Accidentally

Scammers may:

- Record your voice.

- Collect personal clues.
- Use details later in identity theft or voice-cloning scams.

The less you say, the safer you are.

What To Do If You Already Shared Information

If you think you were scammed:

- Contact your bank immediately to report what happened.
- Change all passwords.
- Enable or reset 2FA.
- Monitor transactions daily.
- If you haven't already, **freeze your credit**.
- Report fraud at **ReportFraud.ftc.gov**.

Final Thoughts

Faux fraud alerts are real and a real danger to your finances. Clark says the worst thing you can do is leave it up to the financial institution to protect you or reverse any harm done to your wallet.

"You have to be there for yourself," Clark says. "You have to be your own police officer."

The Unsubscribe Trap

Komando.com, 1/21/26

Your inbox is a disaster. I get it. You're drowning in emails from companies you don't remember signing up for, and that little unsubscribe link at the bottom looks like sweet instant relief. One click and you're free!

Nope. That link might make things worse.

If an email is from a spammer, you waved a flag that says, "Hey, I'm here, and I'm clicking on things!" That makes your email address a bigger target for even more junk.

And that's the best-case scenario.

The worst case? Scam emails imitate real companies. Your bank, a streaming service, a store you shop at. They include an unsubscribe link that takes you to a fake website designed to steal your login or personal info.

You think you're opting out. You're actually handing over your credentials on a silver platter.

This is how they get you

Cybercriminals have gotten scary good at faking familiarity. They make an email look exactly like it's from a brand you trust. Netflix, Amazon, your favorite shopping app. The logo, the colors, the sender name. It all feels right. You don't think twice.

Here's a number that should wake you up: 1 in every 644 clicks on an unsubscribe link in a promo or spam email leads to a malicious website.

Think about how many times you hit unsubscribe in a month. Five? Ten? Across the country, that's millions of clicks a day. At those odds, far too many Americans are getting burned every single day trying to stop the junk.

When it's safe to click

If you are 100% certain an email is legit (like it's really from Netflix, Apple or Chase), it's safe to use the unsubscribe link. Big companies play by the rules because they don't want legal headaches.

But if something feels off, or you never signed up in the first place? Don't touch it. Delete it and move on.

What to do instead

1. Use your email's built-in unsubscribe button. Gmail, Apple Mail, Outlook and others usually show an unsubscribe option near the top of the message, right under the sender's name. This is safer because it's managed by your email provider, not the sender.

2. Mark it as spam (but only if it's actually spam). If you don't recognize the sender or didn't sign up, skip the unsubscribe link entirely. Hit "Report spam" or "Junk." This trains your email to catch this garbage before it ever hits your inbox again.

One more thing. If you signed up for a newsletter and you're done with it, click unsubscribe. Don't hit the spam button. When you mark a legitimate email as spam, you're gone for good. The system boots you permanently, and there's no way back on the list. I see it happen all the time with my own newsletter. Someone marks it as spam, then emails me a week later asking why they stopped getting my tips. Argh.

3. Hover before you click. On a computer, hover your mouse over the unsubscribe link without clicking. Look at where it actually leads. If the URL looks strange, has random characters or doesn't match the sender's domain, that's a red flag. Trust your gut.

The unsubscribe button was supposed to give you control. The bad guys figured out how to turn it against you. Now you know better.

5 Apps Selling Your Every Move

Komando.com, 1/22/26

Larry Johnson in Atlanta installed Life360 to keep tabs on his teenage kids. Good parenting, right? Then he got quoted insane car insurance rates. When he pushed back, he learned the truth. That family safety app had been tracking every turn, every hard brake, every mile his family drove, and it sold all that information to insurance companies.

Larry had no clue. Neither do the **45 million other Americans** getting spied on right now.

The 5 apps (go check your phone)

1. **Life360:** The family tracker. Selling your driving data to Arity, which is owned by Allstate. Yeah, that Allstate.
2. **GasBuddy:** That feature rating your fuel efficiency? It's powered by Arity. Surprise.
3. **MyRadar:** Innocent little weather app. Same tracking garbage hidden inside.
4. **Fuel Rewards:** Saving you 3 cents a gallon while selling you out.
5. **Routely:** Marketed to gig workers. Monetizing your every mile.

Insurance companies buy driving scores based on your speed, braking and routes. Then they use them to raise your rates. You never agreed to this. You never even knew.

Shut them down

iPhone: Settings > **Privacy & Security** > **Location Services**. Find the offenders. Change them to "Never" or "While using." Tap each one and toggle OFF "Precise location."

Android: Settings > **Location** > **App permissions** > [App Name]. Choose "Don't allow" or "Allow only while using the app."

Or delete them. GasBuddy isn't worth your insurance jumping $300 a year.

See what they know about you

You can request your driving report like you pull a credit report. It's free once a year. You might be shocked at what's already in your file.

LexisNexis is the big one. Insurance companies use them constantly to check your history before giving you a quote.

1. Go to **consumer.risk.lexisnexis.com**.
2. Click the red rectangle marked "Request a Consumer Disclosure Report."
3. Fill out the form with your name, address, date of birth, SSN and driver's license number. Yes, you need to give them all that info to confirm it's you. They have it already.
4. They'll mail you instructions to access your report online.

Rather talk to a human? Call 1-888-497-0011.

Your report will show what driving data they have on file, any claims history and who they've shared it with. If something's wrong, you have the legal right to dispute it under the Fair Credit Reporting Act. Same rules as your credit report.

These apps promised to keep your family safe or save you a few bucks on gas. Instead, they've been selling your every move to the highest bidder.

Check your phone. Pull your report. Delete the snitches.