FLUXLABS

GUIDE · NEW SCAMS

Fake voices and video calls

A few seconds of someone's voice is now enough to copy it. Here's how to protect your business and your family.

Scammers use computer programs to copy the voice, and sometimes the face, of a boss, coworker or family member. They call with an emergency and ask for money, gift cards, passwords or a quick favor. The voice can sound exactly right.

Warning signs

- An urgent request for money, gift cards or a wire, with a reason it can't wait.
- "Don't tell anyone" or "I can't talk long".
- A call from an unknown number, or a video call where the person won't move or look around.
- Small oddities: flat emotion, odd pauses, background that doesn't fit.

What to do

1. **Hang up and call back.**
   Use the number you already have for that person, not the one that called you.
2. **Agree on a code word.**
   A word only your team, or family, knows. Ask for it whenever money or access is involved.
3. **Keep the money rules.**
   Payments and bank changes still need a second person and a call back, no matter who asks.
4. **Ask a question only they'd know.**
   Something not on social media: a recent lunch, an inside joke.
5. **Tell IT.**
   If a fake call targeted your business, others on your team are probably next.

Our team code word (keep this page private) _____