Vishing

Responding to Vishing

Vishing (voice phishing) is a scam where criminals use phone calls or voicemails to trick you into sharing sensitive information, sending money, or taking actions that give them access to your accounts or devices.

Scammers often pretend to be:

- Banks, credit card companies, or payment services
- Government agencies (IRS, Social Security, Medicare)
- Tech support or phone carriers

Report unwanted or spoofed calls to the FTC and FCC in addition to using carrier tools.

- Employers, schools, or utilities
- Law enforcement or courts

Vishing relies on urgency, fear, authority, or sympathy to pressure quick decisions.

Common Signs of a Vishing Call

Be cautious if a caller:

- Creates urgency or fear (“Act now,” “Your account is compromised”)
- Threatens consequences (arrest, account closure, service shutdown)
- Asks for verification codes, passwords, PINs, or full SSNs
- Requests payment via gift cards, wire transfers, crypto, or peer-to-peer apps
- Asks you to install software or follow step-by-step instructions
- Refuses to let you hang up or call back
- Spoofs a legitimate caller ID (number looks real)
- If an automated call asks you to press a number, hang up instead.

Caller ID can be spoofed, so save it as context but do not treat it as proof.

If something feels off, trust that instinct.

Vishing – Do This First

Do Not Continue the Call

If you suspect a scam:

- Hang up immediately
- Do not argue or explain
- Do not press buttons or follow prompts

- Legitimate organizations will not punish you for ending a call.

Preserve Details

Before deleting voicemails or call logs:

- Note:
  - Phone number (even if spoofed)
  - Date and time
  - What the caller claimed
  - What they asked you to do
- Save voicemails if possible

Verify Through a Separate Channel

If the call claims to be from a real organization:

- Call the organization using a known, official number
- Log in to the official app or website (do not use links provided by the caller)
- Confirm whether the issue is real

If You Followed Instructions or Shared Information

Act Quickly

If you shared codes, passwords, or PINs:

- Use a safe device to change passwords right away
- Log out of all sessions
- Watch for password reset alerts you didn't request

If you installed software or allowed remote access:

- Disconnect the device from the internet
- Do not continue using it
- Seek professional IT help before attempting removal

Secure Financial Accounts

If you shared financial information or sent money:

- Contact your bank or card issuer immediately
- Report the transaction as fraud
- Follow their instructions to freeze or monitor accounts
- Save case numbers and notes

Watch for Follow-Up Scams

After vishing, scammers may:

- Call again pretending to “fix” the problem
- Pose as fraud departments or law enforcement
- Reference details from the first call
- Do not engage. Verify independently.

Report the Vishing Attempt

Report to Your Phone Carrier

- Many carriers can flag numbers and add account protections
- Ask about call blocking and account PINs

Additional Reporting

- National Reporting
  - FBI Internet Crime Complaint Center (IC3)
  - https://www.ic3.gov
  - (Especially important if money, accounts, or identity data were affected)
- Ohio Resources
  - Ohio Attorney General – Consumer Protection & Cybercrime
  - https://www.ohioattorneygeneral.gov
  - Hotline: 800-282-0515
- Geauga County
  - Geauga County Sheriff’s Office
  - https://www.geaugasheriff.org
  - Local police non-emergency line if fraud or identity theft occurred
  - Call 911 for threats or immediate danger

Recovery – After a Vishing Incident

- Monitor bank and account activity daily for several weeks
- Review account recovery settings
- Expect additional scam attempts referencing the incident
- Consider placing fraud alerts if personal information was exposed

How to Reduce Vishing Risk

- Slow down, urgency is a scam tactic
- Never share one-time codes or passwords by phone
- Hang up and call back using a trusted number
- Don’t trust caller ID alone, it can be spoofed
- Ask for a second opinion before acting under pressure