



ONLINE SAFETY FOR YOU & YOUR FAMILY



Cybersecurity is about protecting our values, our health, our culture, and our democracy.



SPOT WHAT'S NOT REAL — TAKE9 BEFORE YOU SHARE

Scammers and bad actors want you to react fast — without thinking. The **Take9 campaign** is a public service campaign working to promote simple habits to help you stay safe online: **before you share, forward, or act on anything, take 9 seconds to pause and ask: Is this real?**

- **Deepfakes** are videos or images made with AI to show someone saying or doing something they never did. Look for unnatural blinking, blurry edges around the face, or a voice that sounds slightly "off."
- **Fake audio** can copy anyone's voice using AI — a call or message that sounds like a candidate, official, or even a family member may not be real.
- **False election info** includes wrong voting dates, fake polling locations, and messages saying "your vote was already counted" — all designed to stop you from voting.
- **How to verify:** right-click any photo and do a reverse image search. Check the URL — does it end in .gov or a trusted news site? Find the original source before you share.



**Tip: If it makes you feel urgent, angry, or scared — that's the trick.
Real information can wait 9 seconds.**

ROBOCALLS & FAKE VOICES

AI can now clone voices so convincingly that a call may sound exactly like a real person, official, or candidate — but it's not.



- Common scam calls: fake IRS debt, utility shutoffs, Medicare fraud, "you've won a prize"
- If a caller claims to be an official or candidate — hang up and call back using the number from their official website
- No real government agency will ever ask you to pay with gift cards, wire transfer, or crypto

What To Do About ILLEGAL ROBOCALLS

Scammers use robocalls to try to get your money or information.

Companies need your **written permission** to use robocalls to sell you things.



Here's what to do about illegal robocalls:

- ▶ **Hang up.** Don't press any number or call back.
- ▶ **Don't trust caller ID.** It can be faked.
- ▶ **Get call blocking apps or services.** This will help you get fewer robocalls.
- ▶ **Report it.** Tell the FTC at **DoNotCall.gov**.

Learn more at ftc.gov/robocalls



Report scams in Arizona

AZ Attorney General:
602-542-5763

Federal FTC (online):
ReportFraud.ftc.gov

Federal FTC (phone):
1-877-382-4357



Tip: When in doubt – hang up.
You can always call back on the real number.

PROTECT YOUR PHONE & DATA

Apps and social media companies collect your location, contacts, and habits to sell ads. You can limit what they see — without quitting your phone.



- **Location:** Turn off location for apps that don't need it.
Settings > Privacy > Location Services
- **App access:** Check which apps can see your camera, mic, or contacts — turn off what you don't use
- **Ad tracking:** iPhone: Settings > Privacy > Tracking → off.
Android: Google account > Data & Privacy > Ad settings
- **Wi-Fi:** Avoid public Wi-Fi for banking or anything personal — use a VPN if you can
- **Social media:** Review privacy settings — who can see your posts, location, and friend list



**Tip: You don't have to quit social media.
Just know what you're handing over.**

WHERE TO FIND TRUSTED INFORMATION



When you're not sure what's real, go to sources that don't have a reason to mislead you.

- **Election Info:** [vote.gov](https://www.vote.gov) · [azsos.gov/elections](https://www.azsos.gov/elections) · 866-OUR-VOTE (866-687-8683) OR your county website
- **Fact-checking:** visit [FactCheck.org](https://www.factcheck.org) · Snopes · PolitiFact · AP Fact Check
- **Local news & libraries:** free, local, and on your side — no account required
- **Review the URL:** Look for website endings like .gov for government groups or .edu for schools, which have strict rules.
 - Be careful with .com or .net sites that try to sell you something or push a strong personal opinion.
 - Read the "About Us" page to see who runs the site and if they are known and respected.
- **Arizona Native Vote:** arizonanativevote.org — voter resources and community support

✓ Your take-home checklist – 5 things to do this week

- Take 9 seconds before sharing anything online – pause, check, then decide
- Check your phone's app permissions and turn off location for apps that don't need it
- Save azsos.gov/elections and 866-OUR-VOTE in your phone for election questions
- If a call feels off – hang up, find the real number, and call back
- Share this handout with someone in your household or community

References:

1. Election information and safeguards in 2026
<https://openai.com/index/election-safeguards-2026/>

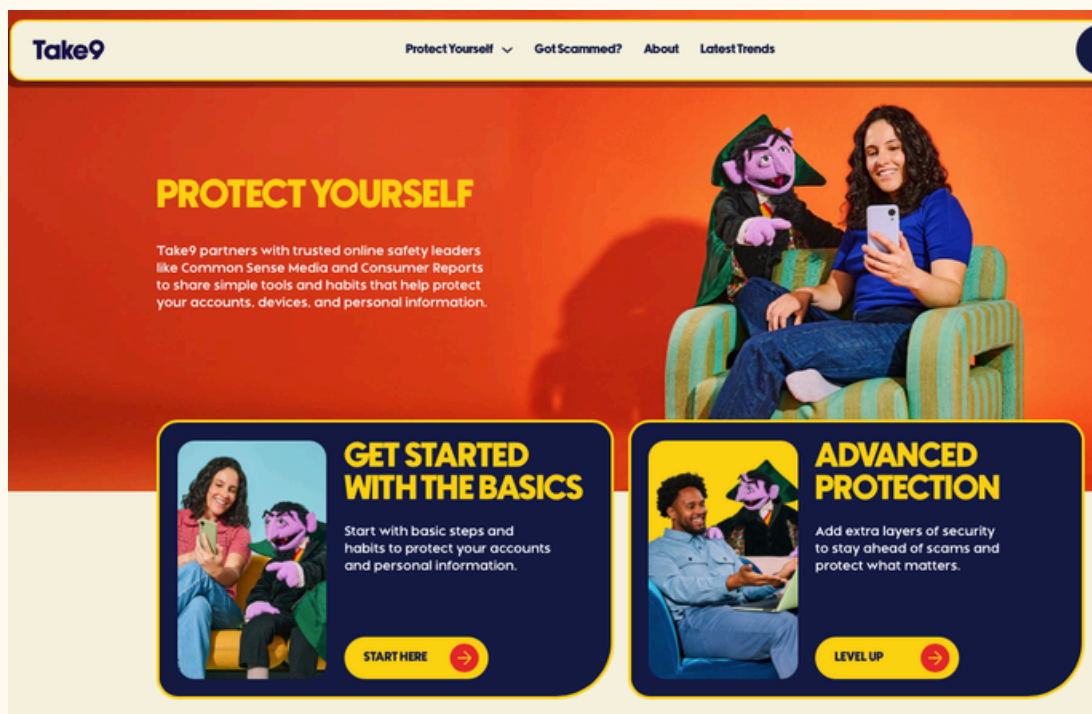
2. pausetake9.org

3. Phone security examples = How to use check your privacy setting so limit Meta
[www.instagram.com/reels/DYpSx5Uo5Z /](https://www.instagram.com/reels/DYpSx5Uo5Z/)

Pop culture examples of AI Fakes and Scams

- Derrick Begay, Navajo Nation, Champion Roper warning community members about scammers on Facebook <https://www.facebook.com/share/v/1Ga2tNgNdD/?mibextid=wwXlfr>
- Example of Misinformation: = County Western Facebook Pages posting false information and AI generated photos and content yet our community members fall for it
- Example of AI/Fake photos & Misinformation = George Straight and Beyonce AND Graham Green and Willie Nelson

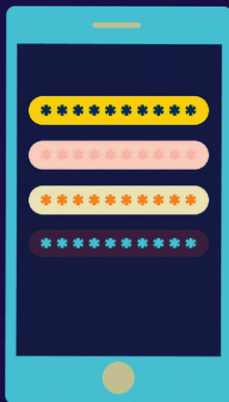
DO YOUR RESEARCH &
FACT CHECK.



Know Digital Scams

Did you know that **39%** of cyberattack or digital scam attempts came from a phishing link?

Most Common Scam Methods	2025
Phishing	39%
Pretending to be your bank or credit card company	25%
Pretending to be tech support	25%
Impersonating someone you know	17%



Phishing is when people receive messages or emails purporting to be from a legitimate source asking for information you normally don't share.

They seem real, but there are some red flags.

Be suspicious of urgent requests for personal information such as your banking information, passwords, personal details, usernames, social security numbers, pet names...

Learn more about protecting yourself from cyber attacks at pausetake9.org

TIPS AND TRICKS TO IDENTIFY SCAMMY BEHAVIOR:

1.

Be suspicious of anyone asking for personal or financial information like passwords or banking details



2.

Confirm the sender and beware of unfamiliar domains



3.

Hover over the hyperlink or do quick search to see if the website is consistent



4.

Look for spelling errors, poor grammar, or unusual sentence structure



5.

Don't let urgency get to you. Scammers want you to feel stressed and take quick action. Take9 instead.



6.

Read the warning signs. Sometimes email providers and browsers will give you a heads up not to trust the sender or link - Listen to them.



Learn more about protecting yourself from cyber attacks at pausetake9.org

Protect Each Other, Report Phishing Messages

Don't just delete fraudulent messages, **report them!**

Reporting ensures that the message is flagged by the service provider as a phishing attack and allows them to block the sender so others don't receive (and potentially fall for!) the bait.

Reporting helps protect the whole community.

Don't be a bystander online, take action.

Learn more about protecting yourself from cyber attacks at pausetake9.org

1 Take 9 seconds to be suspicious

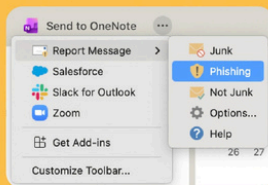
Before clicking, sharing or downloading suspicious content, question it.

Ask yourself: Does this feel right?
Is this email domain legitimate?
Why do I feel nervous?

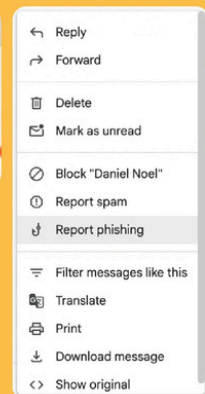
2 Report it

How to report a phishing attempt:

Outlook



Gmail



3 Take a deep breath, take pride in taking initiative

It's better to be safe than sorry.
There are no consequences to reporting fishing.

4 Celebration

You have taken charge of the online safety of yourself and your community with one simple click to report.

Notes

This image shows a full page of white paper with horizontal grey ruling lines. The lines are evenly spaced and run across the width of the page, providing a template for writing or drawing. There are no margins, text, or other markings on the page.