AI DRIVEN SCAMS

Generative AI is getting smarter, which makes fraud attempts harder to detect. Fraudsters use artificial intelligence to mimic voices, create realistic images and videos and imitate writing styles. These AI-driven tactics can increase cybersecurity risk by making it easier to gain unauthorized access to accounts, systems and sensitive data.

Their goal is simple: to make messages feel real enough that you act before stopping to verify.

Understanding how these scams work can help you reduce your risk.

How AI scams work

Fraudsters are increasingly sophisticated, but awareness makes a difference. Here are a few ways scammers use AI to gain access to your financial information:

- **Voice cloning**: Fraudsters can feed AI programs a clip of someone's voice and recreate it, using it to pose as virtually anyone, like a colleague, and request information by phone.
- **Video deepfakes**: Scammers use AI to create realistic-looking videos of real people, which can be used to send requests or simulate video calls. **AI-generated emails and websites**: AI can quickly create emails or fake websites with realistic branding designed to appear as businesses or organizations you trust.

How to help avoid the scams:

- **Pause and think**: Take a moment to evaluate unexpected requests, especially those that create urgency. Legitimate contacts will respect the need to verify.
  Verify information: if you receive a request from a friend, colleague, or business, contact them directly using a known number or trusted channel
- **Spot inconsistencies**: AI is sophisticated, but it's not perfect. Look for mistakes in timing, tone or details,
- **Practice web security**: Never click a link from a suspicious email or text. Confirm website addresses carefully and look for "https://" before entering account login information.
  Keep accounts secure: Use unique, strong passwords for your accounts and opt into multi-factor authentication whenever it is available.

PROTECT **YOURSELF FROM SCAMS**

DO THESE 9 THINGS TO FEEL SAFER NOW

We are all under assault from scammers, and trying to stay safe can seem like a futile effort. But there are some relatively easy things anyone can do right away to improve security, according to AARP's fraud prevention experts. BY AMY NOFZIGER

1 **Update your passwords,** including for your home Wi-Fi. And don't use your pets' or grandkids' names. Instead, try a passphrase you'll remember, but substitute a symbol for a letter, like so: Il@velceCream1960!

2 **Change your settings on your smartphone to send all unknown numbers to voicemail.** (On iPhones, go to Settings, Apps, Phone, then Silence. Android phones vary, so google it.)

3 **On social media, do a privacy checkup.** Under Settings, choose Privacy, and check to make sure only people you choose see your social media posts.

4 **Freeze your credit.** This will prevent crooks from stealing your identity and opening new credit cards and other accounts in your name. Unfreeze it when necessary to allow a credit search.

5 **Take your Social Security card out of your wallet, and put it in a safe place.**

6 **Review your bank and other financial accounts right now for suspicious activity.** Do this daily, weekly or monthly, especially for bank and credit card statements.

7 **Delete apps not in use, including those with saved passwords.**

8 **Go into your device and log out of all your apps to avoid unauthorized access.**

9 **Add the AARP Fraud Watch Network Helpline (877-908-3360) to your contacts for quick access, if needed.**

Visit **aarp.org/fraudwatchnetwork** for more resources.

Amy Nofziger is the senior director of fraud victim support for the AARP Fraud Watch Network.

AARP BULLETIN MARCH/APRIL 2026

HOW TO SPOT A SCAM EMAIL

- **Check the sender.** If you don't know the email address, be careful.
- **Don't click links you weren't expecting.** Scammers hide dangerous links inside emails.
- **Don't open unexpected attachments.** They can harm your computer.
- **Watch for pressure words** . "Urgent," "Immediately." "Your account will close."
- **Look for mistakes.** Bad spelling, strange wording, or odd logos.
- **Be careful with "too good to be true" offers.** Prizes, refunds, or gifts you didn't ask for are usually fake.

HOW TO STAY SAFE

- **Never share personal information.** No passwords, bank info. or codes.
- **Go directly to the website.** Type the address yourself instead of clicking email links.
- **Use strong passwords and keep your device updated.**
- **Delete anything that feels wrong.** Trust your instincts.
- **Ask someone you trust if you're unsure.**

EASY RULE: "If you didn't expect it, don't click it."

Sites offering Scam information:

www.AARP.org (for direct access go **to www. AARP.org/fraud**. You may also call Fraud Watch Network Helpline 1.877.908-3360. You do not have to be an AARP member to utilize this Helpline.

www.AMAC.US

www.BBB.org (Scam Prevention Guide) and or scamnews@iabbb.org

https://oag.ca.gov Office of the Attorney General

https:// ftc.gov/scams Federal Trade Commission

www.dca.gov Department of Consumer Affairs

Technology: Need Help?

Register with the Placerville Senior Center Computer Technology Workshop for Seniors. (Meets the second Thursday of the month – must register for a visit 1.530.621.6150.

- El Dorado Hills Senior Center Computer Workshops for Seniors (call- for information 1 .916.614-3200)

If you have been scammed:

- Call the police and file a report,
  FBI's Internet Crime Complaint Center (IC3)ic3.gov
  Report Fraud ftc.gov Federal trade commission

Miscellaneous information: If you have equipment owned by a company that must be returned at the cancellation or ending of the contract, KEEP YOUR RETURN RECEIPTS FROM THE RETURNING VENDOR (UPS,USPS-examples for at least a year.) *If you receive a notice of not returned and you owe money for the equipment, that receipt may be the only proof you have*. Also keep any and all correspondence emails/texts you receive and keep a log of all talks, time and date as well as the name of person(s) with whom you spoke.

To remove personal information from the internet:

These sites charge for their services but specialize in removal of personal information.

www.optery.com

http://us.cybernews.com

www.pcmag.com

Check other sites using your search engine for sites to remove personal information.

LOOK OUT – AI SCAMS ARE NOW BEING USED

How AI scams work:

Fraudsters are increasingly sophisticated, but awareness makes a difference

Voice Cloning: can feed AI programs a clip of someone's voice and recreate it, using it to pose as virtually anyone, like a colleague, and request information by phone.

VIDEO deepfakes: Scammers use AI to create realistic-looking videos of real people, which can be used to send requests or simulate video calls.

AI generated e-mails and websites: AI can quickly create e-mails or fake websites with realistic branding designed to appear as businesses or organizations you trust.

☆ Quick Takeaway

Email scams rely on urgency, impersonation, and tricking you into clicking or sharing information. Slow down, verify the sender, and never act on an email you weren't expecting.

🔍 How to Spot an Email Scam

1. Check the Sender Carefully

- Scammers disguise addresses to *look* official.
- Look for small changes:
  - support@paypal.com (capital "I" instead of "l")
  - amazon-billing@secure-check.net

2. Look for Urgent or Threatening Language

Scammers want you to panic so you don't think:

- "Your account will be suspended"
- "Unusual activity detected"
- "Immediate action required"

3. Hover Over Links Before Clicking

- The text may say "PayPal," but the link may go to a fake site.
- If the URL looks strange, long, or unrelated — don't click.

4. Unexpected Attachments

- Attachments can contain malware.
- If you didn't expect it, don't open it.

5. Requests for Personal Information

Legitimate companies **never** ask for:

- Passwords
- Social Security numbers
- Bank details
- Verification codes

6. Poor Grammar or Odd Formatting

Not always present, but common in mass scam emails.

7. Too-Good-To-Be-True Offers

- "You won a prize!"
- "We owe you a refund!"
- "Claim your reward now!"

8. Branding That Looks 'Off'

- Wrong colors
- Low-quality logos
- Strange layout

🛡 How to Prevent Email Scams

1. Turn On Multi-Factor Authentication (MFA)

Even if someone steals your password, they can't get in.

2. Use Strong, Unique Passwords

A password manager helps you avoid reusing passwords.

3. Keep Your Devices Updated

Updates patch security holes scammers exploit.

4. Verify Messages Through Official Channels

If an email claims to be from:

- Amazon
- Your bank
- PayPal
- Social Security

Go directly to the official website or app instead of clicking the email link.

5. Use Your Email's Spam Filters

Most services automatically block known scams – make sure filtering is enabled.

6. Report Suspicious Emails

Most companies have dedicated reporting addresses:

- Amazon: stop-spoofing@amazon.com
- PayPal: spoof@paypal.com

7. Never Email Sensitive Information

No Legitimate organization wiLl ask for it.

8. Educate Family and Friends

Scammers target peopLe who aren't aware of the signs.

PREVELANT SCAMS:

Imposter Scams: Fraudsters pose as government officials, bank representatives, claiming the victim owes money.

Grandparent Scams: Scammers impersonal a grandchild or loved one in a fabricated emergency (jail, auto accident) ask for money.

Tech Support: cold calls claim a device has a virus. Ask for money to "fix" problem and access to your computer.

Lottery & Sweepstakes: Victims are told they have won a prize but must pay upfront "taxes" or "processing fees" to claim it (also cruise prizes).

Romance Scams: Fraudsters build fake online relationships, eventually requesting money for emergencies, travel and or investments.

Home Repair Scams: Bogus contractors demand upfront cash for home or roof repairs, then disappear without completing the work.

Using Marriage of Convenience: No public access to information unless court order or you (if involved) .

Identity theft

Phone Scams: *The most important thing is NEVER SAY "YES" OR "OK".* It can be used to prove you agreed to something,