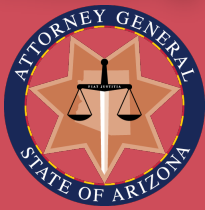
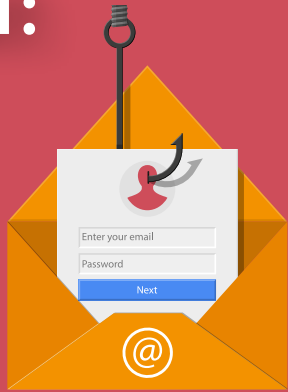


# SCAM ALERT: Phishing



Arizona Attorney General  
Mark Brnovich



## Scam at a glance:

Phishing scams are designed to steal your personal information, usually through email. These fraudulent emails will appear to be from a reputable company asking for your Social Security number, credit card number, or a username and password. The email will either ask for the information directly or urge you to visit a website or call a phone number, where the scammers impersonate a legitimate company.

---

Keep in mind that legitimate businesses should not ask for your information via email.

## Warning Signs:

- The email expresses urgency for you to turn over sensitive information or payment.
- Unsolicited offers or requests for personal information by email that appear to represent a trusted company, agency, or financial institution.
- Vague headers or generic greetings, such as "Hello Customer."
- Emails with poor grammar or illogical sentence sequence.
- Email requesting your Social Security number or other personal identifying information.
- The email contains a request for you to open an attachment.

# Protect Yourself:

- Do not click on or open links in suspicious emails. If you are uncertain whether an email is from a trusted source, use a search engine to get the company's contact information and contact them directly.
- Beware of ads and phony news links that you might click on, opening yourself to phishing attacks or malware.
- If you are browsing the web and receive a pop-up telling you that your computer has a virus or that you have won a prize, beware, these are almost always scams.
- Even if an email or social media communication came from one of your best friends or family members, remember that they also could have been fooled or hacked. Remain cautious in every situation. Even if a message seems friendly, treat links and attachments with suspicion.
- If you discover a phishing scam, report it to the bank, the support desk of your social media network, or whatever other entity the phishing message claims to represent. Take a picture or record as much information as possible.

---

## Resources:

### Arizona Attorney General's Office

[www.azag.gov/complaints/consumer](http://www.azag.gov/complaints/consumer)

Phoenix: (602) 542 - 5763, Tucson: (520) 628 - 6648  
or Toll-free: (800) 352 - 8431

### For additional information go to:

[www.azag.gov/consumer/consumereducation](http://www.azag.gov/consumer/consumereducation)

### Task Force Against Senior Abuse Helpline

(602) 542 - 2124 or (844) 894 - 4735

[www.azag.gov/scamalert](http://www.azag.gov/scamalert)