California State Senate

Senator Benjamin Allen
24TH SENATE DISTRICT

Anyone can find themselves to be a target of a financial predator. Scammers prey upon the unsuspecting and use a variety of tactics to get a victim to send money or share private financial information. Unfortunately, their efforts result in millions of dollars stolen from innocent Californians each year. Fortunately, many of them utilize similar tactics. Understanding how to recognize these tricks and protect yourself can help save you from becoming a victim.

The California Legislature continues to take steps to strengthen the rights of scam victims and to protect consumers from abusive financial practices. The Office of the Attorney General maintains a website devoted to scams and posts consumer alerts on newly-identified scams. Other state and federal resources provide important information on deceptive practices, target groups, and how to protect yourself and your community from fraudulent activities.

This brochure describes three of the most common methods scammers use to target their victims. You will find tips on how to recognize them and how to report them.

For more information, please contact the district office.

RESOURCES

California Office of the Attorney General
OAG.CA.GOV/CONSUMERS/COMMON-SCAMS

Franchise Tax Board
FTB.CA.GOV/HELP/SCAMS

USA.gov
USA.GOV/COMMON-SCAMS-FRAUDS

California Consumer Protection Agencies
DCA.CA.GOV

Federal Trade Commission Fraud Reporting
REPORTFRAUD.FTC.GOV

United States Postal Inspection Service
USPIS.GOV/REPORT

Federal Bureau of Investigation
FBI.GOV/SCAMS-AND-SAFETY

Better Business Bureau
BBB.ORG

Senator Benjamin Allen
24th Senate District

CAPITOL OFFICE
1021 O Street, Suite 6610
Sacramento, CA 95814
TEL (916) 651-4024
FAX (916) 651-4924

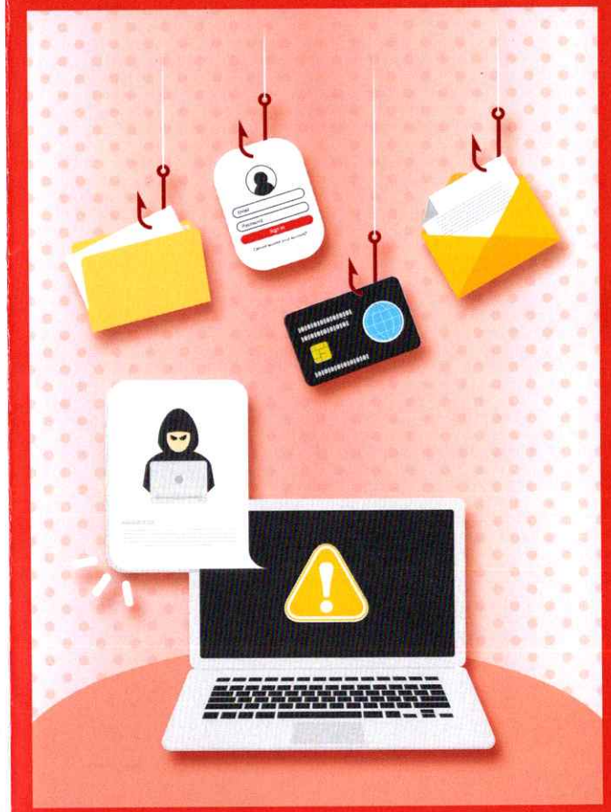
DISTRICT OFFICE
111 Penn Street, Suite 101
El Segundo, CA 90245
TEL (310) 414-8190

senator.allen@senate.ca.gov

www.senate.ca.gov/allen

9/2024

AVOIDING COMMON SCAMS



PROTECT YOURSELF

DON'T BECOME A VICTIM

EMAIL SCAMS

Scams can target you in the form of an email requesting your personal information. This is a tactic known as phishing. These emails may look legitimate because scammers use logos, emails, or phone numbers from the company they are trying to impersonate. These emails may also ask you to visit a website where they will ask you for your information. Some of the information these scams might ask for are:

- username and/or passwords
- credit card numbers
- bank accounts
- Social Security numbers

Legitimate companies will never ask for this information from you. Some of the differences between a scammer's email and a real company's email are:

- Real companies will address you by your name. A scam email will use a generic salutation.
- Real companies will use their company domain name in their emails. A scam email might come from an altered domain name.
- Real company emails are well written. A scam email might have bad grammar and spelling errors.

TELEPHONE SCAMS

Just like email scams, scammers can try to get your money or personal information by contacting you on your phone. These scams can come in the form of a real person, a robocall, or a text message. Some of the tactics these phone calls may try are:

- telling you that you have won a prize or gift
- offering to refinance a loan
- pretending to be your utility company
- selling you fake products

To steal your money, these scammers will ask for your bank account information or they might ask you to pay a fee with gift cards or money orders. These scammers may even threaten you with lawsuits or arrest if you do not comply with their demands.

Some telephone scams will try to reach you through text messages that include links to offers. These links will take you to a website where the scammers will try to get you to enter your personal information. These text messages often come from unknown numbers or even emails. They may also include other phone numbers since the scammers are attempting to scam multiple people simultaneously.

MAIL SCAMS

Some scammers will try to reach you with a mail piece. These scam mailers may offer you a product, a prize, a gift, or investment opportunity in exchange for a processing fee. Some of the signs of scam mailers are:

- a letter with a generic salutation that states you have been specifically selected
- a request for you to confirm your personal information
- a request for you to act immediately in order to receive a deal
- suspicious looking logos from banks or government agencies

Each of these mail scams is designed to get you to send your money to the scammer by calling a provided telephone number, visiting a fraudulent website, or by responding with a payment. The scam mailer might ask you to pay with methods other than your credit card like cash, gift cards, money orders or wire transfers.

WHAT TO DO IF YOU'VE BEEN SCAMMED

If you believe you've been a victim of a scam or fraudulent activity, contact your state consumer protection office.

You can find a list of offices at **DCA.CA.GOV**.

Before sending in a written complaint, confirm with the office that they handle the complaint you will be filing. If you've been scammed for money or possessions, contact your local police department.

You can also report the scam or fraudulent activity to the federal government. The primary agency for collecting reports of scams or fraud is the Federal Trade Commission (FTC). Contact the FTC to report a scam at **REPORTFRAUD.FTC.GOV** or by phone at 877.382.4357 (9 am - 8 pm, ET).

If you've been contacted through a mail piece, or if you've sent money or personal information in the mail, you can contact the US Postal Inspection Service (USPIS). USPIS handles and prosecutes any scam or fraudulent activity that utilizes the US Postal Service. If you've been contacted or scammed by mail, you can report this activity at **USPIS.GOV/REPORT**.