VERMONT

Protect Against Scams

Scams are all too common. If you have experienced a scam, call the Vermont Attorney General's **Consumer Assistance Program: (800) 649-2424**

In 2018, Vermonters filed 5,471 scam reports with the Vermont Attorney General's Consumer Assistance Program (CAP). Scam reports total over one-third of all contacts CAP receives each year, making them one of the most common consumer issues affecting Vermonters. Nationwide, the Federal Trade Commission received 1.4 million fraud reports, and people said they lost money to the fraud in 25% of those reports.

Scammers are good at what they do. That's why the Attorney General's Office is here to help. CAP tracks trends affecting the state and provides timely warnings to the public. Sign up for Scam Alerts so that you can protect yourself and your loved ones from scams. Visit: ago.vermont.gov/cap/sign-up-for-scam-alerts/

Tips to Avoid Common Money Scams

1. Never wire money to a stranger.

2. Do not give out your personal banking, credit card, or debit card information.

3. Do not shop with unfamiliar retailers.

4. Never send cash in the mail.

5. Never send gift cards as a payment method or to someone you do not know personally.

6. Be careful when donating to charities, verify the charity's name, contact information, and how the donation will be used.

7. Do not provide remote access to your computer; this may occur when you click a link from an unfamiliar email.

Protecting Against Phone Scams

If you pick up a call that sounds like a scam, hang up right away. If the scammer calls back, do not answer. Scam callers are extremely difficult to track, but there are steps you can take to stop calls and protect your information:

1. Blocking Robocalls The options for mobile phones depend on your carrier. Some carriers offer free services, while others offer an app for a fee. Some carriers attempt to block scam calls, while others only offer caller ID services to identify possible scammers. For landlines, options depend on your phone company. Some offer call blocking for particular numbers, while others offer blocking for all anonymous calls. You should contact your phone company to get more information on the services they provide.

2. Do Not Call Registry
The National Do Not Call Registry protects you from unwanted telemarketing calls. Unfortunately, scammers do not abide by the Registry, but telemarketers cannot contact you if your number is on this registry. To join the Registry, call (888) 382-1222 from the line that you would like to be added or visit donotcall.gov.

3. Protect Your Personal Information
Do not give personal information over the phone. Sensitive personal information includes your Social Security number, credit card numbers, bank account numbers (including the numbers on your checks), debit card numbers, passwords, personal identification numbers (PIN), your birth date, and any other "account" numbers.

Online Security:
Email Phishing Scams

Phishing is when you receive emails, calls, or texts that seem to be from companies or individuals you are familiar with. These scammers are trying to get personal information from you. Scammers use emails and text messages to ask you to follow a link or share your password. Their goal is to steal your identity or your money, and maybe get remote access to your computer. The Federal Trade Commission provides the following tips for identifying a scam email.

How can you spot a phishing email?

Phishing emails often:

- claim the company noticed some suspicious activity;
- claim there's a problem with your account or payment information;
- claim you must confirm personal information (for example, credit card number or Social Security number);
- attach a fake invoice;
- ask you follow a link to make a payment;
- claim that you're eligible to register for a government refund or grant; or,
- offer coupons for free stuff.

What to do:

If you suspect that you have received a phishing email or text message, report it! You can take the following steps:

- Call the Consumer Assistance Program: (800) 649-2424
- Forward the email or text message to the FTC: SPAM@UCE.GOV or text SPAM (7726)
- **Delete the message and do not respond**

What are the Most Common Scams?

In 2018, the most common scams affecting Vermonters were: IRS Imposter Scams, Social Security Phishing Scams, and Computer Tech Support Scams. Below is some information about how to identify these scams and what you should do:

1. IRS Imposter

The scam: A phone call claiming you owe "back taxes" or payments to the government allegedly from the IRS or "US Treasury and Legal Affairs." They may threaten you with arrest or investigation.

How to spot the scam: The IRS will never call you at home to threaten legal action. Any information provided by the IRS will be provided to you through the mail.

What to do: Don't respond to these callers. If you think you may actually owe back taxes, hang up and contact the IRS directly at 1-800-829-1040. Do not provide any information to the caller.

2. Social Security Number Phishing

The scam: An attempt to obtain your Social Security number by posing as the Social Security Administration or a business. They may try to get access to your Social Security number by telling you it has been compromised or stolen.

How to spot the scam: If Social Security (or any government body) wanted to contact you, they would not call to ask for your personal information, especially your Social Security number, over the phone.

What to do: Be wary when responding to unsolicited contacts and never provide personal information to unknown contacts. Try not to pick up the phone for numbers you do not recognize.

3. Computer Tech Support

The scam: A phone call or pop-up message on your computer claiming to be from Microsoft/Windows, Apple, or another well-known tech company. They will say that there's a virus, malware, or other problem with your computer and try to persuade you to give them remote access to resolve the issue.

How to spot the scam: Legitimate customer service information usually won't display as a pop-up. Companies like Microsoft, Apple, and Google will not call you to notify you of malware on your computer.

What to do: Never provide remote access to your computer to a stranger or click links from an unknown sender in an e-mail or pop-up message. If you get a call from "tech support," hang up. Also, be careful when searching for tech support phone numbers online. Some users have been scammed by calling illegitimate company phone numbers.

RESOURCES:

Report scams to the Attorney General:
Consumer Assistance Program
(800) 649-2424
ago.vermont.gov/cap

Report scams and access more resources:
Federal Trade Commission
(877) 382-4357
ftc.gov

How to protect yourself from identity theft and report fraud:
Federal Trade Commission
(877) 438-4338
identitytheft.gov

Are you receiving scam email or text messages? Forward them to:
Federal Trade Commission
SPAM@UCE.GOV or SPAM (7726)