



## **Top 10 Scams of 2023** **Reported to the Vermont Attorney General's Consumer Assistance Program**

### **1. Computer Tech Support**

The scam: You receive a phone call, pop-up, email or text message on your computer claiming to be a well-known company; sometimes it's a tech company like Norton, Apple, or Microsoft, or it's Amazon saying your credit card has been charged, or there is a package delivery delay. They will urge you to contact them due to a problem: your electronic device has a virus, your device security subscription has been automatically renewed, or you have been charged for services you did not receive or request. You may be prompted to click a link or call a number to contact. They will try to persuade you to give remote access to your device to fix the problem, and sometimes will even ask for immediate payment for their services or have you login to your online bank account to initiate a transfer.

How to spot the scam: Companies will not call with tech support unless you requested that they contact you. Legitimate tech support companies do not display communications to their customers as random notices or alerts on your device. Tech support will not call you to warn of security incidents or to notify you that your account has been renewed for a subscription you do not recognize, and they will not send you random links with instructions for you to click on URLs. If you receive a package that you do not recall ordering, check your statement history to see if you have been charged. Packages without a return address are highly suspicious.

What to do: When contacted about a supposed business relationship, take steps to verify, especially if you do not remember purchasing the products/services. Never click on links or provide remote access to your computer from an unknown sender or pop-up message on your device's screen. If you received a pop-up message you cannot click out of, shut down, restart, or unplug your device. If you get a call from "tech support", hang up. Also, be careful when searching for tech support online. Some users have been scammed by calling inaccurate phone numbers listed online. If you are concerned about charges made to your accounts, log in to your account directly and contact your financial institution. If you receive a package that you did not order, write "return to sender" on it and give it back to the mail carrier.

### **2. Phishing (Bank, etc.)**

The scam: You receive an email or phone call claiming to be from a bank or entity that keeps personal identifiable information (PII), like the Social Security Administration. The communication may claim that your account is in danger or has been suspended, or that your card is on hold due to suspicion activity. Emails may also include links to phony websites. Phone calls may claim that there has been fraudulent activity involving your account, and the scammers demand personal information about you and your account.

How to spot the scam: Scammers mask their actual identity by changing the sender's name to the name of the cloned entity. Look at the email address before opening the email. You will often find an account not affiliated with the claimed entity. Similarly, scammers can spoof phone numbers of real businesses. If you answer a call that appears to be from a company with which you maintain an account and they ask for your personal and/or account information, hang up and call the company directly on a number you trust and verify their attempt to contact you.

What to do: Do not reply to the email or click on any links or attachments included on the message. If you receive a call, hang up the phone. Correspond with entities only using verified contact information, such as information listed on your statement.

### 3. **Law Enforcement Imposter**

The scam: You receive a phone call unexpectedly, claiming to be a police officer, sheriff, U.S. Marshall, or the U.S. Customs and Border Protection. The caller threatens arrest or legal action or says there is a warrant out against you. When you engage, urgent payment is demanded to make the problem go away. Payment does not solve the supposed problem, and they keep calling.

How to spot the scam: Law enforcers do not warn you ahead of time about a pending warrant or arrest. Legal action follows standard due process and there is a lot of paperwork, typically delivered by mail or served in person.

What to do: Hang up on all arrest threats and report them. Watch out for [similar government imposter scams](#) that purport to be agents of government, including from the [Social Security Administration](#), the IRS and more.

### 4. **Medicare Card Phishing**

The scam: Scammers will call, often with a live call and from a spoofed caller ID number, posing as Medicare representatives to gain your personal information and money. These scams are most frequent during times of open enrollment but can occur year-round. The scammers will state they need your Medicare card number or Social Security number to keep your coverage active and verify medical information. The calls may also claim that coverage is expiring or in need of renewal. Scammers will also ask if you received a “new Medicare card.”

How to spot the scam: In general, Medicare cards do not expire. Unless you have called Medicare using the 800 number on the back of your card and requested a callback, Medicare will not call you. If a phone call is required, you would receive a letter from the Social Security Administration to schedule a call. Medicare representatives will never call you in an attempt to verify your information, sell you products, tell you that your coverage is expiring, or to issue you a new card.

What to do: Never provide your Medicare number or other personal information and payment to unknown callers. In Vermont, representatives of the State Health Insurance Assistance Program (SHIP) at 1-800-642-5119 through local Area Agencies on Aging can help address Medicare questions. Other questions and concerns about Medicare coverage can be directed to Medicare at 1-800-MEDICARE.

## 5. [Identity Theft](#)

The scam: Your personal information is compromised and may be used for another's financial gain. This can look like: an unauthorized charge on an account, receiving a letter about a new account opening or a data breach notification. You might stop receiving legitimate bills and other mail or start to get bills for products and services that you didn't purchase.

How to spot the scam: Beware of communications denoting unexpected bank transactions, credit card or benefit applications. If your expected bills are not showing up, or you are receiving correspondence in someone else's name, report it.

What to do: Don't give out personal information, such as your Social Security number, passwords, personal identification numbers, and financial accounts. Review your credit reports at least once a year. ([You can access your credit report for free](#)). Carefully check bank account statements and benefits to verify transactions. [Shred documents](#) and expired credit cards before you throw them out. Verify security breach notification letters received on the [Attorney General's website](#). If your information has been stolen by an identity thief, [take identity theft protection steps](#). You can safeguard your financial information by placing a [credit freeze](#) on your credit report.

## 6. [Sweepstakes/Lotteries](#)

The scam: You will be notified by phone, email, or mail that you won a prize or a quantity of money. In some cases, you will even receive a realistic-looking check – but it is fake! You are instructed to pay fees and give your financial and personal information to claim your prize. They often use a legitimate sweepstakes name, like Publishers Clearing House.

How to spot the scam: Legitimate sweepstakes and contest businesses, like Publishers Clearing House and Mega Millions lottery, will contact you in person if you win a major prize. [For prizes under \\$10,000](#), the notification is done through certified mail by overnight delivery services (FedEx, UPS). They will not contact you by phone, nor require a payment or processing fee to release your prize.

What to do: If it sounds too good to be true, then it's not true. You don't need to pay fees to an entity, whether for processing, shipping/handling, insurance, and taxes, etc., or give your financial information in order to claim a prize.

## 7. [Fake Websites/Online Listings](#)

The scam: Fake websites or phony listings draw you into a purchase that is enticing. Listings may include online storefronts, Facebook Marketplace and Craigslist posts that don't deliver after payment has been made, cheap [pet sales](#), and websites with steep discounts. This scam can also appear in [online rental listings](#) as well as target online sellers.

How to spot the scam: Be skeptical of unrealistic offers. Watch out for requests for money in any form when not made in person. Scammers likely will not want to talk on the phone or meet in person. Heed warnings in user reviews and other online commentary.

What to do: Investigate the person/profile of the seller. If their profile is new and they have no friends and photos, they are likely a scam. Verify the website URL is the actual business' site and not a copycat. Research new websites you are considering doing business with by looking up online reviews and business registrations, taking note of how long the company has been operating. Perform online searches of the business with "scam" and "complaints" to see if issues generate. For classified-type listings, complete your transactions in cash and preferably at a safe place in person.

## 8. [Family Emergency/Imposter](#)

The scam: Scammers pose as someone you trust and pretend to be in a crisis to convince you to send them money or ask for a favor. These scammers pose as grandchildren, friends, relatives, and close contacts, impersonating people you adore to play on your fears and trick you into sending money urgently. After the initial contact, you may be redirected to a lawyer or parole officer. Sometimes the voices in the phone call sound like relatives due to scammers utilizing artificial intelligence. In-person couriers may also come to retrieve funds.

How to spot the scam: Contacts come in as calls, emails, or online messages. Sometimes it's someone you haven't heard from in a while. They require urgency and ask for secrecy. You may be instructed not to speak to your loved one on the phone.

What to do: [Take steps to verify](#). Check out if they really are who they say, even if they sound like a loved one. Slow down your response and contact someone you trust to verify if there is an emergency. You can also choose a "code word" with friends and family to verify the person is who they claim to be. If they don't know the word, they are not your friend or family member. Do not give money to in-person couriers.

## 9. **Deceitful Solicitations**

The scam: You receive unsolicited communication with a deceptive promotion. Unreal offers may appear to be from a known business, like Xfinity, DirecTV, or Dish Network. Solicitations may purport affiliation with a charitable cause or make low-ball offers on the

sale of real estate, urging recipients to complete an enclosed one-page form contract to sign over their home.

How to spot the scam: Beware of unsolicited offers you cannot verify. Be especially wary of offers that ask you to complete the transaction quickly or in one sitting.

What to do: Hang up on unknown callers and let calls go to voicemail. When you receive mailings, take extra time to review by inspecting the details and using your personal contacts as a sounding board. Never give over your payment information or sign on the line when you don't understand the offer or details.

## 10. Rewards Credit

The scam: You get an email or text message that you have unclaimed rewards, or have earned a reward credit in points, a gift card, or redemption coupon. The message displays as being from major retailers and includes a link to click or a number to call. When you do, you are asked to confirm your identity by remitting personal information, then payment is requested for processing or shipping.

How to spot the scam: Rewards points and credits are earned through a pre-established program that you would have opted into. If you are a member of a rewards program, the redemption steps are outlined within the rewards program, and you would not need to resubmit your information. Most store rewards programs are activated with basic consumer information (name/address/email/phone number). If you are not a member of a rewards program, but are receiving notices about one, it's a scam.

What to do: Do not reply to messages or click on any links. If you believe you may be due rewards points or credits, log into your account directly or contact the program's customer service line on a trusted number.

---

### Scams Reported by Businesses in 2023

Of the 3,213 scams reported to the Consumer Assistance Program (CAP) in 2023, 168 were submitted by Vermont businesses.

The five most common scams for businesses include: Imposters of business personnel, fake orders of goods or services, business identity theft, businesses' phone numbers being hijacked or spoofed, and phishing emails contacting businesses.

The top scam for businesses to look out for is the **Imposter of Business Personnel aka the Business Email Imposter Scam:**

The scam: Scammers impersonate employees or familiar business representatives' emails and contact company bookkeepers and office administrators asking them to change bank account information or direct deposit information or asking them to write checks. By impersonating an employee's email address or creating a fake personal email for the

employee, scammers can steal money from businesses and steal paychecks from employees.

How to spot: Scammers will use an email address that only slightly varies from an employee's true email and can be difficult to spot when using a mobile device. Be suspicious of emails coming from outside your company's domain. The sender will refuse to connect on a live call due to being preoccupied (in a meeting, no cell service, very busy).

What to do: Vermont businesses and non-profits should always verify email addresses and speak directly with an employee or business representative in person or via phone when sending money or changing payment information. CAP urges business owners to educate their entire company on scams that target businesses.

To learn more about how to protect your business from these scams, watch CAP's [Avoiding the Business Imposter Email Scam Video](#) and visit the CAP Connections blog post on [Vermont Business Imposter Email Scams Are on the Rise](#).

CAP encourages businesses in Vermont to take the following steps to help prevent scams:

**Train Your Employees:** Your best defense is an informed workforce.

**Verify Invoices and Payments:** Check all invoices closely. Never pay unless you know the bill is for items that were actually ordered and delivered. Tell your staff to do the same.

**Be Tech-Savvy:** Don't believe your caller ID. Imposters often fake caller ID information so you'll be more likely to believe them when they claim to be a government agency or a vendor you trust.

**Know Who You're Dealing With:** Never send money to parties you cannot verify. Check registration history and recommendations and confirm contacts by calling. Before doing business with a new company, search the company's name online with the term "scam" or "complaint."