
An informational guide to recognizing scams, protecting your identity, and being wise consumers.
A Note from the President

Every day, Better Business Bureau of Upstate New York helps people find businesses and charities they can trust.

At BBB, we are dedicated to fostering honest and responsive relationships between businesses and consumers -- instilling consumer confidence and advancing a trustworthy marketplace for all.

We produced this guide as a resource for you to learn how to protect yourself from common scams. We have a dedicated staff that offers free business and charity reviews, complaint resolution services and many other programs and services to assist you in your purchasing and donation decisions.
Common Terms

Phishing
A scam by which an internet user is tricked into revealing personal or confidential information which the scammer can use to steal your identity.

Skimming
The act in which a scammer attaches a small device (such as a credit card reader) to the existing reader in an attempt to steal your personal information. Scammers will often put these devices on self-serve gas pumps.

Vishing
An attempt by scammers to get information from you by impersonating well known companies. You may recognize the company name and be more willing to provide your personal information, such as your account or credit card number.

Smishing
An attack on all cell phones in which a virus is accidentally downloaded resulting in your phone being infected by a virus. These links will often come in a text message.

Pharming
A tactic in which you visit a known website and then you are redirected to a fraudulent site. The fake site may contain viruses or even look exactly like the site you were trying to visit.
6 Ways BBB Helps

**Customer Reviews**
Better Business Bureau verifies all reviews with the business to ensure the reviewer was a legitimate customer. No review is published until the verification process is completed.

**BBB Business Profiles**
BBB provides information and ratings on businesses in the United States and Canada. Simply search BBB.org for the business or charity to read the information.

**Charity Review**
BBB provides reviews on charities and nonprofit organizations in Upstate New York based on BBB’s 20 Standards for Charity Accountability. You can search for the charity on either BBB.org or Give.org.
Complaint/Dispute Resolution
You can request a complaint form or visit BBB.org/complaint to start the process. Submit your complaint in writing either by mail or online.

News and Scam Alerts
BBB publishes news and scam alerts to social media and our website to keep everyone informed with tips on how they can protect themselves. You can also report scams to BBB’s Scam Tracker at BBB.org/scamtracker.

Investigations/Ad Review
BBB investigates businesses in our service area to ensure ethical operations and advertisements. Staff works with law enforcement and other agencies to report on unscrupulous businesses and scams.
Safeguarding Your Identity

Shred Old Documents
Shred bank statements, credit card applications, insurance forms, financial statements, health forms, and household bills. You should shred anything with your personal information once it’s past the time frame for document retention.

Protect your Number
Do not carry your social security card or give out your number without verifying who is on the other end of the computer or phone. Keep your card in a secure location and out of plain sight.

Protect Your Cards
Cut up old cards when they have expired and make sure the number is illegible. Keep an eye on bills and billing cycles.

Protect Your Information
Your bank, credit card company or the IRS will not e-mail you asking for your information. They already have it!

Monitor Your Credit
Monitor your statements monthly for unauthorized transactions and check your credit report at least once a year for any changes.
If you find yourself the victim of a data breach, consider taking these steps:

**Credit Freeze**
You can freeze your credit report and prevent identity thieves from establishing new lines of credit under false names. A credit freeze will not impact your credit score or impair your ability to use existing credit cards.

**Fraud Alert**
A fraud alert flags your credit reports, alerting potential lenders to take extra precautions in identifying somebody who is attempting to open an account in your name. It’s free and it will not interfere with your ability to receive credit.

To be effective, a fraud alert and a credit freeze must be set up with the following credit bureaus:

- Experian: 888-397-3472 · experian.com/freeze/center.html
- Transunion: 888-909-8872 · freeze.transunion.com
- Equifax: 800-349-9960 · freeze.equifax.com

Check your credit annually at annualcreditreport.com
What is a robocall?
If you answer the phone and hear a recorded message instead of a live person, it’s a robocall. Callers use a computerized autodialer to deliver a pre-recorded message to a land line or wireless number. Many different scams use robocalls, from bogus companies claiming to lower utility bills or credit card rates, government grants, vacation packages and calls from individuals posing as IRS agents.

What types of robocalls are allowed?
In the United States, recorded messages regarding candidates running for office or charities asking for donations are allowed. Messages that are solely informational, such as a reminder from your doctor’s office, are permitted. Pre-recorded messages from banks, telephone carriers and charities also are exempt from these rules if the organizations make the calls themselves.

How do I know if a robocall is illegal?
In the United States, an immediate red flag is if the recording is trying to sell you something. If the recording is a sales message and you haven’t given your written permission to get calls from the company on the other end, the call is illegal.
Use Caller ID
Screen calls and consider not answering unfamiliar numbers. If it is important, the caller will leave a message and you can call back. You cannot always believe your caller ID. Scammers can spoof phone numbers and names of legitimate companies on caller ID. This lends to the credibility of their pitches. If you didn’t opt in to calls from a company, hang up and report the number to the Do Not Call Registry. You may receive a call from a local number, or a number that looks familiar. Do not be fooled, this is another spoofing tactic.

Just Hang Up
If you accidentally answer a robocall, ignore the recorded prompts to press digits on your phone keypad, even if they claim it will take you off the calling list. If you press a key, it tells the scammers you have an active number. Your number could be sold to other telemarketing centers and the frequency of calls will increase.

Get on the Do Not Call Registry
You will receive fewer marketing calls and make it easier to identify fraudulent ones. In the United States, you can call 888-382-1222 or register online at donotcall.gov. Remember to do this for both your cell phone and land line numbers.
Common Phone Scams

**Grandparent Scam**
The victim receives a call from somebody stating they are a grandchild in an emergency. Scammers will ask you to send a wire transfer or gift card to help with legal expenses. Look for variations in this scam as it changes day to day.

**Social Security Scam**
The victim receives a call from somebody claiming to be from the social security office. The scammer claims your social security number is linked to a crime and you need to provide your social security and bank account numbers to clear you of charges or to secure your identity.

**IRS Scam**
The victim receives a call from somebody claiming to be from IRS. The scammer will advise that you owe taxes and if you do not pay that instant the police will be sent to your home to arrest you. The scammers will ask you to purchase gift cards and read them the number on the back to avoid arrest.

**Fake Check Scam**
The victim will receive a check in the mail with instructions by the sender to deposit the check then send a specific amount back. The scammer will explain that the amount being sent back is for taxes or fees, or to make sure your bank account is valid. The victim will send money to the scammer but the check will bounce. At that point, there is no way to get the money back that was sent.
Common Phone Scams

Romance Scam
The victim will receive a friend request from somebody they have never met. Oftentimes the photos show real, good looking people. The scammer will start messaging you and building a friendship. Eventually, the scammer becomes someone you trust and confide in. The scammer will begin asking you to send money to help them during an “emergency.” The requests get bigger and bigger until you have no money left.

Sweepstakes Scam
The victim receives a call from somebody claiming they have won a prize. Whether it’s the foreign lottery, a cruise, or a free night’s stay in a hotel, they are all scams unless you specifically entered to win the prize. Watch out for Publisher’s Clearing House imposters.

Tech Support Scam
The victim receives a call from somebody claiming to be from either Microsoft or Apple Support. The scammer advises that your computer has a virus and requests remote access to your device so it can be fixed. Upon receiving access, a fake diagnostic test will run showing a virus and the scammer will ask you to pay to fix the problem. Now that they have access to your device, they also have access to all files, photos, and personal information stored on your computer.

If you encounter a scam, remember to report it to BBB’s Scam Tracker and call BBB if you’ve lost money to the scam.
Charity

Research
Look up the charity that is asking you for money before you donate. Check the website and social media for inconsistencies and to make sure it is a legitimate organization.

Beware of Emotional Pleas
When a charity asks you to donate “right here, right now” consider it a red flag. Don’t let a seemingly good cause cloud your judgement.

Ask Questions
Ask the person who is representing the organization about the mission and where your donation is going. Make sure the “pitch” is consistent and their story doesn’t change throughout the conversation.

Use Traditional Forms of Payment
If a charity is asking you to buy gift cards or use other payment methods that seem non-traditional, that’s a red flag. Gift cards are not an acceptable form of payment.

Check Give.org
BBB reviews nonprofit organizations using 20 Standards of Charity Accountability. Check Give.org to see if BBB has a charity report on the organization.
Charity

Better Business Bureau Accredited Seal Holders

Catholic Charities of Buffalo
Crisis Services
Educate the Children, Inc.
Friends of Night People
Helping Hounds Dog Rescue
Hunter’s Hope Foundation
Joyful Rescues, Inc.
Roswell Park Alliance Foundation
United Way of Greater Rochester
United Way of Northern New York
Water for South Sudan

Other BBB Accredited Charities

Association for the Blind & Visually Impaired - Goodwill of the Finger Lakes
CURE Childhood Cancer Association
Food Bank of Central New York
Greater Niagara Frontier Council, Boy Scouts of America
Jewish Family Service of Buffalo and Erie County
Literacy New York Buffalo-Niagara
Lollypop Farm, Humane Society of Rochester and Monroe County
Mohawk Hudson Humane Society
Parks and Trails New York
United Way of the Adirondack Region
United Way of Tompkins County

**The organizations listed above are located throughout Upstate New York and have met the 20 Standards for Charity Accountability as of December 2019**

Please visit Give.org for the most updated list of Accredited Charities.
10 Tips to Avoid Scams

1. Never send money by wire transfer or through a cash sending app to someone you have never met in person.

2. Do not click on links or open attachments in unsolicited e-mails. If you were not expecting to receive an e-mail, it’s possible the link could contain a virus.

3. Make sure you protect your computer with antivirus software as a line of defense in case a virus tries to take over your system.

4. Don’t believe everything you see. Scammers are great at mimicking official logos, fonts, and other details. Just because a website or e-mail looks official does not mean it is.

5. Don’t buy items online unless the website has “https” in the URL. The extra ‘S’ is for “secure” and indicates the company has taken extra steps to secure your information. You will also see a small lock icon on the web address bar. It is best to deal with businesses online that also have a physical location should you have any issues.
6. Never share personal identifiable information with someone who has contacted you unsolicited - this could be by phone, e-mail, or on social media.

7. If somebody in person, online, or over the phone is making an emotional plea, be skeptical of his or her true intentions. Scammers will use high-pressure sales tactics to instill fear or empathy.

8. Use secure, traceable transactions when making payments for goods, services, taxes, and debts. A gift card is never an acceptable form of payment unless it is a store gift card and you are using it at that store or on the retailer’s website.

9. Whenever possible, work with businesses that have proper identification, licensing, and insurance. BBB.org is a great place to start in your research.

10. Be cautious about what you share on social media. Check your security setting on your social media account to make sure only people you accept as your friend can see your content.
BBB is here to help!
Reach out to any of our specialists for questions about BBB’s Services.

800-828-5000
info@upstatenybbb.org
BBB.org

Stay connected!
Follow us on
Instagram, Facebook, LinkedIn, and Twitter.