Spot and Avoid Common Scams

The most common types of scams will target you through emails (phishing), text message (SMSishing or smishing) or calls. The scammer may:

- Instruct you not to trust the bank
- Pressure you to send money right away
- Threaten to arrest you or have charges brought against you
- Instruct you to purchase gift cards and provide codes as a form of payment
- Ask you to deposit a check that overpays for something you're selling, then ask you to return the difference
- Request your banking or identity details to get payment

Signs of Fraudulent Emails

- The message is missing your name
- Appear to come from a legitimate source. Never rely on the name or address in the "From" field, as this is easily altered.
- Say they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- Has spelling and grammatical errors
- Asks you to confirm personal information
- You are pressured to act now – or something bad will happen

If you suspect you have received a fraudulent email, do not click on any links or attachments. Delete the email, do not respond as that will alert the scammers that the email is active and you may receive additional scam emails from them. Go directly to the website to login and check your account status. Do not log in through the suspicious email.

Common Scams

Grandparent Scam

Scammers will pose as a relative or representative of a relative (such as a lawyer or law enforcement agent). The scammer explains someone is in trouble and needs their grandparent to send them funds that will be used for bail money, lawyer's fees, hospital bills, or another fictitious expense. They may ask you to wire money or buy gifts cards and give them the numbers. Resist the urge to act immediately, no matter how dramatic the story is. Call a phone number for your family member or friend that you know to be genuine. Check the story out with someone else in your family or circle of friends, even if you've been told to keep it a secret.

IRS Scam/SSA Scam/ Imposter Scam

Scammers will pretend to be a government agency such as the Internal Revenue Service or the Social Security Administration. They will call or leave voicemails saying you owe money and you'll be arrested if you do not pay right away. Hang up immediately if you receive one of these calls. The IRS and SSA will never call you unsolicited. All notices from the IRS come by mail. Your social security number cannot be suspended and the SSA will never tell you to wire money, send cash or put money on a gift card. If you think you may owe the IRS back taxes, call the IRS at 800-829-1040 or visit irs.gov/balancedue.

Charity Scam

Charity scammers may pressure you to give right away and request payment by cash, gift card or wire transfer since they know those methods are harder to trace. Another red flag will be thanking you for a donation to make you think you've already given to their cause. Keep a record of your donations for future reference. Scam charities will mimic real non-profits and contact consumers through direct mail, well-designed websites and by phone. Veteran's and natural disaster relief causes seem to be most imitated and charity scams are especially active during the holiday season. Always do your research before giving to ensure an organization is legitimate. Use resources such as the Better Business Bureau's Wise Giving Alliance, Charity Navigator and CharityWatch to view ratings, reviews and tax and financial data for non-profit organizations.

Tech Support Scam

Phone Call – scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist.

Pop-up Warning – Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help. Real security warnings and messages will never ask you to call a phone number.

Romance Scam

Signs of a romance scam include quick professions of love, claims to be overseas for business or military service, claims to need money for emergencies, hospital bills or travel. Scammers will make plans to visit but back out at the last minute due to an "emergency". Ask the person a lot of questions and watch for inconsistencies. Check their photo using Google's "search by image" feature. If the same picture shows up elsewhere with a different name attached to it, that's a sign the scammer may have stolen it. Cut off contact immediately if you begin to suspect that the individual may be fake and notify the dating site or app of the fraudulent profile.

Overpayment Scam

If you receive an overpayment for an item you are selling with a request to deposit the check and return the overpayment via wire or gift card it is a scam. A legitimate buyer would never overpay. Other red flags include having someone else pick up the item because the buyer is out of town or unavailable.

Free Sample/Trial Scam

Never pay for a freebie! A freebie isn't a freebie unless it's free! If a website asks for your credit/debit card information to receive a free item/information read the fine print. You are often agreeing to be charged monthly for product that you may or may not receive. Unless you are actually making a purchase, there is no need to share your card information. In addition, these sites are often harvesting your personal information to sell to other companies.

Debt Relief Scam

A sign of a debt relief scam is if they ask you to pay before they have done anything to help you. A legitimate debt relief company will not make you pay upfront because it is illegal. If you receive a call from a debt collector claiming you owe money, ask for a validation notice which says what you owe and to whom. If you are struggling with debt you can speak to your creditors directly to negotiate a modified payment plan or talk to a Bank of the Rockies lender about a debt consolidation loan.

Lottery/Sweepstakes

Fraudulent email will claim your email address was randomly picked to participate in a drawing. A red flag would include being asked to prepay fees or taxes in order to receive the prize you supposedly won.