



01/20/46

DITCH THE PITCH

a guide for guarding against scams

A Publication from the SC Department of Consumer Affairs



Carri Grube Lybarker
Administrator/
Consumer Advocate

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

293 Greystone Boulevard Suite 400
P. O. BOX 5757
COLUMBIA, SC 29250-5757

PROTECTING CONSUMERS SINCE 1975

Commissioners
David Campbell
Chair
Columbia
W. Fred Pennington, Jr.
Vice Chair
Simpsonville
Mark Hammond
Secretary of State
Columbia
James E. I. Lewis
Myrtle Beach
Jack Pressly
Columbia

TABLE OF CONTENTS

Dear Fellow South Carolinian,

Thank you for taking this step to arm yourself with the tips you need to spot and avoid scams. Education is, and always has been, a large part of the South Carolina Department of Consumer Affairs' mission. We understand navigating the ever-changing marketplace can be a daunting task. And with the rapid development of technology, scammers are more active (and more successful) than ever. It is with that fact in mind that SCDCA created this guide to avoiding scams.

"Ditch the Pitch" is meant to help you get ahead of the fraudsters. It also serves as a call to action; encouraging you to "beware and share" this information with your friends and family. You play an invaluable role in helping us warn more of our citizens about scammers. Thank you!

With Warm Regards,

Carri Grube Lybarker, Esq.
Administrator and Consumer Advocate



- scam red flags 2
- roadmap to avoid scams 3
- spoofing - scammers tricky tactic 4
- phishing - fake emails & text messages 6
- internet and social media scams 8
- keep digital devices safe 11
- other popular scams 12
- does a scammer have your information? 18
- important contact information 19
- other scdca education 20
- help us spread the word 21

No matter the scam... **THE RED FLAGS ARE THE SAME**

We may not be able to know every scam out there, but if you know the red flags, you can avoid getting scammed. Here are the most common signs of a scam:



Scammers PRETEND to be someone you know or recognize.

Whether it's a government agency, business or organization you know, scammers love to act like people they think you'll trust. They may even claim to be your "friend" on social media.



Scammers say there's a PROBLEM or a PRIZE.

Playing on your emotions is a key scammer tactic. They might say you're in trouble with the government, that you owe money or someone in your family had an emergency. Some scammers say there's a problem with a financial account and you need to verify information. Others say you won money in a lottery or sweepstakes, but you must pay a fee to get it.



Scammers PRESSURE you to act now.

Scammers are in a rush to scam you before you can catch onto their act. They want you to act before you have time to think. They might threaten to arrest you, sue you, or shut down your accounts. Others say the "deal" or "opportunity" will go away unless you act now.



Scammers tell you to PAY in a specific way.

Scammers love to ask for payment in ways that are difficult to trace. These include wire transfers, prepaid debit cards, gift cards, cryptocurrency and payment apps. Some fraudsters will send you a fake check, tell you to deposit it, and then send them money back.



Roadmap to **AVOID SCAMS**

1

Don't answer calls or respond to text messages from numbers you don't know. Block these numbers as they come in.

2

Don't give personal or financial information in response to a request you didn't expect.

3

Don't fall for high pressure tactics. Anyone who pushes you to make a decision, pay or give over personal info is likely a scammer.

4

Know the forms of payment scammers like to use. Avoid methods that are difficult to trace and are as good as cash.

5

Think something is suspicious? Stop and talk to a friend, family member or neighbor about what happened.

SPOOFING - SCAMMERS TRICKY TACTIC



Spoofing is when scammers mask where they are contacting you from or pretend to be someone you know. It first started with phone calls, where someone's phone number could be replaced with any phone number they wanted. Now, spoofing applies to every form of contact. They will spoof in any way they can.

PHONE NUMBERS



Scammers disguise who they really are when they call or text, making the information on your caller ID show a number they choose. "Neighbor" spoofing makes their phone number look as if it's coming from your area. They may even use a number from a company or a government agency you already know and trust.

EMAILS



Scammers create an email message with a fake address in hopes of tricking you into thinking the email came from someone other than them.

"Display name spoofing" shows the name of the person being impersonated (John Doe) but not the sending email address. You would have to click or hover over the displayed name to see the actual email address. Scammers can also spoof the entire email address or just the domain name (what follows the "@" symbol).

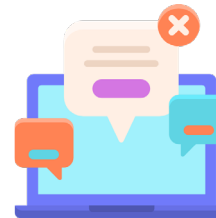
SOCIAL MEDIA & WEBSITES



A scammer can easily fake a social media profile or website by stealing pictures and information from a person or business to act as them. This tactic is often used by scammers claiming to be looking for love, renting out a vacation home or selling fake goods or services.

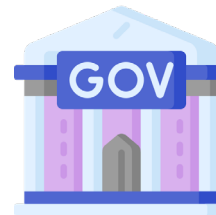
Use Caution: Just because a profile or website looks real or legitimate and has convincing photos does NOT mean it's real. Anyone can make a convincing website or profile.

COMPUTER POP-UPS



You're shopping online and you get a pop-up saying they detect unusual activity. Scammers try to trick you into clicking. They will even create ads that look like your virus protection services or for products at rock bottom prices.

PEOPLE YOU TRUST OR LOVE



Government agencies, charities, businesses, the list goes on. Scammers are going to try to use the well-known names of anyone they can to gain your trust. They could even act like your co-workers or loved ones.

PHISHING - FAKE EMAILS & TEXTS

What is phishing?

Phishing is a scam where a fraudster pretending to be a person, organization or business you know sends either an email or text asking for personal information. The scammer may try to steal information like your passwords, financial account numbers or Social Security number.

Sometimes scammers will already have some information about you and use that to make themselves more believable - this is called **spear phishing**.

SPOT A PHISHING ATTACK

Phishing emails and texts range from obviously fake to very convincing. Here are some signs that it is fake:



First time contacts - It's normal to get a message every now and again from someone you don't know, but it can also be a sign of phishing. When this happens, take a moment to carefully look at it before you click any links or respond.

Generic greetings - If it's an organization you know and work with, or a loved one, they should know your name. If the message starts with "Dear customer" or some other generic greeting, that's a sign of a scam.

Act now - or else! - Plenty of emails will claim you "won a prize" or your "account has been compromised." Some ask you to "confirm," "update" or "verify" your personal information and logins. No matter what tactic is used, the scammer wants you to act now!

The domain doesn't match - The domain is everything after the "@" sign in an email address. Emails may claim to be from a well-known company like Microsoft or your bank, but if the domain doesn't match the business name, be suspicious. Also watch out for a hard to catch misspelling like "@microso0ft.com" where the letter "o" has been replaced with a zero.

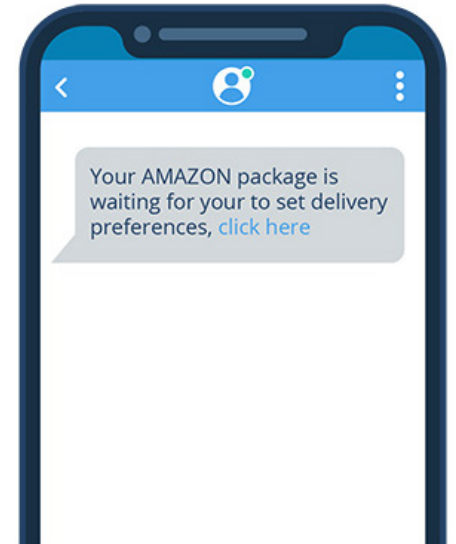
REPORT A SCAM

If you get an **unwanted text message**:

- 1 Forward the text to 7726 (SPAM).
- 2 Report it on the messaging app you use. Look for the option to report junk or spam.

If you get a **phishing email**:

- 1 Forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.
- 2 Notify the person or company being impersonated about the scam.



DO'S & DON'TS



- Do not reply to any message that asks for personal or financial information.
- Do not open any attachments or click any links.
- Do not call or text back a number contained in the message.




- Use antivirus software and a firewall. Make sure to regularly update all of your device's software.
- Carefully review your personal and financial statements. Review your credit report at least once a year by visiting www.annualcreditreport.com or calling (877) 322-8228.

INTERNET & SOCIAL MEDIA SCAMS

When you see the red flag icon, it's a reminder that the common red flags from page 2 apply. Phishing and spoofing apply to ALL the scams you see from here on out, too. Be on guard!

ONLINE SHOPPING



The Pitch: Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a legit retail site. All the common red flags apply. 

the defense

- Always shop on secure websites. Look for the "s" after the "http" and the lock to the left of the URL.
- Only use a credit card when shopping online or use secure payment services like PayPal.
- Beware of prices that are too good to be true.
- Review your financial statements and keep your receipts.

JOB LISTINGS

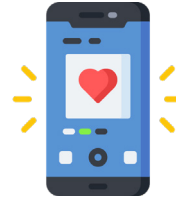



The Pitch: Scammers advertise jobs the same way legitimate employers do: in ads, on job sites, and on social media. They promise you a job, but what they want is your money and your personal information. 

the defense

- Steer clear of offers that come through the mail with a check included or that ask for payment upfront for background checks or other items.
- Look for a legitimate secret shopper job through the Mystery Shopper Providers Association by visiting mspa-americas.org.
- Never cash a check from someone you don't know and wire the money.

DATING/ROMANCE




The Pitch: There are plenty of fish in the sea, but there are unfortunately some sharks, too. Don't be so quick to believe that an online admirer is the real thing. They often steal the names and photos of soldiers or claim to be a person of high status abroad. Fraudsters may also pretend to have common interests to reel you in. 

the defense

- Talk to someone you trust about your new love interest.
- Scam artists use a wealth of excuses and sob stories to try to get cash from you. Never send your hard-earned money to someone you have not met.
- Look out for poor grammar and/or spelling.
- Be skeptical of people who ask for money.

AUCTION/AD SITES



The Pitch: Sites like eBay, Craigslist and Facebook Marketplace can be great tools for buying and selling. Scammers also love them. Often a fraudster will send a check in an amount above the asking price of an item, tell you to cash the check and send them the rest back. Once you've done it, the check bounces and you're on the hook. 


the defense

- Never cash a check for more than the selling price.
- Request a check drawn on a local bank so you can make sure it is valid.
- If you can, sell to local buyers and only accept cash.
- If you get scammed, report the person to the site you are using.

INTERNET & SOCIAL MEDIA SCAMS

SURVEY & GIVEAWAY SCAMS




The Pitch: Survey scams take many forms: a call, text, email, online ad or social media post inviting you to participate in a poll or questionnaire. Scammers might impersonate well-known businesses. Sorry to burst your bubble, it's a scam. 

the defense

- Don't click on links or respond to unexpected messages — including ones offering free items.
- If you think it could be legit, contact the company using a website or phone number you know is real.
- Remember, if it sounds too good to be true, it probably is.

TECH SUPPORT



The Pitch: Scammers contact you claiming to be computer techs working with well-known companies like Microsoft. They say your software needs to be updated or you have viruses to trick you into giving them remote access to your device or pay for software you don't need. Their goal is to take your money or personal information, not protect it. 

the defense

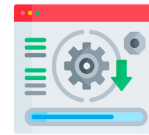
- Don't give control of your computer or passwords to a third party who calls you out of the blue.
- Don't trust online search results. Scammers often place online ads and pay to boost search results so their information appears above legitimate companies.
- If you need tech support, look for a company's contact information on their software package or on your receipt.

KEEP DIGITAL DEVICES SAFE



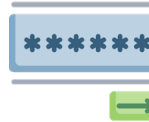
Think Before You Click!

When you see a link, think before you click. It could be an attempt to get sensitive information or install malware.



Update Your Software.

Outdated software makes it easier for scammers to hack your device. If you see a software update notification, don't wait to do it! Better yet, turn on automatic updates in your device settings.



Use Strong passwords.

Use passwords that are long and different from each other. Use a password manager to generate and remember different, complex ones for each of your accounts. It will also encrypt passwords. <https://staysafeonline.org/online-safety-privacy-basics/password-managers/> is a great resource for password managers.



Use Multi-factor (Two-factor) Authentication.


You need more than a password to protect your online accounts, and using multi-factor authentication helps keep hackers out. This requires an extra step after entering in your password — like a temporary code sent to your email or by text to verify it's you.

For more cybersecurity tips, read SCDC's full "[Cybersecurity Basics](#)" flyer.

OTHER POPULAR SCAMS

LOTTERY/SWEEPSTAKES




The Pitch: You get a call, an email, a message or a letter in the mail that says you've just won \$5,000! Or maybe even \$5 million, a fabulous diamond ring, or luxury vacation. Sound too good to be true? It's a lottery and sweepstakes scam. 

the defense

- Don't respond to calls, emails, messages or letters about a foreign lottery.
- Ask yourself - "Did I enter or buy a ticket to win?" No? Then you can't win!
- Never send money to claim a prize. Legitimate lotteries and sweepstakes will not ask you to pay a fee to collect your winnings.
- Don't play along with the scammer. It will only make them reach out more!
- Never cash or deposit a check for someone and send money back to them.

HEALTH FRAUD




The Pitch: It might be an offer for new durable medical equipment, "free" DNA swab testing or a claim that your benefits are expiring and you need to give over information to renew. 

the defense

- Be wary of ads for free medical services or products.
- Remember, Medicare and Medicaid will never call and request your personal information over the phone.
- If called, do not agree to enroll in health insurance plans or to get healthcare products over the phone. Ask for information in writing.
- Reach out to your doctor if you are interested in a certain test, screening or healthcare product.

TAX SCAMS




The Pitch: Fraudsters often pose as the IRS or, more recently, as the state Department of Revenue to scare and trick you into disclosing personal information or sending them money. 

the defense

- Remember: the IRS will not call, email, text or message you requesting credit or debit card numbers, or a specific payment method.
- Reach out to the IRS or state Department of Revenue at a number or email you know belongs to them when you are contacted about a bill or tax refund by email, text or social media.
- Always check your tax preparer's license and qualifications before they do your taxes.

GRANDKID/FAMILY SCAMS



The Pitch: You get a phone call claiming to be a grandchild or another close relative who is in trouble and they need money NOW! Or, it could be a "lawyer" saying they need immediate payment to help your family member. They will tell you not to call the police or tell anyone in your family. 


the defense

- Verify that it is your family member by contacting them at a number you know belongs to them.
- Call another family member to check out the story.
- Resist pressure to send money quickly and secretly.
- Check your social media settings and limit what you share publicly.

OTHER POPULAR SCAMS

FAKE DEBT COLLECTORS




The Pitch: The scammer will try to get you to pay or settle a debt you supposedly owe. The fraudster may ask you to pay a fraction of the amount, immediately, over the phone. In exchange, the debt will be forgiven. The scammer may have your personal information, making the claim seem true. 

the defense

- A legitimate debt collector will not make threats to put you in jail or contact your employer, family or friends.
- Ask for something in writing from the “debt collector” so you can verify the claim. Federal law requires debt collectors to send you a letter about the debt.
- Check your credit report to see if the debt is there. Get a free copy of your credit report at www.annualcreditreport.com or by calling (877) 322-8228.

HOME REPAIR SCAMS




The Pitch: The scammer may offer you a discounted deal claiming they have left over materials from another job. Or they may show up after a disaster. They say something's wrong that they can fix, you need to make a decision NOW and pay upfront. 

the defense

- Do not pay in full upfront and never pay cash or by wire transfer.
- Make sure all details are in a written contract you understand and get a completed copy.
- Check with the SC Department of Labor Licensing and Regulation at www.llr.sc.gov to verify licensure. They may need a county or city license, too.
- Ask friends or family for recommendations. Do an internet search and check consumer.sc.gov and bbb.org for complaints.

FAKE CHARITIES




The Pitch: Fake charity scammers may choose a name similar to a legitimate charity or create a fake ID in the name of an actual charity, complete with a copy of the logo. They collect “donations” for their scam by setting up a table at a local mall or on the street, knocking on your door or making an email or telephone request. 

the defense

- Check the Secretary of State's Office list of charities. Visit sos.sc.gov or call (888) CHARITI (242-7484) or (803) 734-1790.
- Avoid charities soliciting door-to-door.
- Ask any cold caller to send you information about the charity before giving.

INVESTMENT/CRYPTO



The Pitch: You meet someone and after chatting for a bit, your new friend has an incredible investment opportunity for you! The investment could be a regular investment or in cryptocurrency. 


the defense

- Legitimate offers will not disappear overnight. Do not feel pressured to make a quick decision.
- Involve a family member or professional when someone promises big profits or quick returns on an investment.
- Think twice if you are told “your profit is guaranteed” or “there is no risk.”
- Don't trust testimonials. They can be faked and you can't verify them.
- Ask for information in writing before you commit to invest. If you must recruit your friends to get involved, send money offshore, or open an e-currency account to transfer money, it's a scam!

OTHER POPULAR SCAMS

RENTAL SCAMS




The Pitch: Whether you're looking for a vacation rental or a place to live, be on guard against scammers who list fake rentals. Some advertise rentals that either don't exist or aren't available. Others hijack a real rental or real estate listing by copying it and placing an edited ad on another site. 

the defense

- Always meet with the landlord and tour the property. If you can't visit it yourself, ask someone you trust to go for you.
- Background the property. Search online for complaints or multiple listings using different names. You can also reverse image search the listing's photos to see if they are stock images or copies from another posting.
- Do not provide payment prior to finalizing a lease, aside from an application fee.

GOVERNMENT GRANTS




The Pitch: You're approached saying you may qualify for free money from the government. Some say you can use the money for pretty much anything you want. All you need to do is give over your information. They might even promise a refund if you aren't happy. 

the defense

- The government won't reach out to you about grants.
- Don't pay for a list of government grants. The only legit listing is at www.grants.gov and it's free.
- Don't pay any up-front fees. No government agency will ever ask you to pay to get a grant.

CRIME/WARRANT & JURY DUTY




The Pitch: The scammer says you can avoid arrest for a crime you've committed or jury duty you've missed by paying a fine right now. The scammer may have information about you, names of law enforcement officers, court officials, and judges to appear more legit. Scammers may even "spoof" a phone number on caller ID so the call falsely appears to be from a court or law enforcement agency. 

the defense

- **Remember:** You will never receive a phone call, email, text or social media message from a government agency that tells you about a warrant for your arrest or demands money and/or personal information.
- Ask for the warrant number, person's name and name of agency they work for. Reach out directly to that agency at a number or email you know belongs to them.
- Information about jury duty, including missed summons, will come through the mail, not a phone call. Call your local courthouse if you are unsure about jury duty claims.

FINANCIAL AID / SCHOLARSHIPS



The Pitch: Going to college or vocational school can be expensive. Scammers say they will help you get financial aid or scholarships, but they're really just trying to get your money or personal information. 

the defense

- Legitimate scholarship programs do not require upfront fees.
- Don't trust people claiming to have special access to programs or forgiveness options.
- Fill out the free FAFSA form at studentaid.gov to apply for financial aid.

DOES A SCAMMER HAVE YOUR INFORMATION?

If you shared your information with a scammer, there are some steps you can take to minimize the damage!

STEP #1: FRAUD ALERT

Place a Fraud Alert: It's FREE, stays in place for one year and requires a business to take steps to verify that it is in fact you that is applying for the good or service. Call one of the credit bureaus and they'll notify the other two.

STEP #2: SECURITY FREEZE

Consider a Security Freeze: It's FREE and will prevent a business from accessing your credit report for new products or services, unless you temporarily lift the freeze. You must call each of the credit bureaus to do this.

Equifax: (800) 685-1111
TransUnion: (800) 680-7289
Experian: (888) 397-3742

You can use these numbers for both the fraud alert and the security freeze.

STEP #3: MONITOR

Monitor Financial and Personal Statements: Be sure that your bills and statements are arriving on time and are correct. ID Thieves don't just use your information to get money. Your SSN can be used to receive:

- Government benefits
- Driver's License / ID
- Tax Refund
- Medical Benefits

Monitor ALL of your statements, and always be on alert for any suspicious or unexpected letters or phone calls!

IMPORTANT CONTACT INFORMATION

FOR ADDITIONAL HELP:

Contact the South Carolina Department of Consumer Affairs' ID Theft Unit for more tips on dealing with identity theft and scams.

(844) 835-5322 (toll free in SC)

(803) 734-4200 or consumer.sc.gov

REPORT SCAMS TO:

SCDCA: (844) 835-5322 (toll free in SC), (803) 734-4200 or consumer.sc.gov

FTC: (877) 382-4357 or ftc.gov/complaint

FCC: (888) 225-5322 or consumercomplaints.fcc.gov

DO NOT CALL REGISTRY:

Add your number to the **Do Not Call Registry:**
Donotcall.gov or (888) 382-1222

STOP UNSOLICITED OFFERS:

Opt out of snail mail marketing:

Dmchoice.org

Opt out of preapproved credit offers:

www.optoutprescreen.com or call (888) 567-8688

FREE CREDIT REPORTS:

Get a copy of your FREE credit report:

www.annualcreditreport.com or call (877) 322-8228

SCDCA OFFERS FREE PRESENTATIONS!



Education is a core component of SCDCA's mission. We give in-person presentations and webinars for consumers and businesses. All of our presentations are **always free**.

Request a presentation by going to consumer.sc.gov and clicking "How Do I..." and choosing "Request a Presentation?" or email scdca@scconsumer.gov or call (803) 734-4200 for more information.

POPULAR PRESENTATION TOPICS

- General ID Theft & Scams Basics
- Social Media Safety
- Cybersecurity Basics
- Credit Reports & Scores
- Financial Literacy Basics
- Consumer Protection and Law
- Debt Collection
- Landlord/Tenant Act

WANT TO STAY INFORMED?



Get email updates, request a presentation, request more free brochures like Ditch the Pitch to be sent to your mailbox, and connect with us on social media.

You can sign up by going to consumer.sc.gov, scrolling down and clicking the button that reads "Learn More" below the "Stay Informed" header or you can scan the QR code below with your smart phone camera. It will give you the direct link to sign up.



HELP US SPREAD THE WORD

Use this magnet as a reminder to warn your friends, family and others about the dangers of scams.



Scam reports help SCDCA identify fraud trends and get the word out to consumers on what to avoid. There is no report too small!



Find the latest scam alerts and news here.

twitter.com/scdca



Check out our YouTube channel.

youtube.com/scdcatv



Look here for updates & educational materials.

facebook.com/SCDepartmentofConsumerAffairs



South Carolina

DEPARTMENT OF CONSUMER AFFAIRS

PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov

© South Carolina Department of Consumer Affairs, 2024.

This brochure may be copied or reproduced for non-commercial, educational purposes, so long as no changes or modifications are made.