South Central Power
Stop Scams

Don't get tricked. People around the country have been receiving emails and phone calls from scammers. South Central Power wants to help you keep your money and prevent scams. Review the helpful tips below.

Know South Central Power's Procedures

- Members should only give payment information over the phone if they initiate the call. Callers who give short deadlines and threaten to cut off service within an hour or two are probably running a scam. South Central Power has a set routine for collecting payments from members.
- South Central Power will mail a termination notice if a bill is past due.
- South Central Power only calls members who owe a past due balance.
- South Central Power usually uses an automated phone system with a recorded message. Occasionally South Central Power employees make personal "collection" phone calls but will transfer the member to our automated phone system to make their payment.
- Collection calls are made about seven days before service is scheduled to be terminated.
- South Central Power does not make collection calls or terminate service on weekends or holidays.
- If service is going to be terminated, a South Central Power employee will knock on the member's door before turning off service.

If a member is concerned about the status of an account, a South Central Power member service representative can provide helpful information. Members should call 800-282-5064. The phone number is printed at the top of the billing statement and South Central Power's member service representatives are available M-F 8 a.m. to 5 p.m.

Because South Central Power does initiate automated collection calls, and members can choose to make a payment over the phone, some phone calls are legitimate.

South Central Power wants to prevent phone scammers from victimizing members by simplifying the payment process. South Central has a number of ways members can pay their bills:

- Members can use budget billing to pay the same amount every month.
- Members can use AutoPay to have payments made automatically each month with a credit or debit card.
- Members can easily go online to make weekly payments if that helps them with their personal budget.

- Members can pay online though the MyAccount section of the website.
- Members can pay over the telephone through the IVR 24/7 or by speaking to a member service representative during regular office hours (M-F 8 .m. to 5 p.m.).

Avoid e-mail scams

South Central Power's e-mails contain specific information and distinct colors. Do not open emails from unfamiliar sources.

- If an e-mail looks suspicious, it may contain malware or links to a virus-infected website.
- Members can simply delete the suspicious e-mail and contact South Central Power by phone or log on to the bill payment website.
- Members should not provide personal information, credit card, debit card, banking information or user names and passwords in an e-mail.

Avoid Phone Scams

Know what you owe. You know your mortgage company, your phone company, credit card company, electric utility and anyone you regularly pay for services. You know how much you pay and when you pay. If you know you've paid your bills, and someone calls to demand payment, just hang up.

You can always call your service provider at the number printed on your bill. Every legitimate company that issues bills will have a way for you to contact them printed on your bill.

Legitimate companies will normally send you a letter in the mail if there is an issue with your payment. They may also call you, but you don't have to talk to them. Just hang up. If you think you might owe the company money, **call them at the phone number printed on the bill**.

Several phone scams that have been operating recently:

- Caller claims to have detected a virus on your computer, tells you to go to your computer and they will walk you through several steps which give the caller access to your computer and your personal information.
- Caller claims to be from a solar company; don't give them your electric account information.
- Caller claims your grandchildren/niece/nephew/cousin is in trouble, or hurt in an accident, or arrested, and if you provide money or a Green Dot card the caller will take care of him/her.

- Caller claims to be able to access an inheritance that someone left you. Caller asks you for a small fee or percentage to process paperwork.
- Caller claims you owe money and asks you to meet at the local CVS or other store to make payment.
- Caller claims to be raising funds for Ebola virus/orphans/widows/whatever; don't give them your credit card or checking account information.
- Caller claims to be from the IRS, threatens legal action and arrest. **Remember, once you give a scammer money, they will continue to call and harass you.** Government agencies do not call or e-mail people; government agencies send letters via the U.S. mail.
- Do not provide personal, financial or account information to unauthorized callers.
- Do not provide Green Dot, Western Union or Moneygram payments to unauthorized callers.
- Never meet unauthorized callers at a local store or bank to make a payment – your personal safety could be at risk.

Scammers are difficult to recognize.

- Scammers can sound like really nice people on the phone. They may talk to you about your kids and grandkids, your church, shows you watch or where you live. Don't tell them how old you are, or where you live, or where you bank or shop. Don't tell them about your kids and grandkids. They just want your money.
- Conversely, scammers who call you may be very mean on the phone, threatening to call the police or take you to court. You don't have to talk to them. Just hang up.
- Scammers frequently prey on the elderly and people who speak English as a second language.
- Scammers target businesses. Businesses usually have higher monthly bills and scammers will take advantage of that, claiming the business customer owes $1,500 rather than just $200. Businesses may have more than one person authorized to pay bills, and scammers exploit the lack of communication between employees and business owners.
- Scammers can make the name of the utility appear on a customer's caller ID.
- Scammers can trick people by duplicating voice recordings and imitating utility phone systems.

Avoid Mail Scams

Are you a Sweepstakes Winner? No, you're not. Throw that junk mail away.

Don't respond to mail that you receive if you are not familiar with the company or the sender.

South Central Power
Stop Scams

Scammers will send mail advising you of “pending legal action,” and offering legal services. Don’t fall for it. If you believe the letter is legitimate, ask a friend or relative, or call a lawyer. Don’t call the phone number on the mailer.

Once you respond to a mailer, your name and address will be distributed to other frauds who will send you mail scams or call you.

Avoid E-mail Scams

- E-mails that contain several grammar and spelling mistakes are probably not legitimate.
- If an e-mail looks suspicious, it may contain malware or links to a virus-infected website.
- If you receive a suspicious e-mail, do not open it or click on any links; simply delete the e-mail.
- Do not provide personal information, credit card, debit card, banking information or user names and passwords in an e-mail.
- Do not send personal information, such as your Social Security number or bank account number, in an e-mail.
- If you receive a suspicious or unexpected e-mail, don’t click on any links in the message.
- If you click on an Unsubscribe link in a marketing e-mail, or reply to the message, the marketer will know that your e-mail address is active and may sell it to other companies. Instead, simply delete the message, or mark it as junk or spam.
- Do not share your passwords or other login credentials, especially over e-mail.

Ensure Computer Security

Perhaps the most important safeguard for any computer system is the user. No matter how many protections are in place, careless behavior can still threaten computer security and compromise sensitive information. Here are some ways you can protect your personal information at home.

- Install anti-virus software from a reputable company on your home computers.

- If you have Wi-Fi in your home, set up a password to prevent neighbors and others from using your Internet access.
- Use strong passwords on any computers and websites that you use. These are any combination of uppercase and lowercase letters, numbers and symbols. Avoid using relatives' names in your passwords, as these are easy to find out. Try Googling yourself to see what information about you is on the web for anyone to see.
- Before downloading any freeware or shareware for your home computer, search for reviews and feedback about the software. Some of these programs have hidden components that gather your personal information while hogging your computer's memory resources and Internet bandwidth.