

MPUA PUBLIC OUTREACH RESOURCES

APRIL 2016

Spring Utility Scams: TIPSHEET and NEWS RELEASE formats

[1. TIP SHEET Format]

SPRING SCAMS BLOOM ANEW

Ah, Spring! Bringing forth the buds, the blooms, the birds. And also – the utility fraud criminals.

Somehow, the change of seasons often seems to prompt a renewal of criminal fraud, and customers of **[YOUR UTILITY NAME]** should be on the alert for phony callers and e-mails trying to scare them into making immediate payments.

A phony contact from one of these criminals usually appears very convincing. The caller sounds professional, or the email has a familiar logo. They say if you don't pay your utility bills right away, your gas, electricity or water will be shut off. They ask you to pay now, using a specific – maybe unusual – method.

Be warned: The call or email is a trick to steal your money. Utility companies, consumer protection agencies, and the Federal Trade Commission regularly receive complaints from consumers about utility bill scams.

[YOUR UTILITY NAME] does not make calls demanding immediate payment. **[ADD any other BRIEF description on how your utility makes customer contacts].**

Here are a few signs you are dealing with a scammer:

- You get a call or an email claiming your services will be cut off unless you call a number or click on a link and give your account information. **[YOUR UTILITY NAME]** won't ask you to send your account information by email.
- Someone calls demanding you wire the money or use a prepaid or reloadable debit or gift card to pay your bill. Legitimate companies don't demand you use those methods to pay.
- The caller tells you to call a phone number and give your credit, debit or prepaid card number. If you do that, the scammer can access the money from your credit, debit or prepaid card, and you can't trace where your money went. Once it's gone, it's gone.
- Fake utility calls of this kind often come after hours or on weekends, outside of the utility's usual business hours. Scammers also may use caller ID equipment that spoofs the utility's identity, or impersonate voice recordings to appear to be from the utility, then persuade customers to make a callback to another number for payment.

If you get a call, email, or personal visit from someone about your utility service:

- Never give out your Social Security Number, credit card number or banking information to anyone requesting it over the phone or at your home unless you initiated the contact or expected the call from **[YOUR UTILITY NAME]** **[or other utilities].**

MPUA PUBLIC OUTREACH RESOURCES

APRIL 2016

Spring Utility Scams: TIPSHEET and NEWS RELEASE formats

- Never wire money to someone you don't know — regardless of the situation. Once you wire money, you can't get it back.
- Do not click links or call numbers that appear in unexpected emails or texts — especially those asking for your account information. If you click on a link, your computer could become infected with malware, including viruses that can steal information and ruin your computer.
- Never allow anyone into your home to check electrical wiring, gas pipes or appliances unless you scheduled an appointment or reported a utility problem. Always ask utility employees for proper identification. *[add anything brief and specific about your utility's employee identification policy]*
- Make sure you're dealing with **[UTILITY NAME]** before you pay any amount. Confirm where and how to pay your bill.
 - *[UTILITY OPTION: "To determine the status of your account [give details, website for lookup, phone number to call, business hours].*
 - *[UTILITY OPTION: If you fall behind on your utility bill, contact [UTILITY NAME] to see if you can work out a payment plan and a way to keep your service on.*
 - *[UTILITY OPTION: may wish to add brief payment/policy info here, or link to online info on policy]*

If you think a fake utility bill collector or any other scammer has contacted you, report the contact:

- Notify **[YOUR UTILITY NAME]**.
- Call the police *[or specify city/county police here, and correct contact number]*
- File a complaint with the Missouri Attorney General's Consumer Protection Division (online at <https://www.consumer.ago.mo.gov/> or by phone at 1-800-392-8222.) Be ready to include in your complaint any notices received or caller ID numbers for the incoming call.

[2. Similar info in NEWS RELEASE Format]

(For immediate release)

Contact: **[spokesperson]**
[Telephone # of contact]

[UTILITY/CITY NAME] Cautions Customers About Utility Scams

[CITY, MONTH & DATE, YEAR] -- **[YOUR UTILITY NAME]** advises customers to be alert for con artists who may impersonate utility workers and threaten a service disconnection unless a payment is made immediately.

"The change of seasons often brings a renewed cycle of utility-themed scams," said **[Spokesman]**

MPUA PUBLIC OUTREACH RESOURCES

APRIL 2016

Spring Utility Scams: TIPSHEET and NEWS RELEASE formats

[NAME], **[TITLE]** at **[UTILITY NAME]** "**[CITY NAME]** residents and businesses should be wary of any caller, email or visitor who threatens disconnection of utility service unless payment is made right away."

[If your utility/community has reported/received actual scam activity, add any appropriate story/details]

In these scams, the person making contact may ask the targeted victim for a credit card number, to wire money directly, or go to a local store and purchase a reloadable debit or gift card used for phone or online payments. Calls from such swindlers are often received after hours or on weekends, outside of the utility's usual business hours. Scammers may also use caller ID that spoofs the utility's name, or impersonate voice recordings to appear to be from utilities and to persuade customers to make payments. Fraudulent callers may also tell you to call a phone number and give your credit, debit or prepaid card number.

[UTILITY NAME] cautions customers with the following tips if they get a call, email, or personal visit from someone about your utility service.

- Never give out your Social Security Number, credit or debit card number or banking information to anyone requesting it over the phone or at your home unless you initiated the contact or expected the call from **[UTILITY NAME]** *[or other utilities]*.
- Never wire money to someone you don't know — regardless of the situation. Once you wire money, you can't get it back.
- Do not click links or call numbers that appear in unexpected emails or texts — especially those asking for account information. If you click on a link, your computer could become infected with malware, including viruses that may steal information or ruin a computer.
- Never allow anyone into your home to check electrical wiring, gas pipes or appliances unless you scheduled an appointment or reported a utility problem. Always ask **[UTILITY NAME]** employees for proper identification. *[add anything brief specific about your utility's employee identification policy]*

Make sure you're dealing with **[UTILITY NAME]** before you pay any amount. Confirm where and how to pay your bill. **[UTILITY NAME]** employees are not allowed to take payments in the field.

- *[UTILITY OPTION: "To determine the status of your account [give details, website for lookup, phone number to call, business hours].*
- *[UTILITY OPTION: If you fall behind on your utility bill, contact [UTILITY NAME] to see if you can work out a payment plan and a way to keep your service on.*
- *[UTILITY OPTION: may wish to add brief payment/policy info here, or link to online info on policy]*

MPUA PUBLIC OUTREACH RESOURCES

APRIL 2016

Spring Utility Scams: TIPSHEET and NEWS RELEASE formats

If you think a fake utility bill collector or any other scammer has contacted you, report the contact in the following ways:

- Notify **[UTILITY NAME]** by calling **[add any specific phone number or contact info]**.
- Call the police **[add any specific city/county police contact number/info]**
- File a complaint with the Missouri Attorney General's Consumer Protection Division (online at www.consumer.ago.mo.gov or by phone at 1-800-392-8222.) Be ready to include in your complaint any notices received or caller ID numbers for the incoming call.

###