UTILITIES UNITED
AGAINST SCAMS

Tips to Avoid the Most Common Impostor Utility Scams

PHONE

- **Hang Up on Calls from Crooks**
  Hang up if you receive a call demanding immediate payment of a utility bill to avoid disconnection or shutoff. Never be fooled by a phony caller ID; never return a call to the call-back phone number provided by an unknown caller; and never provide any payment or personal information to a caller you do not know. If you have questions, call your utility company at its phone number on your monthly bill or the utility's website.

- **Keep Cell Phones Safe**
  Do not reply to text messages or click on links you receive from people you do not know, and if you receive a message from a friend, consider verifying they meant to send you the link before clicking on it. Never install apps from text messages, and if you have any doubt about a text message, exercise caution and do not open it. Several cellular service providers are now offering free scam blocking, and several smartphone apps are available for download.

IN-PERSON

- **Shut the Door on Scammers**
  Be suspicious of anyone who arrives at your home or business without an appointment demanding immediate payment, offering utility products or services, or requesting access to your dwelling to check your electrical wiring, water pipes, natural gas pipes, appliances, or other utility-related issues. Do not let unknown individuals into your home. If you have any questions, call your utility company.

- **Always Ask for Proper Identification**
  If you feel you are in personal danger, call 911. Always ask to see a company photo ID, and if you have doubts about a person at your door claiming to be from your utility, call your utility company to verify their information and work to be done before allowing them into your home or business.

INTERNET

- **Delete Suspicious Emails**
  If you receive an email that appears to be from your utility company that you are unsure about, delete it. Do not click on links, open attachments, download pictures, forward it, or respond to it. Be careful in providing information online. If you have questions about such emails, call your utility company.

- **Ensure Website Security**
  A secure website starts with “https://”—remember the “s” is for secure. In general, “http:” websites are vulnerable to attack. Remember the best protection against phishing and malware is being careful about what email attachments you open, keeping software updated and maintained, and installing a quality antivirus program. If you have any questions, call your utility company.