



Cybersecurity and Data Privacy of Advanced Metering Infrastructure (AMI)

'The Digital Foundation to Enhance the Customer Experience'

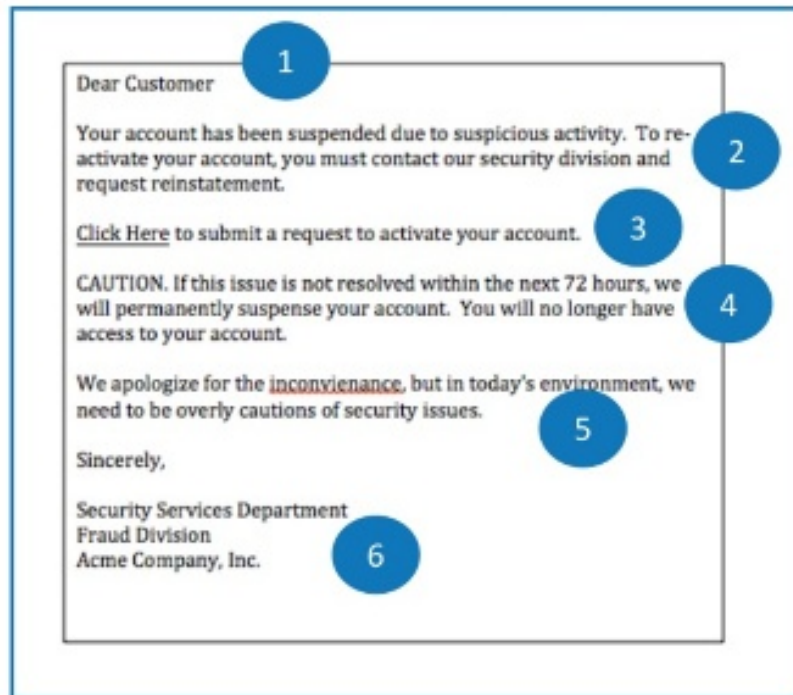
Public Utility Board
Study Session
February 13, 2019



Cyber safety moment

PHISHINGBOX

COMMON PHISHING TRAITS

A screenshot of a phishing email with six numbered callouts (1-6) pointing to specific traits. The email text is as follows:

Dear Customer **1**

Your account has been suspended due to suspicious activity. To re-activate your account, you must contact our security division and request reinstatement. **2**

[Click Here](#) to submit a request to activate your account. **3**

CAUTION. If this issue is not resolved within the next 72 hours, we will permanently suspend your account. You will no longer have access to your account. **4**

We apologize for the inconviencance, but in today's environment, we need to be overly cautions of security issues. **5**

Sincerely,

Security Services Department
Fraud Division
Acme Company, Inc. **6**

1. Generic Greeting
2. Invokes Fear
3. Requires Action
4. Threatening Language
5. Grammar Issues
6. Generic Closing

Objectives

1. How Cybersecurity requirements were reflected in the AMI procurement process
2. How UTS will apply cybersecurity methods to the AMI system
3. Understanding customer data privacy concerns and AMI meter data

Cybersecurity requirements

- External Requirements were modeled from the Federal Risk and Authorization Management Program (FedRAMP)
- Internal requirements were modeled using NIST 800-53 Security Controls
- Over 900 security controls concerning confidentiality, integrity, and availability of the systems were vetted during the procurement phases.



Protecting AMI

System Wide Security

- Multi-Layer Encryption to the Endpoint
- Tamper Prevention and detection
- Time-Windowed Commands
- Pass-through devices
- Behavior Monitoring

Meter Security

- Non-Repudiation
- Modifications must originate from Headend
- All Modifications are logged
- No commands accepted from the field network



Protecting customer data

- Data collected from the AMI meters is the same as data collected from traditional meters. Smart meters have no visibility within the home.
- All data is encrypted from the home to the Headend and digitally verified before being collected.
- Per policy, TPU does not release customer data without prior written consent from the customer. This is published on our website along with the Customer compliant process and is located [Here](#).

Smart Energy Consumer Collaborative

- SECC is a nonprofit organization that works to learn the wants and needs of energy consumers in North America, encourages the collaborative sharing of best practices in consumer engagement among industry stakeholders, and educates the public about the benefits of smart energy and energy technology.



Questions

