



# The Monthly Brief

Volume 8 Issue 8 August 2020

## Disaster Scams

It's hurricane season in Florida and like the pandemic, natural disasters will unleash scammers following headlines in pursuit of their next victims.

Read How The FCC Says It Works:

After any major disaster strikes, scammers impersonate government agencies, calling with offers to help you apply for FEMA assistance or conduct an inspection for a fee.

Scam contractors will show up at doors in affected communities, offering to do post-disaster repairs on the spot, but only if you prepay.

Scammers seek donations on the internet and in person for disaster relief, but what they raise they keep for themselves.

**What You Should Know:**

No government agency will charge a fee to help you get assistance.

Legitimate contractors will not require an on the spot payment.

Scam charity names are often very similar to real charities.

Hang up on callers claiming to be from the government; generally it doesn't work that way. If you get such a call, verify the phone number and Google search it for info.

Get written estimates and check references before hiring. If the contractor's offer is for that day or moment only, walk away.

Research charities before donating using sites like Charity Navigator or Give.org, Charity Watch, GuideStar, and NASCO.

*AARP, FCC, BBB, FEMA

## Follow Us On Facebook

Subscribe: philarcher@sa18.org

## Utility Imposter Scam

In this con, scammers impersonate water, electric, and gas company representatives and threaten deactivation of service without an immediate on the spot payment. These company imposters will typically reach you with a telephone call or knock on your door. In the most common scenario, the scammer informs you that payment is overdue and the service will be turned off if a payment isn't made immediately.

In another version a "representative" may appear at your door in a plausible work uniform claiming that the electric meter is not working properly and must be immediately replaced— at your expense. They may also ask for access to your home to perform "repairs" or an "energy audit" with the intent of stealing your valuables. These cons may also involve promises of energy discounts with the aim of taking your money, personal information, or possibly the account details needed to switch you to another utility provider without your consent (an illegal practice known as "slamming"). Here's what to look for and tips to protect yourself:

***Prepaid cards or wire transfers are a red flag**. Utilities take checks & credit cards.

***Pressure to pay immediately** and may try to get your personal and banking info.

*Hang Up (or close the door) and call customer service at the number on your bill.

***Never allow anyone into your home** without a scheduled appointment or reported problem. Always ask to see company identification

*Source BBB, FPL, OUC

## Account Alert Phishing Scams


Phishing scams have been around for years. Why? Because they continue to pay off for scammers. It's called Phishing because the same email is sent to thousands of people simultaneously hoping someone will "take the bait". To increase the chances you'll bite, scammers pose as large companies with millions of accounts like PayPal (200m), Netflix (180m), Visa (340m) and Bank of America (67m).

Scammers send realistic looking emails claiming to "alert" the receiver to problems with their account. Examples include suspicious activity, declined payments, outdated info, locked account, or purchases you didn't make. By creating fear to act immediately, they hope you'll use an included link to access the account. The link goes to a fake website or login page and will capture email and password credentials. Next they'll ask for personal or financial info required to correct the problem. Just like that the real account has been compromised and they have enough info for further identify fraud.

How to Avoid Phishing Scams. **1. Never follow links in emails**. Logon to your account via the website or app on your phone. **2. Grammar and misspellings** - always a scam if so. **3. Generic Greeting** -The email doesn't include your first and last name or account number, addressed to "Customer" or "Dear". **4. Google it!** Search the content of the message, email address, or the company name with "phishing scam". Chances are you'll find a match. Learn more about account phishing with tips and a video from PayPal a company scammers frequently pose as.

* Source FTC, PayPal