Identify PHISHING
to avoid getting caught!

SPEAR PHISHING
Targets Specific Users

Researches personal and publicly available information to target individual

- **Secure** – your personal information online by setting your social media accounts to private
- **Recall** – if you received similar communications from the sender in the past

DECEPTIVE PHISHING
Disguises as Credible Sender

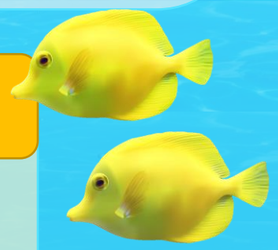
Imitates a legitimate source to steal personal data or login credentials

- **Inspect** – URLs carefully to identify redirection to unknown or suspicious websites
- **Review** – sender's email address for unfamiliar or odd domain names

VISHING & SMISHING
Phishing Over the Phone

Mimics known entities via phone call and text to steal sensitive information

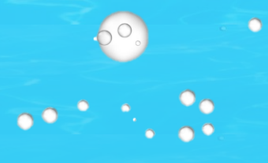
- **Beware** – of false claims of ties to your organization or colleague name dropping
- **Recognize** – pushy and too-good-to-be-true offers like "act fast" and "sign up now"



CLONE PHISHING
Copies a Real Message

Recreates already delivered message and replaces links/attachments with malicious versions

- **Verify** – legitimacy of identical email by contacting sender via phone
- **Compare** – message with original to identify minor grammatical errors and differences to link addresses prior to accessing



ANGLER PHISHING
Phishing via Social Media

Masquerades as a social media customer service representative to gain access of personal data or account credentials

- **Research** – customer service account to ensure they are verified and are the "official account" of social media
- **Contact** – social media's customer service department directly to verify and resolve issue

Search "Cybersecurity Awareness" on our site or contact cybsectrn@hq.doe.gov for more information on Phishing!