Fry a Better Phish

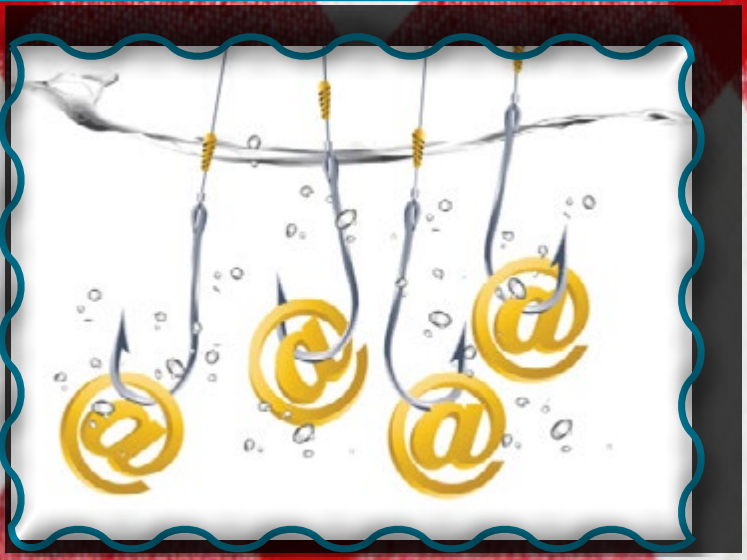
Best Phish Bait on the Market

Phishing is an unsavory social engineering tactic that uses email, malicious websites, or phone calls from criminals posing as trustworthy organizations with the most wholesome of intentions. An attacker might send an email, carefully crafted to look like it's coming from a reputable credit card company or financial institution, requesting personal account information. But take a closer look and these emails definitely smell phishy! They will often suggest that there's a problem with your account to scare you into giving out the information they've requested. ***Don't take a bite!*** Crooks can use the information to poach sizable morsels of your private accounts.

Hard-boiled cyber criminals have become super-savvy at reeling people in, luring them with sneaky links, tantalizing tricks, and seemingly harmless but corrupted attachments. Their emails can appear truly authentic - exactly like they would if they were coming from a real financial institution, government agency, or any other type of service or business. Be careful! Just because it looks gourmet, that doesn't mean it's tasteful!

A Tempting Dish

Phishing attacks usually urge you to act quickly. They might threaten to deactivate a particular account, or state that your account has somehow been compromised or frozen (and frozen phish is never tasty)! They may even insist that an online order you've just made can't be fulfilled until personal information or payment arrangements have been updated. ***Don't get hooked!*** This is just another scare tactic used by foul Internet foes.



Regardless of any network defender's best efforts, it's impossible to prevent every unappetizing phishing campaign. While there is no magic solution for combatting every possible ploy, there are a number of things *YOU* can do to be in-the-know and on the lookout! By following ***these simple recipes***, you can keep yourself safe from freeze-dried phishing shenanigans!

National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

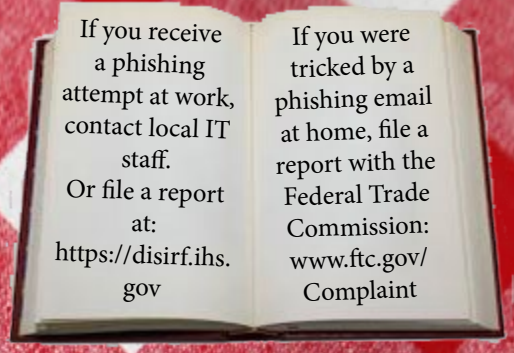
Fry a Better Phish

Recipe #1 - Discover With a Quick Hover

Type of Phish: An email urging you to click on a link, taking you to a website that asks for your password!

Ingredients: One email, a handful of savvy cyber criminals, a dash of social engineering, one fake link, and a pinch of malware.

Directions: Hover over the link **BUT DON'T CLICK ON IT**! Hovering will reveal the actual web address. If it looks suspicious, CALL your local IT staff or EMAIL irt@ihs.gov!!



Recipe #2 - Social Media, Bait to Feed Ya

Type of Phish: Social engineers research your social media profiles to piece together your identity and interests! Then, they lure you into their net by pretending to be someone you know with content that interests you. Accepting the request or viewing the attachment launches their malware!

Ingredients: An array of social media flavors, one sneaky impersonator, malware added to taste.

Directions: Adjust your privacy settings so only friends see your profiles. Always examine senders' email addresses to make sure they're legitimate. Also examine website URLs. If it seems phishy, CLOSE THE PAGE!!

Recipe #3 - Think Twice With Your Mobile Device

Type of Phish: A text message on your mobile device directs you to a fake website asking you for account information... especially the credit cards associated with the account!

Ingredients: One cell phone, a smidgeon of SMiShing, and a heaping spoonful of unsuspecting texters.

Directions: Don't respond to unfamiliar texters requesting personal information. Beware of messages from non-phone-numbers like "4325." That's a tactic scammers use to mask their identity by using email-to-text services that conceal their actual phone number. DON'T RESPOND!!

Recipe #4 - Don't Stall with a Phony Phone Call

Type of Phish: Scammers obtain your name, job title, and contact information from public directories and call you up! Once on the line, they pretend to be tech support and try to confuse you with a healthy smattering of technical terms. Then they ask you to perform a series of tasks on your computer, claiming you've got a virus or software issue!

Ingredients: One telephone, a skosh of data mining, and a sprig of spear phishing.

Directions: Never give personal software information or passwords over the phone! If you get a call from some kind of "tech support," call the company yourself using a phone number you know to be genuine. Hang up and GET OFF THAT LINE!!