A Phishing attack is generally characterized by a lure, hook, and catch

The Lure
The lure is an enticement delivered through email. The email contains a message encouraging the recipient to follow an included hypertext link. The hyperlink often masks a spoofed uniform resource locator (URL) of a legitimate website.

The Hook
The hook is a malicious website designed to look and feel like a legitimate website. The authentic-looking website asks the victim to disclose privacy-related information, such as user identification and password. Often the hook is an obfuscated URL that is very close to one the victim finds legitimate and is really a site under the attacker’s control.

The Catch
The catch is when the originator of the phishing message uses the information collected from the hook to masquerade as the victim and conduct illegal financial transactions.

Today, more than ever, spear phishing attacks are focusing on national security targets and our federal users. For this reason, it is important to understand how to identify a phishing email and what steps to take to prevent identity theft, unauthorized system access, or mission compromise.

Remember to . . .
STOP, THINK, before you CLICK!

Don’t Be Phished!
ONE click could compromise . . .

☐ your personal information
☐ your agency’s information
☐ your computer system
☐ your computer information

Don’t Be Whaled!

“Phishing the Big Fish”
As Senior Leaders, you are in the spotlight of your agency. This makes you a more valuable target for nefarious people on the Internet.
Phishing is largely a criminal activity employing social-engineering tactics to defraud Internet users of sensitive information and steal credentials, money and/or identities. A phishing attack begins with a spoofed email masquerading as trustworthy electronic correspondence that contains hijacked brand names of banks, credit card companies, or commerce sites. The language of a phishing email is misleading and persuasive by generating either fear or excitement to ultimately lure the recipient to a fraudulent Web site.

Spear Phishing is an e-mail spoofing fraud attempt that targets a specific organizations and users, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by organized perpetrators out for financial gain, trade secrets, or national security information. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source.

Whaling is a spear phishing attempt to target Senior Executives/Leadership (i.e. the big fish).

**High-Profile Gmail Users Target of Chinese Phishing Scam**

Google's Gmail service was the target of a massive China-based phishing scam, according to the company's blog. The goal seemed to be the gathering not of money but information. "This campaign, which appears to originate from Jinan, China, affected what seem to be the personal Gmail accounts of hundreds of users, including US senior government officials.

"The goal of this effort seems to have been to monitor the contents of these users' emails, with the perpetrators apparently using stolen passwords to change peoples' forwarding and delegation settings. (Gmail enables you to forward your emails automatically, as well as grant others access to your account.)"

Be cautious, do not be fooled, & remember your information is precious to YOU!