How can I identify Phishing Emails? Let’s go over an Example!

1. This description is very detailed, very direct, individualized, and gives information that is not included in Service Desk emails.
2. Language indicating that the matter is extremely serious, but requires YOU to resolve the threat.
3. **BIG CLUE**: Actual Service Desk technicians and System Administrators will NEVER ask you for your domain password. They do not need it.
4. Look at the phone number. It is not the official Service Desk phone number, but an “800” toll number.
5. Phishers often use threatening language to lead the victim to believe they will face adverse consequences if they fail to comply.
6. No digital signature: if the message had come from the Service Desk, it would be signed.

**Phishing** is an attempt to acquire information such as usernames, passwords, account numbers, and credit card details by masquerading as a trustworthy entity in an electronic communication. When in doubt, examine the message for clues to its authenticity!

**Situation**

How many emails do you receive every day? 50? 100? For some users, significantly more! From both internal and external sources, our inboxes are flooded with messages, most of which are legitimate. However, every now and then an email shows up in our inbox that looks legitimate... but it is meant to deceive. With just a few mouse clicks and keystrokes, this fraudulent message can gather your credit card or bank information, install malware or viruses onto your machine, steal your identity, or gain access to government systems.
How can I avoid being the victim of a Phishing attack on my domain account?

**Do:**

- Take the time to carefully read emails that request any type of information from you, in order to determine their authenticity.
- Be careful of divulging PII (Personally Identifiable Information) in email form unless the recipient has been verified and the message itself is properly protected (encryption).
- Contact the service desk directly utilizing previously tested methods (saved phone numbers, Global Address List) if you receive email messages requesting account information (contact information provided below). As a matter of policy, most legitimate entities will never ask for your account information, username, or password in an email message.
- Be suspicious of unsolicited messages that seem “custom tailored” to you and your role within the organization (Spear Phishing), or are not digitally signed.
- If you receive an e-mail that is obviously SPAM or inappropriate for government systems, or if you believe that you have been the target of a phishing attempt, please conduct the following:
  - Send the email as an attachment to OSD.SPAM@mail.mil, so that analysis can be conducted on the message to determine its nature, and to enable us to block messages from those malicious sources in the future.
  - For further information regarding the suspected phishing attempt please contact:
    - The JITSPP – WHS EITSD Computer Incident Response Team (CIRT) by phone: (571)372-8000 or by email: whs.pentagon.eitsd.list.cirt@mail.mil
    - The JITSPP – ITA Pentagon Computer Incident Response Team (PENTCIRT) by phone: (703)695-2478 or by email: usarmy.pentagon.hqda-ita-eima.mbx.pentcirt-ndwo@mail.mil
    - The JITSPP – WHS EITSD Service Desk (24 Hours) by phone: (703)693-9600 or by email: eitsdcustsupport@osd.mil
    - The JITSPP – ITA Service Desk (24 Hours) by phone: (703)571-4482 or by email: usarmy.pentagon.hqda-ita.mbx.ita-service-desk@mail.mil

**Do Not:**

- Click on or open links embedded into an email if you cannot verify the authenticity of the message and of the sender.
- Open or forward chain emails or strange offers. Not only does this expose other users to phishing attempts, it also causes unnecessary traffic on internal government networks which can degrade performance.
- Input information into any form fields, either within the message or at any site to which the message links, unless you have verified the site and the source.
- Auto-forward email between your personal and government accounts. Not only is this dangerous from a phishing perspective, it is also prohibited by the Acceptable Use Policy (AUP).

★ ★ ★ ★ ★ ★ ★ ★
Remember, vigilance is our first line of Defense. The best way to defend against attacks to government infrastructure is to prevent unauthorized access from occurring in the first place!
★ ★ ★ ★ ★ ★ ★ ★