THINK BEFORE YOU CLICK!

At the Department of Energy, security – both physical security and cyber security – is one of our priorities. And it takes vigilance from everyone – it's important that we all THINK BEFORE WE CLICK.

Phishing is the most common means an adversary uses to initially bypass cyber security controls. A spear phishing attack is an email sent to a specific user group that allegedly provides information, often in the form of link or attachment, which interests that group. Opening attachments or clicking on links in e-mail messages that contain malware may provide a hacker with access to an organization's firewall-protected system.

In the event you receive a suspicious email, you should report the incident to your local cyber security team. You may also forward suspicious e-mail messages and attachments directly to malware@ctfo.doe.gov. After reporting and forwarding the message, delete it. Never open attachments or click on links from people or offices unknown to you.

Some of the best practices users should follow include:

- Do not open unexpected e-mail attachments, especially those with unusual file types or contained in suspicious emails.
- Do not respond to any unsolicited (spam) incoming e-mails or click on links contained within those messages.
- Review the URL (web address) to determine if the message has any unusual characteristics.
    - For instance, DOE Headquarters emails should refer to an hq.doe.gov address, but a suspicious one may reference an hq.doe.net, .org or .edu extension.
- Review message content for unusual language.

If there are any questions, please contact: Cyber.Security@hq.doe.gov and/or your local IT help desk.