**DEPARTMENT OF DEFENSE**
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAR 1 8 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITES

SUBJECT: Shielding the Department of Defense and Family Members from "Phishing" and "Spear Phishing"

Cyber criminals continue using phishing and spear-phishing attacks; and their tactics are evolving in an increasingly predatory manner. Your cybersecurity training helps prepare you to deal with a suspicious email. But is your family prepared? How about your parents? Could they recognize a phishing email? Rather than directly targeting you, criminals are tracking and mining social media—Facebook, LinkedIn, etc.—to interact with people and compromise accounts.

Phishing continues to be successful because attackers do more research, evolve their tactics and seek out easy prey. We need to arm ourselves and our families with the defensive skills and knowledge to protect them from being victimized by a phishing email, computer or phone scam.

- Never trust links or account/password prompts within email messages
- Phishing emails sometimes have poor grammar or misspelled words
- Do not trust—Verify threatening emails or phone calls
- Never provide your user identification and/or password
- Refuse social media connection requests from anyone you haven't personally met
- Make use of spam filters for your personal email
- Never email personal or financial information (even if you know the person)
- Be wary of pop-ups… don't click links or enter any data
- Don't copy web addresses from a pop-up into a browser
- Don't click on links, download files or open attachments

Attached you will find a number of resources to share with family and friends as a great place to start a dialogue and arm them with defensive knowledge. I recommend and encourage everyone to share this document and resources with their families, friends, and communities.

Terry A. Halvorsen

Attachment:
As stated

# FREE CYBER DEFENSE EDUCATION RESOURCES

- Leverage existing youth programs in which your children may already be involved:
  - The Boy Scouts of America has a number of age-appropriate videos and resources for children, grades one through twelve known as "Cyber Chip" found at: http://bsaseabase.org/Scouting/Training/YouthProtection/CyberChip.aspx
  - The Girl Scouts, as part of the National Cybersecurity Awareness Campaign, has a number of age-appropriate resources at: http://forgirls.girlscouts.org/internet-safety/
- The FTC provides videos and fact sheets on "Chatting with Kids About Being Online" at: https://www.onguardonline.gov/media/video-0001-net-cetera-chatting-kids-about-being-online
- "A Parent's Guide to Facebook" instructs parents on how to help their children strengthen privacy controls and use social media safely: http://www.ikeepsafe.org/parents/parents-guide-to-facebook/
- ConnectSafely offers resources on smart video-gaming, dealing with teen sexting, cyberbullying, cellphone and virtual world safety tips at: http://www.connectsafely.org/
- The National Cyber Security Alliance's resources for parents, children, teachers, and small businesses covers data privacy, mobile shopping, and laptop security: https://www.staysafeonline.org/
- McGruff the Crime Dog, a program your children are likely familiar with through school programs in partnership with the National Crime Prevention Council helps you reinforce what your children have been taught and how to protect their grandparents: http://www.ncpc.org/topics.
- iKeepSafe is focused on ensuring that generations of children grow up safely using technology and the Internet and offers many resources for parents, educators, and communities to leverage: http://www.ikeepsafe.org/
- The BEaPRO Parent app assesses your family's cybersecurity habits, offers online safety advice, and explains how parents can improve the family's technology safety: http://www.ikeepsafe.org/beapro-parent-app/
- The Securing Our eCity Foundation offers extensive materials for families, businesses, and communities: http://securingourecity.org
- Microsoft has developed a very good document on how to recognize phishing email messages, links, or phone calls: http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx