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

CHIEF INFORMATION OFFICER

October 1, 2015

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

SUBJECT: DoD CIO Personal Note to the Workforce on OPM Data Breach Progress

DoD Team Mates,

I am writing to update you on progress made to help those within the DoD community who have been impacted by one of the largest data breaches ever carried out against the U.S. Government. The second Office of Personnel Management (OPM) data breach affected background investigation records of 21.5 million military, civilian, and contractor personnel. Attached is the postmaster and blog that OPM that sent to its workforce earlier today, and I wanted to address some issues for DoD in this letter.

Given the nature of our work and the requirement to hold a clearance, a large portion of the Department was affected. I want to explain what you can expect over the next several months as we work with our federal partners to notify as many of you as possible.

The Government awarded a contract to Theft Guard Solutions, Inc., doing business as ID Experts, in September 2015. ID Experts will provide a suite of identity theft and credit monitoring services for up to three years, at no cost, to impacted individuals and their dependent minor children.

This week, the Government began sending notification letters to impacted individuals via U.S. Postal mail. Notifications will only be sent via postal mail. If you are contacted by email or other means, do not provide any information. The notification letter will come from OPM, include a unique personal identification number (PIN), and explain the enrollment process. ID Experts does not have your personal information, so if you decide to enroll in credit monitoring services, you will be required to provide certain Personally Identifiable Information (PII). We anticipate that the notification process will take a considerable amount of time – likely several months.

Approximately 5.6 million of the affected individuals also had their fingerprints compromised. If an individual's fingerprints were taken, this will specifically be noted in their letter.

In addition to the services the U. S. Government is offering, there are actions that you can take to protect yourself and your family. Please see the attached list of tools and information to help guard yourself from risks associated with breaches of PII.

DoD leadership will continue to provide you with information about the notification process and how to protect your PII in the coming months. Many of your questions may be answered at OPM's online cybersecurity resource center at www.opm.gov/cybersecurity. I thank you for your continued cooperation and patience as we work to notify you individually and provide you these identity theft protections and resources.

T. A. Halvorsen

Attachments:
1. OPM Notifications Postmaster and Blog
2. Select Cybersecurity Resources for DoD Personnel
3. JITSPP Phishing Fact Sheet
4. JITSPP Phishing Warfare Brochure

Dear Colleagues,

Yesterday, we began mailing notification letters to the individuals whose personal information was stolen in a malicious cyber intrusion carried out against the Federal Government. Impacted individuals will be notified by OPM via U.S. Postal Service mail. Email will not be used.

The letters being mailed to those affected by this incident will describe the comprehensive suite of identity theft protection and credit monitoring services that will be provided for at least three years, at no cost, to impacted individuals and to their dependent minor children. An impacted individual is someone whose personal information, including Social Security Number, was stolen.

As we have noted before, those impacted by this breach are already automatically covered by identity theft insurance and identity restoration services. However, the Federal Government is providing additional services that impacted individuals are encouraged to enroll in, free of charge.

The notices will contain a personalized identification number (PIN) number which is necessary to enroll in the covered services. Please note that neither OPM, nor anyone acting on OPM's behalf, will contact you to confirm any personal information. If you are contacted by anyone asking for your personal information in relation to compromised data or credit monitoring services, do not provide it.

As you know, a very large number of people were impacted by this breach, and the nature of the information involved has national security implications as well. OPM and the Department of Defense have continued to analyze the impacted data to verify its quality and completeness, and in this process, we determined that approximately 5.6 million of the impacted individuals had their fingerprints stolen. If an individual's fingerprints were taken, this will be noted in their letter.

While Federal experts believe that, as of now, the ability to misuse fingerprint data is limited, an interagency working group with expertise in this area will review the potential ways adversaries could misuse fingerprint data now, and in the future. This group will also seek to develop potential ways to prevent such misuse. If in the future, new means are developed to misuse the fingerprint data, the government

will provide additional information to individuals whose fingerprints may have been stolen in this breach.

All of these factors make it important that we take the time necessary to make sure the notification process is carried out carefully. We're committed to getting this right. What this means is that, while the notifications are beginning this week, it could take considerable time to deliver them all.

I understand that many of you are frustrated and concerned, and would like to receive this information soon. My personal data was also stolen in this breach, and I am eager to get my notification letter as soon as possible so that I can sign up for these services. However, given the sensitive nature of the database that was breached – and the sheer volume of people affected – we are all going to have to be patient throughout this notification process.

In the meantime, please check OPM's online cybersecurity resource center at www.opm.gov/cybersecurity for updates and additional information. This website has valuable suggestions about how to reduce the risk of becoming a victim of cybercrime, has answers to many frequently asked questions, and allows you to sign up for automatic updates. We are continually refreshing the site and will continue to do so as this process unfolds.

OPM and our partners across government are working hard to protect the safety and security of the information of Federal employees, contractors and others who entrust their information to us.

Together with our interagency partners, OPM is committed to delivering high quality identity protection services to the Federal community. We will continue to update you as this process continues. Thank you for your patience, your service to the American people, and your continuing support.

Sincerely,

Beth F. Cobert
Acting Director, Office of Personnel Management

# Select Cyber Security Resources for DoD Personnel

## For OPM breach-specific Information

Visit the **OPM Cybersecurity Resource Center** at https://www.opm.gov/cybersecurity

This site contains valuable information about reducing the risk of becoming a victim of cybercrime, and answers many frequently asked questions. OPM is continually updating the website, and you can also sign up for automatic alerts. Questions not answered there can be asked by emailing cybersecurity@opm.gov.

## For DoD-specific information on cyber-security

**JITSPP Phishing Fact Sheet:** Provided as Attachment C, and available online at https://eitsdext.osd.mil/JITSPP_DoDComm/Documents/Unclass%20Phishing%20Awareness%20Flyer_JITSPP_20150825%20(3).pdf

**JITSPP Phishing Warfare Brochure:** Provided as Attachment D and online at https://eitsdext.osd.mil/JITSPP_DoDComm/Documents/Unclass%20Phishing%20Brochure_JITSPP_20150826v2.pdf

**Protecting Your Identity Toolkit**: Available online at http://pyi-toolkit.cdse.edu

**Free Antivirus software:** Available to active duty military and civilian employees for download at http://www.disa.mil/Cybersecurity/Network-Defense/Antivirus/Home-Use

**Department of the Navy OPM Data Breach**: Available online at www.secnav.navy.mil/OPMbreachDON

**US Air Force Cybersecurity**: Available online at www.af.mil/cybersecurity.aspx

***Remember, cyber-security is everyone's responsibility.***
***We must continue to be as vigilant as our adversaries.***

**Current as of October 1, 2015**

Joint Information Technology Service Provider-Pentagon (JITSPP)

# Phishing

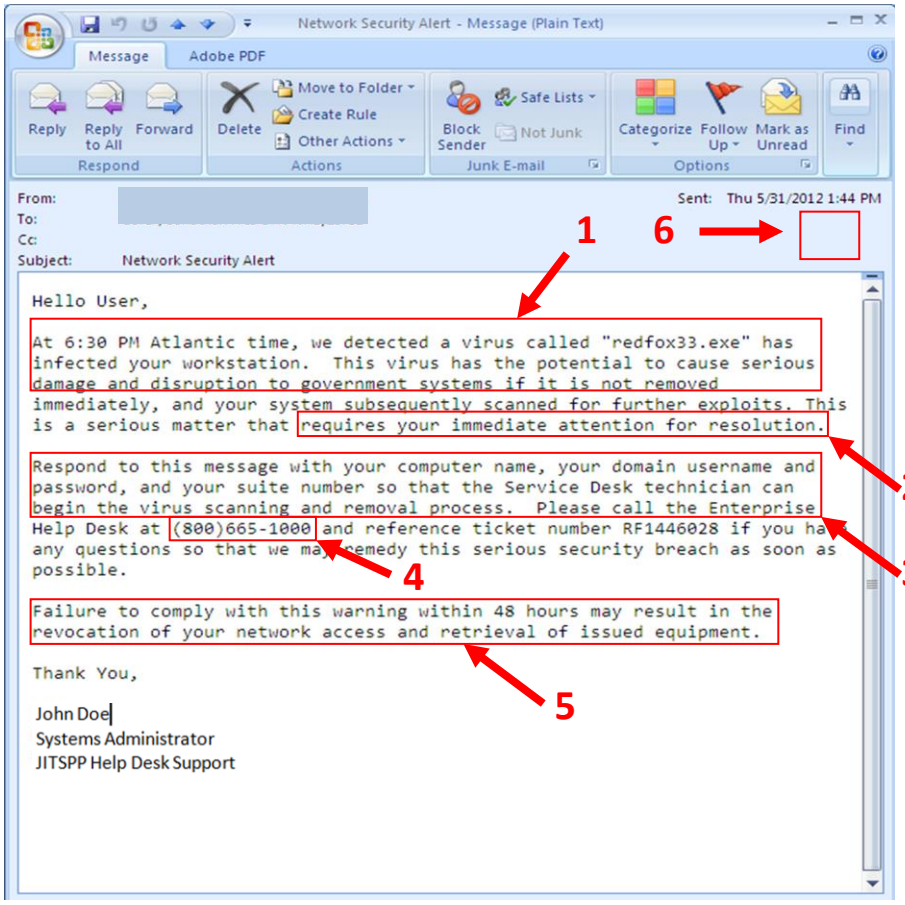
## How can I identify Phishing Emails? Let's go over an Example!

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.

## *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.

**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!



## *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!*

★★★★★★★★★★


**JITSPP – WHS EITSD CIRT**
(571)372-8000
whs.pentagon.eitsd.list.cirt@mail.mil

**JITSPP – ITA PENTCIRT**
(703)695-2478
usarmy.pentagon.hqda-ita-eima.mbx.pentcirt-ndwo@mail.mil

**QUESTIONS ABOUT THIS FLYER?**
**CONTACT**
**Cyber Security Division**
(571)372-0400
whs.pentagon.eitsd.list.isso@mail.mil

**JITSPP – WHS EITSD Service Desk**
(703)693-9600
eitsdcustsupport@osd.mil

**JITSPP – ITA Service Desk**
(703)571-4482
usarmy.pentagon.hqda-ita.mbx.ita-service-desk@mail.mil

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

## 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 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 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.



UNCLASSIFIED

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

**********CAUTION**********

If you believe that you have been the target of a phishing attempt, please conduct the following:
o 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.

### Questions about Phishing? Contact:

Cyber Security Division
Ph: (571) 372-0400
Email: whs.pentagon.eitsd.list.isso@mail.mil

JITSPP - WHS EITSD COMPUTER INCIDENT RESPONSE TEAM (CIRT)
PH: (571) 372-8000
Email: whs.pentagon.eitsd.list.cirt@mail.mil

JITSPP - ITA PENTAGON COMPUTER INCIDENT RESPONSE TEAM (PENTCIRT)
PH: (703) 695-2478
Email: usarmy.pentagon.hqda-ita-eima.mbx.pentcirt-ndwo@mail.mil

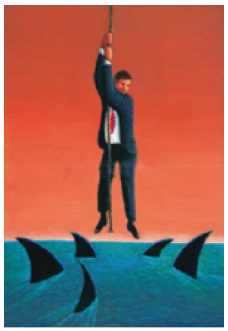
UNCLASSIFIED

# Phishing Warfare

UNCLASSIFIED

**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 ecommerce 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 unauthor - ized 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.



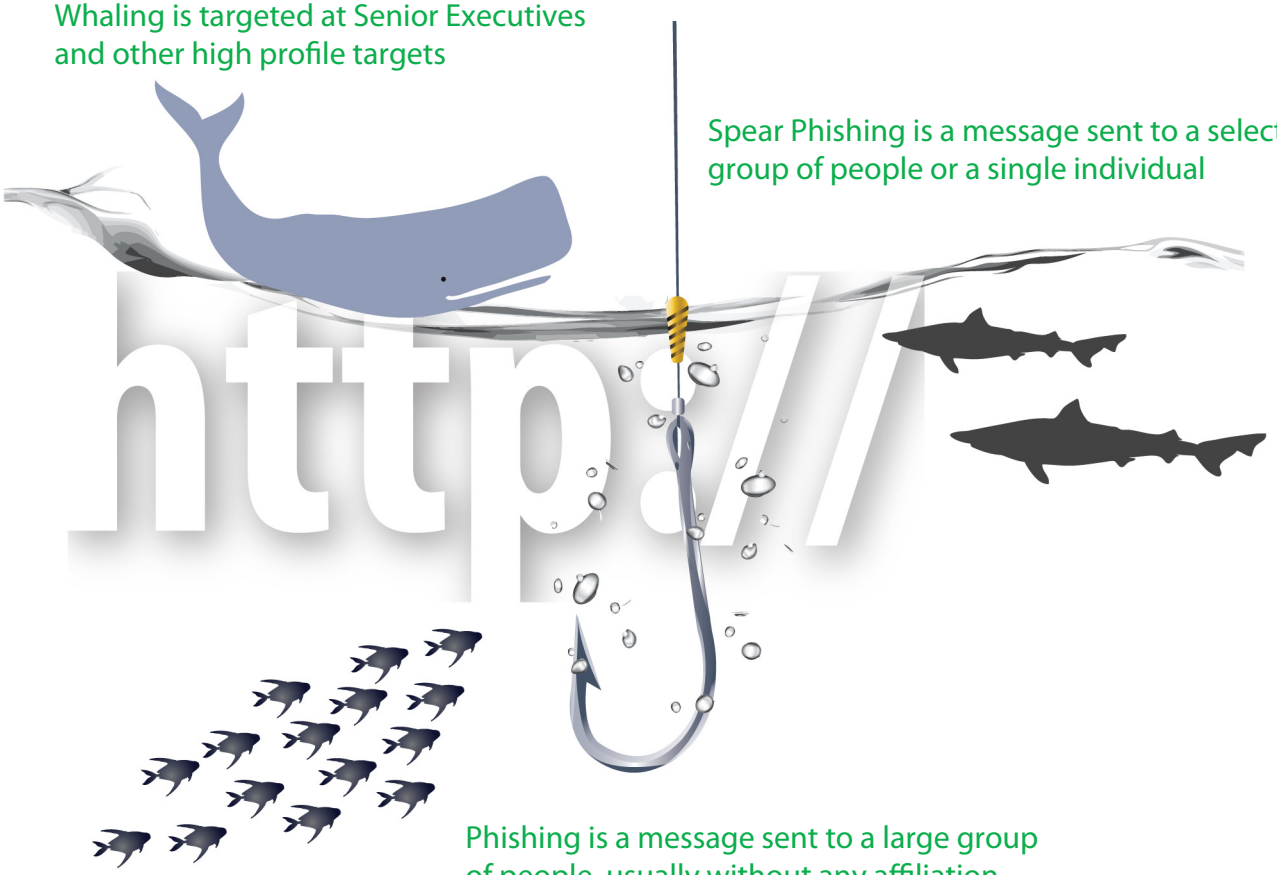
**Whaling** is a spear phishing attempt to target Senior Executives/Leadership (i.e. the big fish).

UNCLASSIFIED

UNCLASSIFIED

Whaling is targeted at Senior Executives and other high profile targets

Spear Phishing is a message sent to a select group of people or a single individual




Phishing is a message sent to a large group of people, usually without any affiliation

## What could be the Technical and Operational Impact?

In 2010, during a joint military exercise sponsored by a functional Combatant Command, a service Red Team (as part of their exercise pre-positioning phase), identified 190 potential targets (first name, last name, and military ranks). The Red Team deduced, selected, and targeted 7 user e-mail accounts with 1 phishing email. The phishing e-mail was neither digitally signed nor encrypted and contained malicious code attached to a Microsoft Excel file. 2 of 7 targeted users clicked the phishing email.

This set forth a spiral of events that allowed the Red Team to establish connections, steal files, capture data, and remotely execute commands of their choosing. The Red Team eventually achieved Domain Admin Privileges over more than 6,800 user accounts, 5,400 computer accounts, and all associated password hashes. The detrimental impact on the technical and operational capabilities of the organization to perform its mission was high (high impact to the confidentiality and integrity of information systems and networks).

UNCLASSIFIED

UNCLASSIFIED