Why Phishing Works

• We are easily fooled — we trust known brands/logos
• Lack of user education and awareness
• Lack of Information Assurance knowledge and warning indicators
• Visually deceptive text
• Image mimicking Windows
• Image masking
• Spear phishing is a message sent to a smaller, more specific group of individuals
• Phishing is targeted at a smaller group of people

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear as if they were sent from a legitimate organization. Predictive analytics are used to identify phishing emails and determine whether or not to forward them to the recipient.

Help! I think I’ve been Phished!

Anti Phishing Quick Reaction Drill

• Change your password immediately at the real website:
  - Type the website name in your browser’s address bar.
  - Sign into your account and click the “user profile” or “change password” link.
  - Follow the website’s instructions to change your account information and password.
  - If you are using a government computer, contact your local Information Assurance Officer and servicing Network Enterprise Center (NEC).

Recognizing & Avoiding Email Scams:
http://www.us-cert.gov/reading_room/emailscams_0905.pdf

SUSPICIOUS ACTIVITY REPORTING

Report Phishing Attacks to Your Local Information Assurance Officer and your servicing Network Enterprise Center (NEC)
SUSPICIOUS ACTIVITY REPORTING

Why Phishing Works

• We are easily enticed — we trust known brands/logos
• Lack of user education and awareness
• Lack of Information Assurance knowledge and warning indicators
• Visually deceptive text
• Image masking
• Image mimicking Windows

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear as if they were sent from a legitimate organization or known individual. These emails often attempt to attract users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords that can further expose them, their network, and their unit to future compromises.

In order to fully understand phishing and how it can impact you and your unit, you should be aware that there are different types of phishing:

**Phishing** is usually an e-mail sent to a large group of people that attempts to scam the recipients. The people the message is sent to often do not have anything in common.

**Spear phishing** is a message sent to a smaller, more select group of targeted people or to a single individual.

**Whaling or whale phishing** is a highly personalized message sent to senior executives, high-level officials, or their personal executive staff members.

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear as if they were sent from a legitimate organization or known individual. These emails often attempt to attract users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords that can further expose them, their network, and their unit to future compromises.

In order to fully understand phishing and how it can impact you and your unit, you should be aware that there are different types of phishing:

**Phishing** is usually an e-mail sent to a large group of people that attempts to scam the recipients. The people the message is sent to often do not have anything in common.

**Spear phishing** is a message sent to a smaller, more select group of targeted people or to a single individual.

**Whaling or whale phishing** is a highly personalized message sent to senior executives, high-level officials, or their personal executive staff members.

Why Phishing Works

• We are easily enticed — we trust known brands/logos
• Lack of user education and awareness
• Lack of Information Assurance knowledge and warning indicators
• Visually deceptive text
• Image masking
• Image mimicking Windows
Why Phishing Works

- We are easily enticed—we trust known brands/logos
- Lack of user education and awareness
- Lack of Information Assurance knowledge and warning indicators
- Visually deceptive text
- Image masking
- Image mimicking Windows

Phishing

- Phishing is usually an e-mail sent to a large group of people that attempts to scam the recipients. The people the message is sent to often do not have anything in common.

Spear phishing

- Spear phishing is a message sent to a smaller, more select group of targeted people or to a single individual.

Whaling or whale phishing

- Whaling or whale phishing is a highly personalized message sent to senior executives, high-level officials or their personal executive staff members.

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear as if they were sent from a legitimate organization or known individual. These emails often attempt to attract users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords that can further expose them, their network, and their unit to future compromises.

In order to fully understand phishing and how it can impact you and your unit, you should be aware that there are different types of phishing:

Phishing

Spear phishing

Whaling or whale phishing

Help!

I think I've been Phished!

Anti Phishing Quick Reaction Drill

- Change your password immediately at the real website:
  - Type the website name in your browser's address bar.
  - Sign into your account and click the "user profile" or "change password" link.
  - Follow the website's instructions to change your account information and password.
  - Click the "contact us" link found on most websites.
  - Change your password immediately at the website and inform your local Information Assurance Officer and your servicing Network Enterprise Center (NEC).

Recognizing & Avoiding Email Scams:

http://www.us-cert.gov/reading_room/emailscams_0905.pdf

Report Phishing Attacks to Your Local Information Assurance Officer and your servicing Network Enterprise Center (NEC).
User Awareness

- Most phishing attempts are for identity theft, but phishing is also being used to gain access to online banking, federal, and DoD information
- Phishing Attacks can be geared to collect personal information such as: SSN, mother’s maiden name, date of birth, passwords, credit card numbers, etc.
- Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software
- Malicious software can be viruses and other computer code designed to allow a hacker to use your computer for illegal Internet activity, or to access your unit's network to gather DoD information
- Malicious code may capture your keystrokes or capture your personal and work files and send them to people without your knowledge

Protect Yourself and Your Organization

**DO**

- Watch out for phishing
- Delete suspicious emails
- Contact your Information Assurance Officer or your servicing Network Enterprise Center (NEC) if you have questions about emails
- Report any potential incidents

**DO NOT**

- Open suspicious emails
- Click on suspicious links in emails or pop-up windows
- Call telephone numbers provided in suspicious emails
- Disclose any information
User Awareness

- Most phishing attempts are for identity theft, but phishing is also being used to gain access to online banking, federal, and DoD information.

- Phishing attacks can be geared to collect personal information such as: SSN, mother's maiden name, date of birth, passwords, credit card numbers, etc.

- Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software.

- Malicious software can be viruses and other computer code designed to allow a hacker to use your computer for illegal Internet activity, or to access your unit's network to gather DoD information.

- Malicious code may capture your keystrokes or capture your personal and work files and send them to people without your knowledge.

Protect Yourself and Your Organization

**DO**

- Watch out for phishing
- Delete suspicious emails
- Contact your Information Assurance Officer or your servicing Network Enterprise Center (NEC) if you have questions about emails
- Report any potential incidents

**DO NOT**

- Open suspicious emails
- Click on suspicious links in emails or pop-up windows
- Call telephone numbers provided in suspicious emails
- Disclose any information
User Awareness

- Most phishing attempts are for identity theft, but phishing is also being used to gain access to online banking, federal, and DoD information
- Phishing Attacks can be geared to collect personal information such as: SSN, mother’s maiden name, date of birth, passwords, credit card numbers, etc.
- Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software
- Malicious software can be viruses and other computer code designed to allow a hacker to use your computer for illegal Internet activity, or to access your unit’s network to gather DoD information
- Malicious code may capture your keystrokes or capture your personal and work files and send them to people without your knowledge

Protect Yourself and Your Organization

DO

- Watch out for phishing
- Delete suspicious emails
- Contact your Information Assurance Officer or your servicing Network Enterprise Center (NEC) if you have questions about emails
- Report any potential incidents

DO NOT

- Open suspicious emails
- Click on suspicious links in emails or pop-up windows
- Call telephone numbers provided in suspicious emails
- Disclose any information
SUSPICIOUS ACTIVITY REPORTING

Phishing

Phishing is a message sent to an individual, more commonly an email, to a large group of people that are sent to not have anything in common with the recipient. The people who receive the messages are targeted because of their network and their trust in other companies.

Phishing is usually an email sent to a large group of people that attempts to scam the recipients. The people the message is sent to may have no connection to the sender of the message.

Spear Phishing

Spear phishing is a more personalized method of phishing. It involves sending a targeted email to a specific individual or group of people. The email is designed to appear as if it were sent from a legitimate source and contains personalized information that makes it more convincing to the recipient.

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear legitimate, and they often contain links or attachments that, when clicked, can download malicious software or direct the user to a fraudulent website.

Why Phishing Works

• We are easily tenticed—we trust known brands/logos
• Lack of user education and awareness
• Lack of Information Assurance knowledge and warning indicators
• Visually deceptive text
• Image mimicking Windows
• Image masking
• Brand/Logos
• We are easily missed—we trust known brands/logos

Help!
I think I’ve been Phished!

Anti Phishing Quick Reaction Drill

• Change your password immediately at the real website:
• Type the website name in your browser’s address bar.
• Sign into your account and click the “user profile” or “change password” link.
• Follow the website’s instructions to change your account information and password.
• Click the “contact us” link found on most websites and inform them about the phishing attack you just experienced.
• If you are using a government computer, contact your local Information Assurance Officer and servicing Network Enterprise Center (NEC).

Recognizing & Avoiding Email Scams:
http://www.us-cert.gov/reading_room/emailscams_0905.pdf

Report Phishing Attacks to Your Local Information Assurance Officer and your servicing Network Enterprise Center (NEC)